19. Wahlperiode

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Wortprotokoll
der 103. Sitzung

Ausschuss für Inneres und Heimat
Berlin, den 26. Oktober 2020, 10:00 Uhr
Berlin
Konrad-Adenauer-Str. 1, 10557
Paul-Löbe-Haus, Raum E 700

Vorsitz: Andrea Lindholz, MdB

Tagesordnung - Öffentliche Anhörung

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen

BT-Drucksache 19/21986

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss für Wirtschaft und Energie
Ausschuss Digitale Agenda
Haushaltsausschuss

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung

Berichterstatter/in:
Abg. Josef Oster [CDU/CSU]
Abg. Helge Lindh [SPD]
Abg. Dr. Bernd Baumann [AfD]
Abg. Manuel Höferlin [FDP]
Abg. Ulla Jelpke [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

Inhaltsverzeichnis

Mitglieder des Ausschusses

	Ordentliche Mitglieder	Stellvertretende Mitglieder
CDU/CSU	Lindholz, Andrea Oster, Josef	
SPD	Lindh, Helge	
AfD	Baumann, Dr. Bernd	
FDP	Höferlin, Manuel	
DIE LINKE.	Jelpke, Ulla	
BÜNDNIS 90/DIE GRÜNEN	von Notz, Dr. Konstantin	
fraktionslos		

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 26. Oktober 2020, 10:00 Uhr
„Passgesetz“

Roland Appel
Roa.Consult, Bornheim

Prof. Dr. Georg Borges
Universität des Saarlands, Saarbrücken

Prof. Dr. Christoph Busch
Hochschule Darmstadt

Friedemann Ulrich Ebelt
Digitalcourage e.V., Bielefeld

Dr. Stefan Hofschen
Bundesdruckerei GmbH, Berlin

Dr. Thilo Weichert
Netzwerk Datenschutzexpertise GbR, Kiel

Einziger Tagesordnungspunkt

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen

BT-Drucksache 19/21986

Vors. **Andrea Lindholz** (CDU/CSU): Dann darf ich Sie alle heute Morgen ganz herzlich zu unserer 103. Sitzung des Ausschusses für Inneres und Heimat und zur heutigen Anhörung begrüßen. Entwurf eines Gesetzes zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen. Zunächst einmal herzlichen Dank für die Teilnahme aller Sachverständigen. Wir haben auch von allen Sachverständigen entsprechend vorher Stellungnahmen bekommen. Für die Bundesregierung ist Herr Ministerialdirigent Bürger heute bei uns. Wir haben zugeschaltet per Videokonferenz Herrn Professor Busch und Herrn Professor Borges. Und bei uns sind Herr Appel, Herr Ebelt, Herr Dr. Hofschen und Herr Dr. Weichert. Für die Anhörung ist wieder ein Zeitfenster von zwei Stunden vorgesehen. Wir werden die Anhörung im Parlamentsfernsehen übertragen, wie üblich. Im Anschluss wird auch ein Protokoll erstellt, das auch nochmal zur Durchsicht übersandt und entsprechend auch in der Gesamtdrucksache mit umfasst wird. Die Anhörung erfolgt so, dass wir zunächst den Sachverständigen die Möglichkeit geben, ein fünfminütiges Eingangsstatement abzugeben. Sie können in der Regel davon ausgehen, dass die Kolleginnen und Kollegen Ihre Stellungnahmen auch gelesen haben und sich dann sozusagen auf das Wesentliche beschränken. Nach diesen Eingangsstatements werden wir die Fragerunde durch die Berichterstatterinnen und Berichterstatter haben und hinterher in alphabetischer Reihenfolge die Antwortrunde. Bei der Frageregelung gilt bei uns Folgendes: In der ersten Fragerunde können zwei Fragen an einen Sachverständigen gestellt werden, eine gleiche Frage an zwei unterschiedliche Sachverständige oder an zwei unterschiedliche Sachverständige jeweils eine unterschiedliche Frage. Wie weit wir dann für eine zweite Runde kommen, werden wir sehen. Gibt es von Ihrer Seite noch Fragen? Wenn das nicht der Fall ist, dann würden wir jetzt einsteigen in die Eingangsstatements und beginnen würde ich mit Herrn Appel. Bitte schön.

SV **Roland Appel** (Roa.Consult, Bornheim): Danke schön, Frau Vorsitzende, sehr geehrte Damen und Herren Abgeordnete. Der Gesetzentwurf, der uns vorliegt, handelt von Sicherheit, Erhöhung der Sicherheit. Die höchste Sicherheit böte zweifellos die Fotoaufnahme im Amt. Manipulationen von Bildern sind in Fotostudios und in der Cloud grundsätzlich nicht auszuschließen. Insofern ist der vorliegende Gesetzentwurf in der heutigen Form inkonsistent und widersprüchlich. Private Anbieter von Fotokabinen und -terminals sind bundesweit in über 1.500 kommunalen Standorten tätig, von Berlin über Köln bis München bis in die kleinste Kommune Hürup mit knapp über 1.100 Einwohnern – das liegt in Schleswig-Holstein –, mit angepassten Lösungen. Sie gewährleisten Service innerhalb von wenigen Stunden und sind flexibel. Die Bundesdruckerei dagegen fristet am Markt der Bildaufnahmen in den Kommunen eher ein Nischendasein. Ihre hier präsentierten Zahlen entsprechen wohl den Produktionszahlen von Geräten zur Erstaufnahme von Flüchtlingen, nicht aber dauerhaften Standorten in Meldeämtern. Trotzdem möchte die Bundesregierung die Bundesdruckerei zum einzigen Lieferanten von Geräten zur Bildaufnahme bestimmen und führt in ihrer Begründung hierfür die große Erfahrung bei der Passherstellung in der Integration von Chips in Ausweisen an. Ersteres gilt natürlich exakt seit 1879 mit der Gründung der Reichsdruckerei, aber ob die Verteilung per Post von 27.000 Unterschriftenpads oder auch die Integration von elektronischen Chips in Pässen etwas über die Kompetenz zur digitalen Bildaufnahme aussagt, das möchte ich doch in Zweifel ziehen. Es bedarf dafür mehr als der postalische Weg. Der vorliegende Gesetzentwurf stellt zweifelsfrei einen Eingriff in die Berufsfreiheit nach Artikel 12 Grundgesetz dar und dieser könnte sogar zulässig sein, wenn er geeignet, erforderlich und verhältnismäßig wäre, um das Ziel ‚Mehr Sicherheit' zu erreichen. Geeignet wäre er, wenn die Geräte der Bundesdruckerei zweifelsfrei sicherer wären als die privaten Geräte. Das trifft aber nicht zu. Die Bundesdruckerei erfüllt die BSI-Norm TR03121-32 mit ihren SST-Terminals bis heute nicht. Erforderlich ist der Eingriff nicht, weil die Systeme der privaten Hersteller nicht nur die technischen Normen erfüllen, sondern hinsichtlich Datenschutz und Sicherheitszertifikaten diese sogar übertreffen, übrigens als Ergebnis des Wettbewerbs unter den Anbietern. Der Eingriff ist zudem unverhältnismäßig, weil er

den freien Markt abschafft, obwohl sich der Wettbewerb als Innovationstreiber bewährt hat. 2006 entwickelten Private die medienbruchfreie übertragende Fotokabine, die das Foto also elektronisch von der Kabine auf den Tisch des Sachbearbeiters liefert, Small Business 2007 und 2011 das Multifunktionsterminal. Die Bundesdruckerei brachte ihre entsprechenden Geräte, das SST 2014 und ein Gerät für Flüchtlingsfotos 2015, um Jahre später auf den Markt. Die Bundesregierung will folglich ein System ohne Mängel – das den Kommunen obendrein Einnahmen einbringt durch die Beteiligung an den Einnahmen – durch ein System ersetzen, das nichts Neues zu bieten hat, aber 171 Millionen Euro zusätzlich kostet. Damit verstößt sie gegen die EU-Dienstleistungsrichtlinie. Die Unternehmen haben sich deshalb an die EU-Kommission gewandt und dort beobachtet man bereits mit Aufmerksamkeit, was hier im Bundestag beschlossen werden wird. Der Gesetzentwurf nennt erstaunlicherweise auch keine sicherheitsrelevanten Kriterien wie zum Beispiel Zertifizierungen. Die Wahl eines Anbieters als wesentliche Entscheidung, die dem BMI übertragen werden soll, bedeutet aber noch nicht an sich mehr Sicherheit. Der Gesetzentwurf widerspricht damit auch dem Grundsatz der Rechtstaatlichkeit nach Artikel 20 Absatz 3 Grundgesetz. Denn nach der ständigen Rechtsprechung des Bundesverfassungsgerichts dürfen Sie als Gesetzgeber Bundestag nicht wesentliche Entscheidungen anderen Normgebern überlassen.

Fazit: Das Gesetz verletzt die Berufsfreiheit, das Rechtsstaatsprinzip sowie die EU-Dienstleistungsrichtlinie. Gestatten Sie mir ein kleines Wort am Ende. Wir feiern dieses Jahr 30 Jahre Wiedervereinigung. Dreißig Jahre nach dem Mauerfall wäre es meines Erachtens etwas anachronistisch, einen VEB Bildaufnahme Bundesdruckerei zu etablieren. Danke schön.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Appel, vielen herzlichen Dank. Wir kommen jetzt zu Herrn Professor Borges, bitte.

SV **Prof. Dr. Georg Borges** (Universität des Saarlands, Saarbrücken): Sehr geehrte Frau Vorsitzende, sehr geehrte Damen und Herren Abgeordnete, liebe Kollegen Gutachter, ich freue mich über die Gelegenheit, hier einige Worte zu dem Gesetzentwurf sagen zu können. Ich habe am Freitagnachmittag meine schriftliche Stellungnahme eingereicht. Das war relativ kurzfristig, weil ich auch relativ kurzfristig erst bestellt worden bin. Ich bitte um Nachsicht. Ich gehe davon aus, dass Sie aufgrund der Kürze der Einreichung meiner Stellungnahme noch nicht Gelegenheit hatten, diese eingehend zu studieren. Ich werde deswegen die wesentlichen Thesen meiner schriftlichen Stellungnahme kurz zusammenfassen. Lassen Sie mich zunächst kurz zum Hintergrund meiner Stellungnahme etwas sagen. Ich selbst bin Jurist. Ich leite an der Universität des Saarlandes das Institut für Rechtsinformatik und bin Inhaber eines Lehrstuhls für IT-Recht und Rechtsinformatik. Mit dem Thema IT-Sicherheit beschäftige ich mich seit 15 Jahren in der Forschung. Identitätsmissbrauch ist einer meiner Forschungsschwerpunkte und deswegen werde ich mich auf den Aspekt der Bekämpfung des Morphing begrenzen. Das Gesetz fasst ja eine ganze Vielzahl an Gegenständen an. Ich werde mich aber auf diesen einzigen im Wesentlichen konzentrieren. Und wenn wir fragen, was soll das Gesetz zur Bekämpfung von Morphing beitragen, so muss man sich vielleicht die spezielle Dimension des Morphing vor Augen führen. Tatsächlich geht es bei dieser Manipulation von Bildaufnahmen um weit mehr als um Themen, die im Rahmen des Pass- und Personalausweiswesens zu finden sind. Ich habe mich daher gefragt, was genau die Gefahr ist, die durch das Gesetz bekämpft werden soll. Man denkt, ausweislich der Gesetzesbegründung, an Grenzüberschreitungen. Das heißt, wir würden vielleicht annehmen, dass ein ausländischer Terrorist mit Hilfe eines deutschen Komplizen, der über einen deutschen Pass verfügt, ein Bild in den Pass schmuggelt, mit dessen Hilfe der ausländische Terrorist in das Bundesgebiet einreisen kann. Das ist eine sehr ernst zu nehmende Gefahr. Man kann sich fragen, warum der ausländische Terrorist nicht einen ausländischen Pass verwendet, mit dem er genauso gut einreisen kann, aber immerhin gilt die Conclusio: Offensichtlich gibt es Gefahren aus dem Missbrauch von Ausweisen mit Hilfe manipulierter Lichtbilder – und diesen gilt es zu begegnen. Das Grundanliegen des Gesetzentwurfs kann man daher nur begrüßen.

Zweitens ist sicherlich zu begrüßen, dass die Anforderungen an den Schutz von Lichtbildern gegen Manipulation gesetzlich geregelt werden. Wie der Gutachter Appel gerade schon ausgeführt hat, sind Regelungen, die man insofern treffen möchte, ja

notwendigerweise mit Eingriffen in Grundrechtspositionen, aber auch in Positionen etwa der Kommunen, verbunden. Fragt man sich also, was das Schutzkonzept des Gesetzentwurfs ist, so geht es offensichtlich darum, die Aufnahme dadurch zu schützen, dass die Aufnahme als solche, aber auch die Übermittlung an die Behörde, geschützt wird. Das ist nicht selbstverständlich. Zu denken wäre etwa an technische Lösungen gegen Veränderungen. Man konnte letzte Woche in der FAZ lesen, dass das Unternehmen Adobe eine Art elektronisches Wasserzeichen erforscht, das diese Aufgabe erfüllen würde. Dazu kann ich nicht Stellung nehmen. Ich gehe davon aus, dass aus derzeitiger technischer Sicht keine Alternative zur Kontrolle der Aufnahme und der Übermittlung besteht. Und dann ist das Anliegen des Gesetzes im Grundsatz sicherlich richtig. Wenn man aber in die Umsetzung und das Konzept schaut – und als Juraprofessor neige ich immer dazu, in die Konzeption von gesetzlichen Maßnahmen zu schauen –, so kommen einem gewisse Zweifel oder zumindest Fragen.

Zunächst mal geht der Gesetzentwurf davon aus, dass Lichtbilder innerhalb und außerhalb der Behörden gefertigt werden können. Ich möchte dies ausdrücklich begrüßen. Vermutlich wäre eine andere Regelung grundrechtlich auch kaum zu rechtfertigen. Der Gesetzentwurf beschränkt dann die Aufnahme von Lichtbildern auf Dienstleister, wie es im Entwurf heißt. Der Begriff des Dienstleisters wird nicht näher erläutert. Der Gesetzentwurf verweist insoweit ausschließlich ohne nähere Inhaltsangabe auf eine zu fertigende Rechtsverordnung. Das ist fragwürdig und bedenklich. Auf jeden Fall schließt es aber eine inhaltliche Stellungnahme zu der noch zu fertigenden Rechtsverordnung aus. Ich möchte nur auf zwei Fragen hinweisen, die sich dabei stellen werden und die sicherlich auch grundrechtlich von Bedeutung sind: In der Verordnungsermächtigung wird von der Registrierung und Zertifizierung von Dienstleistern gesprochen. Damit – immerhin dem Klarheitsgebot genügend – wird angedeutet, dass das Bundesministerium des Innern die Möglichkeit haben soll, derartige Dienstleister einer Zertifizierungspflicht zu unterwerfen. Nun weiß ich aus meiner Befassung mit Zertifizierungsdiensten unter dem Gesichtspunkt von IT-Sicherheit, dass Zertifizierungen ausgesprochen teuer sind. Man findet in dem Gesetzentwurf keinen Hinweis zu der Frage, welche Art von Zertifizierung angedacht ist. Sollte es sich tatsächlich um eine Zertifizierung durch unabhängige Dritte handeln, die hier geregelt werden soll, dürfte das faktisch einen Marktausschluss für die meisten Dienstleister bedeuten. Kein Fotograf, der im Jahr – sagen wir mal – tausend Passfotos fertigt, wird die Kosten einer solchen Zertifizierung typisch ohne weiteres stemmen können. Und wenn diese Kosten auf die wenigen Kunden umgelegt werden müssen, dann ist das Passfoto beim Fotografen ein für Viele unerschwinglicher Luxus. Das bleibt zu bedenken, wenn man diesen Weg gehen will. Wie gesagt, der Gesetzentwurf schweigt sich zu den Anforderungen an Dienstleister aus. Ich möchte dies kritisieren. Es ist eigentlich grundrechtlich geboten und im Übrigen gute Praxis, den Grundsatz, zum Beispiel das Erfordernis hinreichend vertrauenswürdige Dienstleister, ins Gesetz zu schreiben. Wir finden hier aber zu diesem wichtigen Aspekt nicht ein einziges Wort. Das ist bedenklich.

In der zweiten Frage regelt das Gesetz die Fertigung von Aufnahmen im Behördenbereich. Es liegt nahe, dass die Aufnahme von Lichtbildern zur Passerzeugung im Behördenbereich wohl eine erhöhte Sicherheit verspricht. Den Ansatz des Gesetzes begrüße ich daher, soweit es dort heißt, dass bei Zweifelsfällen die Behörde die nachträgliche Fertigung eines zusätzlichen Lichtbilds in der Behörde unter Aufsicht anordnen kann. Damit wird zugleich klargestellt, dass dies nicht der vorrangige Weg sein soll. Wird nun die Aufnahme im Behördenbereich gemacht, bedarf es spezifischer Geräte, an die technische Anforderungen zu stellen sind. Das tut der Gesetzentwurf mit einer Verordnungsermächtigung und dem Verweis auf die Kontrolle des BSI. Das ist uneingeschränkt zu begrüßen. Was nicht zu begrüßen ist, ist ein Aspekt, den der Gutachter Appel schon hervorgehoben hat. Und das ist die Frage des Monopols der Bundesdruckerei. Für ein solches Monopol gibt es keinen sachlichen Grund aus Sicht des IT-Sicherheitsrechts. Der übliche Weg wäre eigentlich, durch technische Richtlinien die Anforderungen zu bestimmen. Und insofern erhält der Gesetzentwurf ja auch das richtig Element, indem die Sicherheit der Verfahren durch das BSI zu bestätigen ist. Zusätzlich hier ein Monopol auf einen bundeseigenen Anbieter einzurichten, ist daher aus sachlichen Gründen in keiner Weise zu rechtfertigen. Damit stellen sich zugleich verfassungsrechtliche Bedenken. Insofern hat der Kollege Appel ja einiges gesagt. Ich muss gestehen,

dass ich das in der Sache in dem Punkt „verfassungsrechtliche Zweifel am Monopol zugunsten der Bundesdruckerei“ durchaus teile.

Ein letzter Punkt. Der Gesetzentwurf beschränkt sich auf die Sicherheit der Lichtbilder in Personalausweisen und Pässen. Das ist überraschend, weil sich dieselbe Frage ja auch bei Aufenthaltstiteln für Ausländer stellt. Nun haben wir im Aufenthaltsgesetz bereits eine Regelung für die Erzeugung von Lichtbildern von Antragstellern für Auslandstitel, die aber nicht kongruent ist mit dem jetzigen System. Es scheint mir unter keinem Gesichtspunkt sinnvoll, dass Bundesbürger bei der Beantragung eines Personalausweises wesentlich anderen oder strengeren Regeln unterworfen werden sollen als Ausländer, die einen Aufenthaltstitel, etwa eine EU-Niederlassungserlaubnis oder Ähnliches, beantragen. Das Schutzbedürfnis ist auf jeden Fall gleichermaßen hoch. Es ist also dringend anzumahnen, hier eine Angleichung der Regelung mit einem einheitlichen Konzept zu erzeugen. Schluss. Vielen Dank für Ihre Aufmerksamkeit.

Vors. **Andrea Lindholz** (CDU/CSU): Der nächste in der Runde wäre dann Herr Professor Busch, bitte.

SV **Prof. Dr. Christoph Busch** (Hochschule Darmstadt): Schönen guten Tag, Frau Lindholz, sehr geehrte Damen und Herren, ich bedanke mich ganz ausdrücklich für die Einladung zu der Anhörung. Ich hoffe, ich bin gut zu hören. Zu meiner Person: Ich bin Informatikprofessor an der Hochschule Darmstadt. Ich betrachte den Gesetzentwurf also aus technischer Hinsicht und nicht aus juristischer oder wettbewerblicher Hinsicht. Ich begrüße das Gesetz ausdrücklich. Ich denke, der Entwurf ist in seinem Wesen richtig und wichtig und wird es ermöglichen, dass Deutschland endlich zu den europäischen Vorreitern im Live Enrolment Schweden und Norwegen aufschließen kann. Die Praxis der Vorlage von analogen Lichtbildern, wie sie in den letzten Jahren, Jahrzehnten ausgeübt wurde, muss so schnell wie möglich enden. Das ist sicherheitsrelevant. Ich kann bestätigen, dass nach meinem Wissen alle Produkte, die in der automatisierten Gesichtserkennung an der Schengen-Grenze eingesetzt werden, durch Morphing-Angriffe verwundbar sind. Deswegen besteht unmittelbar Handlungsbedarf. Warum ist das so? Durch die Toleranz von Gesichtserkennungssystemen ergeben sich hohe Übereinstimmungswerte für beide in einem Lichtbild enthaltenen Personen, wenn ein Morphing-Angriff durchgeführt wurde. Das bedeutet, dass die Personaldokumente – und das spielt jetzt keine Rolle, ob das ein Reisepass oder ein Personalausweis ist – ihren eigentlichen Wert verlieren, da eben diese biometrische Bindung, die man ja eingeführt hat, an den Inhaber nicht mehr gewährleistet ist.

Was sind die Alternativen? Die Handlungsalternativen sind im Gesetzentwurf auch erkennbar. Erstens Live Enrolment in Deutschland und allen anderen europäischen Ländern. Zweitens – und das ist sozusagen der gute Wille, um die Fotografen im Betrieb zu halten – eine elektronische Übertragung von digital signierten Lichtbildern direkt von den autorisierten Fotografen oder Dienstleistern in die Passbehörde. Die Beibehaltung der Verwendung ausgedruckter Lichtbilder ist aus meiner Sicht nicht zeitgemäß und auch nicht zu verantworten, ganz unabhängig von dem Einklang dieses Gesetzentwurfs mit den Digitalisierungsbemühungen, die an vielen anderen Stellen vorrangig sind. Die Frage der Wasserzeichen: Da muss ich leider enttäuschen. Das wird keine technische Lösung sein, die hier zu betrachten ist.

Unabhängig von diesen beiden Lösungsoptionen 1. und 2., die im Gesetzentwurf bedacht sind, ist es notwendig, Morphing-Attack-Detection-Verfahren zu entwickeln, die für den Einsatz an der Grenze zur Detektion von Pässen mit gemorphten Lichtbildern aus den vergangenen Jahren oder auch in Zukunft bei Reisenden aus Drittstaaten geeignet sind. Da stehen wir aber noch am Anfang. Meine Arbeitsgruppe ist beteiligt an diesen Forschungsaktivitäten. Die Erkennungsleistung und die Detektionsraten, die wir momentan erreichen können – das wird ja international getestet, u.a. vom US NIST (National Institute of Standards and Technology) – sind für einen operativen Einsatz derzeit nicht geeignet.

Ich komme zu dem zweiten Aspekt meiner Stellungnahme, die Betrachtung von Fingerbildern im Dokumentwesen. Die derzeitigen Fälle von gemorphten Pässen in polizeilichen Ermittlungen oder an Grenzen sind eigentlich Zufallsfunde. Sie sind durch Fehlverhalten der Reisenden entdeckt worden. Selbst, wenn man annehmen würde, dass es in den nächsten Jahren eine Leistungssteigerung der Morphing-Attack-Detection-Verfahren geben

sollte, bleibt der sichere Nachweis, die biometrischen Verbindungen von Personaldokumenten zu Passinhabern – also das, was man erreichen wollte, diesen starken Link, ein Pass, ein und nur ein Nutzer – bis auf Weiteres nur möglich, wenn wir die beiden Fingerbilder aus dem Pass mit den Fingerabdrücken des Reisenden vergleichen. Und dieser Fingerbildvergleich dient der Zielerreichung einer sicheren Identitätsfeststellung. Dieser Vergleich gehört momentan nicht zum Standardprozess in der Grenzkontrolle, könnte jedoch die derzeitig praktizierten Kontrollschritte in der Zukunft im Verdachtsfall ergänzen. Also, ich spreche von einer Second-Line-Inspection. Unabhängig davon, wie gesagt, ich bin kein Jurist, aber wenn ich die EU-Verordnung 2019/1157 und natürlich auch die EU-Verordnung 2252 von 2004 durchlese, dann ist das gar keine Diskussion, ob wir Fingerbilder speichern sollen, sondern das ist dort eben vorgegeben. Ich teile auch die Sorge von Kollege Weichert nicht, dass der Fingerabdruck oder die Fingerbilder als nationale Kennziffer genutzt werden könnten. Wir haben kein nationales Register von Fingerbildern und wir sollten es auch in Zukunft weiterhin nicht haben.

Ich komme zu dem technischen Vorschlag, in Deutschland statt der Indexfinger die kleinen Finger zu verwenden. Da habe ich einerseits Bedenken, dass wir nicht mehr ICAO-9303-kompatibel sind. Das ist ja das, was sozusagen die technische Spezifikation hinter diesen EU-Verordnungen ist. Es wäre also völlig unpassend, wenn Deutschland als einziges Land die kleinen Finger speichert, während alle anderen EU-Länder die Indexfinger speichern. Und aus technischer Sicht ist es natürlich auch so, je kleiner die Fingerfläche, desto weniger Minutienpunkte, je weniger Minutienpunkte, desto weniger Gewissheit habe ich für das Ergebnis des biometrischen Vergleichs. Und last not least zeigen die Usability-Studien auch, dass es wesentlich einfacher ist, den Indexfinger auf einen Fingerabdrucksensor aufzulegen als den kleinen Finger.

Kontrovers diskutiert wurde in den Gutachten ja die Frage der Anzahl der Anbieter. Es gibt gute Gründe für einen Anbieter, es gibt gute Gründe für viele Anbieter. Das ist nicht meine Aufgabe, das zu entscheiden. Ich denke, es ist klar, dass ein einziger Anbieter vielleicht schneller mögliche Probleme in der Technologie umsetzen könnte. Ein Anbieter würde vielleicht auch dazu führen, dass wir sicherstellen können, dass auch im ländlichen Raum – Herr Appel hatte ja kleine Kommunen angesprochen – für alle ein erschwinglicher Preis in der Passantragstellung gewährleistet werden kann und nicht sozusagen der hohe Umsatz dann nur in den Städten zu einem günstigen Preis und auf dem Land zu einem teuren Preis führen wird. Die Frage der Qualität ist davon unbenommen. Es wurde ja im Gesetzentwurf schon darauf verwiesen, dass das BSI Zertifizierungen durchführt und es gibt eine solche Zertifizierung für diese Erfassungsgeräte, die in den Passbehörden aufgestellt werden. Herr Appel hat sie genannt – BSI TR-03121. Ich denke, es ist zwingend erforderlich, dass der Lieferant oder die Lieferanten diese Richtlinie erfüllen. Es gibt auf der Homepage des BSI eine Liste der heute verfügbaren Produkte, die diese Zertifizierung schon erreicht haben. Da möchte ich gar nicht weiter darauf eingehen. Diese Liste liegt Ihnen vor und insofern wird die beste Technologie diejenige sein, die sicherstellen kann, dass diese Zertifizierung auch durchlaufen wurde. Die Frage des Sicherheitsniveaus ist also aus meiner Sicht eher von der Zertifizierung abhängig als von der Frage, welcher Anbieter das ist.

Abschließend möchte ich nochmal betonen: Das Gesetz ist zwingend notwendig. Im Gesetzentwurf heißt es, dass die Funktion des Passes als Dokument zur Identitätskontrolle im Kern bedroht ist. Ich finde das eine sehr vorsichtige Formulierung. Das muss man aus technischer Sicht weit dramatischer darstellen. Sollte sich die Kenntnis über die Verwundbarkeit der Gesichtserkennung bei Morphingangriffen ausbreiten, dann sind die derzeitigen Prozesse an der Grenze eigentlich nur noch als Abschreckung vor Angriffen zu bezeichnen, aber nicht mehr als Kontrolle oder Abweisung von unerlaubten Grenzübertritten. Und das Szenario, das Herr Borges gerade geschildert hat, eines Terroristen oder vielleicht auch einer Person, die aus gutem Grund nicht zur Einreise in den Schengen-Raum ermächtigt wurde, dass diese Person sich mit einem EU-Bürger zusammentut und eben über einen Morphingangriff in den Schengen-Raum einreist, das ist nicht Theorie, das ist Praxis. Das hat es nachweislich gegeben und deswegen besteht unmittelbar Handlungsbedarf. Damit möchte ich meine Stellungnahme hier beenden. Danke für die Aufmerksamkeit.

Vors. **Andrea Lindholz** (CDU/CSU): Professor Busch, vielen Dank. Wir kommen jetzt zu Herrn Ebelt.

SV **Friedemann Ulrich Ebelt** (Digitalcourage e.V., Bielefeld): Vielen Dank für die Gelegenheit zur Stellungnahme. Sehr geehrte Frau Vorsitzende, sehr geehrte Damen und Herren, mein Name ist Friedemann Ebelt. Ich vertrete hier die Position der Datenschutz- und Grundrechteorganisation Digitalcourage in Bielefeld. Mit unserer schriftlichen Stellungnahme, die auch für alle Interessierten auf bundestag.de und digitalcourage.de öffentlich ist, begründen wir, warum wir der Ansicht sind, dass die geplante Fingerabdruckpflicht schnellstmöglich gerichtlich überprüft werden sollte. Ab Juli 2020 haben wir unter dem Schlagwort „Perso ohne Finger“ begonnen, Bürgerinnen und Bürger über die geplante Pflicht zur Abgabe von zwei Fingerabdrücken zu informieren. Digitalcourage rät allen Bürgerinnen und Bürgern, die einen Personalausweis ohne Fingerabdrücke wollen, bis 2. August 2021 ein fingerabdruckfreies Dokument zu beantragen. Warum? Unserer Ansicht nach ist eine anlasslose und generelle Fingerabdruckspeicherpflicht nicht sinnvoll und auch nicht notwendig. Außerdem verstößt sie gegen Grundrechte. Als wirksamsten, schnellsten und kostengünstigsten Weg einer umfassenden Grundrechteprüfung schlagen wir vor, lehnen Sie den Gesetzentwurf ab und legen Sie dem Europäischen Gerichtshof die Frage vor, inwieweit die EU-Verordnung im Lichte der EU-Grundrechtecharta verhältnismäßig ist. Unserer Ansicht nach ist die Verordnung und die geplante Fingerabdruckpflicht nicht verhältnismäßig und damit auch das hier besprochene deutsche Gesetz, der Entwurf dazu, ist es nicht.

Die Begründung: In Stichpunkten ausgeführt sind die wie gesagt in der Stellungnahme, da auch mit Quellen und Verweisen. Erstens. Die geplante Fingerabdruckpflicht ist aus unserer Sicht ein Generalverdacht gegen Bürgerinnen und Bürger, denn erfasst werden sollen ja millionenfach hochsensible biometrische Körpermerkmale von allen Menschen, die einen Personalausweis möchten oder brauchen, also von fast ausschließlich rechtstreu lebenden Menschen, die keine kriminellen Absichten haben. Zweitens. Die geplante Fingerabdruckpflicht hat im Grundgedanken aus unserer Sicht nichts mit Freizügigkeit zu tun, sondern es ist eine Pflicht, ein Zwang, also grundsätzlich Unfreiheit. Ich kann nicht entscheiden, ob ich meine Fingerabdrücke speichern lassen möchte oder nicht. Also, vielleicht noch die Anmerkung: Aktuell ist das eben bis 2. August 2021 auf jeden Fall noch möglich. Drittens. Eine allgemeine Fingerabdruckpflicht ist auch kein gezieltes und wirksames Mittel gegen Terrorismus. Viertens. Die geplanten Maßnahmen sind nicht notwendig, um Fälschungs- und Manipulationssicherheit von Personalausweisen zu erhöhen und zu verbessern. Fünftens. Die seltenen Einzelfälle – soweit wir das den Zahlen, die wir zur Verfügung hatten, entnehmen können – dienen lediglich einer zeitlich schnelleren Überprüfung der Identität einer Person im Zweifelsfall. Und das steht unserer Ansicht nach in keinem Verhältnis zu einer anlasslosen generellen Fingerabdruckpflicht. Sechstens. Die Zahlen, die uns vorliegen, sagen erstens, dass deutsche Personalausweise verhältnismäßig selten gefälscht werden, und das liegt wahrscheinlich – so ist unser Eindruck – an aufwendigen Sicherheitsmerkmalen im Gegensatz zu anderen Personaldokumenten. Und zweitens eine Zahl, die auch schon im Bundestag gefallen ist: Es kam 2019 etwa zu 1.000 Anzeigen wegen Ausweismissbrauchs durch ähnlich aussehende Personen. Wozu uns allerdings keine Informationen vorliegen ist die Frage: In wie vielen Fällen konnte die Identität dann doch über die schon vorhandenen Verfahren geklärt werden? Und zweitens, was wurde genau angezeigt? Ging es da um den unberechtigten Erwerb von Alkohol oder vielleicht Leistungserschleichungen mit einer Bahn-Card oder Ähnliches? Siebtens. Sowohl die Empfehlungen der Folgenabschätzung der Europäischen Kommission als auch die Position des europäischen Datenschutzbeauftragten und der Europäischen Grundrechteagentur wurden – soweit wir das beurteilen können – bisher leider ignoriert. Achtens. Wir befürchten langfristige – das ist wichtig – langfristige Gefahren für IT-Sicherheit und Privatsphäre der Bürgerinnen und Bürger. Denn Fingerabdrücke beziehungsweise eben Minutien und Muster werden bereits jetzt als Schlüssel beziehungsweise als Passwörter verwendet für Büros, für Fahrzeuge, für Wohnhäuser, für Smartphones. Das ist der Zugang zu unserem Online-Banking, das ist der Zugang zu unserem Privatleben, auch zu unserer privaten Kommunikation. Wir befürchten, langfristig mehr Verbreitung von digitalisierten Fingerabdrücken heißt mehr Sicherheitsrisiken. Und Neuntens. Damit werde ich dann

jetzt auch schließen. Es existieren zum Gesetzentwurf bessere Alternativen, die, soweit wir wissen, nicht ausreichend geprüft worden sind. In unserer Stellungnahme nennen wir sechs Alternativen beziehungsweise Regulierungsspielräume. Einige wurden schon angesprochen. Die erste Alternative wäre die Optimierung des bisherigen Verfahrens zur Überprüfung der Identität, also die Frage, warum dauert das aktuell so lange. Aber auch Zahlen: Wie oft ist das denn überhaupt notwendig? Der europäische Datenschutzbeauftragte argumentiert in seiner Position für die Verwendung von Minutien und Mustern statt kompletter vollständiger Fingerabdrücke. Dann die eben angesprochene Option, nicht die Zeigefinger zu verwenden, sondern Ringfinger oder kleine Finger. Dr. Thilo Weichert wird noch auf einen Regulierungsspielraum hinsichtlich einer engeren Zweckbindung eingehen. Grundsätzlich möglich ist natürlich auch die Reform der Ausweispflicht, weil die zugrundeliegende Verordnung sagt, sie erstreckt sich nicht auf Aufenthaltskarten, die allen Menschen, unabhängig von deren Staatsangehörigkeit, ausgestellt werden. Das wäre gegebenenfalls auch diskriminierungsärmer. Und schließlich als sechste Option gezielte Sicherheitsgesetzgebung, also mit einem Fokus auf konkrete Bedrohungen und nicht mit dem Fokus auf die gesamte allgemeine Bevölkerung. Soweit mein Statement und ich danke für die Aufmerksamkeit.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann bitte Herr Dr. Hofschen.

SV **Dr. Stefan Hofschen** (Bundesdruckerei GmbH, Berlin): Ja, sehr geehrte Frau Vorsitzende Lindholz, sehr geehrte Damen und Herren Abgeordnete, vielen Dank, dass auch wir uns hier heute äußern dürfen. Mein Name ist Stefan Hofschen. Ich bin Geschäftsführer der Bundesdruckerei. Ich betrachte den Gesetzentwurf in erster Linie aus technischer Perspektive und aus der Perspektive des Unternehmens, das heute für den Betrieb dieses Systems in großen Teilen verantwortlich ist. Vielleicht kann ich da ein paar Dinge beitragen. Im Wesentlichen geht es um das Thema Morphing, das bereits mehrfach angesprochen worden ist, neben einigen anderen Aspekten im vorliegenden Gesetzentwurf. An dieser Stelle möchte ich mich aber auf die Frage des Morphings und der Aufnahme der Gesichtsbilder konzentrieren, ein Thema das auch in der ICAO sehr intensiv diskutiert wird. Und wie schon mehrfach anklang, gibt es Stand heute keine technischen Möglichkeiten, um Morphing wirklich zuverlässig zu erkennen. Das kann ich bestätigen. Wir selbst haben uns an entsprechenden Forschungsprojekten beteiligt. Es ist bisher ein schwieriges Thema, so dass der einzige Weg bleibt, die Bilder in einer kontrollierten Umgebung aufzunehmen und dann in das System einzuspielen. Wir müssen von der heutigen Praxis wegkommen, ausgedruckte Passbilder zu scannen. Mit dem vorliegenden Gesetzentwurf sollen ab Mai 2025 nun ausschließlich digitale Passbilder zugelassen werden. Dies begrüßen wir in diesem Zusammenhang ganz ausdrücklich. Bevor ich auf die geplante Umsetzung eingehe, möchte ich kurz ein paar Worte zu unserer heutigen Rolle in dem deutschen Pass- und Ausweiswesen sagen, da ich glaube, dass dies für den Gesamtzusammenhang ganz wichtig ist.

Ja, die Bundesdruckerei hat natürlich eine lange Historie als Sicherheitsdrucker. Das ist zweifelsfrei richtig. Aber schon mit dem Jahr 2005 – und da geht es gar nicht allein um die Einführung der Chiptechnologie beim Reisepass – hat das Thema Biometrie im Kontext Lichtbilderkennung- und Bewertung Einzug gehalten,. Spätestens mit der Einführung des elektronischen Personalausweises im Jahr 2010 hat sich die Bundesdruckerei zu einem IT-Sicherheitsunternehmen entwickelt und dazu möchte ich jetzt gerne noch ein paar Worte sagen. Mit der Einführung des neuen Personalausweises musste nicht nur eine neue Fertigungstechnologie eingeführt werden, um die neuen Sicherheitsmerkmale entsprechend zu implementieren, sondern auch, unter hoheitlicher Kontrolle, eine IT-Infrastruktur zur Erfassung, Übermittlung, Auslesung, sowie Änderung der Daten aufgebaut werden, an die neben den über 6.000 Pass- und Personalausweisbehörden, auch die Ausländerbehörden – das klang in dem Beitrag von Herrn Professor Borges eben schon an – sowie die Botschaften und Konsulate des Auswärtigen Amts direkt angeschlossen sind. Also ein großes bundesweites IT-Gesamtsystem, um hier u.a. die Bilder zu übermitteln, aber auch alle anderen notwendigen Vorgänge (wie z.B. Auslesung oder Änderung der Daten, s.o.) zu ermöglichen. Die Infrastruktur, die die Behörden dafür benötigen, kommt ebenfalls im Wesentlichen von der Bundesdruckerei und wird von ihr bereitgestellt. Das umfasst zum Beispiel die Software für die Erfassung und die Biometrieprüfung der Bilder und der Fingerabdrücke, die IT-Infrastruktur zur

Anbindung, die Software zur Übertragung der Daten inklusive Signierung und Verschlüsselung sowie z. B. über 28.000 Fingerabdruckscanner und über 26.000 sogenannte Änderungsterminals, mit denen Sie Adressen- und Pinänderungen vornehmen können. Also im Prinzip die Infrastruktur, die heute bereits bei den Behördenmitarbeitern auf dem Arbeitsplatz steht. Insbesondere die Hersteller der Biometriealgorithmen und der Biometriehardware – wir arbeiten in erster Linie mit deutschen Partnern zusammen –, die wir an der Stelle unterbeauftragen und deren Komponenten wir einsetzen, sind alles Firmen, die international anerkannt sind, aber hier in Deutschland entwickeln und fertigen. Das ist im Übrigen nicht selbstverständlich, weil nicht alles, was nach Deutschland aussieht, dann auch am Ende tatsächlich in Deutschland entwickelt und in Deutschland gefertigt ist. Um zu der geplanten Änderung in Bezug auf die Erfassung von Lichtbildern zurückzukommen: der Gesetzentwurf sieht vor, dass nur noch eine ausschließlich digitalisierte und medienbruchfreie Übermittlung von Lichtbildern zulässig ist. Dafür sieht er zwei Optionen vor. Die erste Option ist, dass Bürger weiterhin Lichtbilder von privaten Dienstleistern wie Fotografen und - ich sage das an dieser Stelle ausdrücklich – nach meinem Verständnis auch von Betreibern von Fotoautomaten und anderen Aufnahmegeräten, erstellen lassen können und der Dienstleister diese dann anschließend über eine standardisierte Schnittstelle an die Behörden übermittelt. Details dazu, wie dieser Prozess und die technischen Anforderungen genau aussehen sollen, soll in einer separaten Rechtsverordnung geregelt werden. Dazu kann man heute noch nichts sagen. In jedem Fall ist es nicht so – aber das wäre dann eine Frage, die sicherlich auch noch einmal an die Bundesregierung zu richten wäre –, dass die Bundesdruckerei auf diese Art und Weise ein Monopol in den Behörden bekommt, auch wenn ihr das vielleicht gefallen würde.

Die zweite vorgesehene Option ist, dass Bürger ihr Lichtbild auch direkt durch die Behörde selbst erstellen lassen können. Und hierfür sollen die Behörden in der Tat mit Arbeitsplatzgeräten und/oder Selbstbedienungsterminals ausgestattet werden. Dazu plant das Bundesministerium des Inneren eine bedarfsgerechte Erweiterung des bestehenden Gesamtsystems. Dies ist aus unserer Sicht auch schon insofern erforderlich, da sichergestellt sein muss, dass eine dem Gesetzentwurf entsprechende Infrastruktur – es sind ja neue technische Anforderungen – tatsächlich auch in allen Behörden und zu jeder Zeit zur Verfügung steht.

Weiterhin ist geplant, die Bundesdruckerei diese Erweiterung durchführen zu lassen. Hierfür sehen wir verständlicherweise eine ganze Reihe von guten Gründen. Zum einen verfügen wir über einschlägige Erfahrungen. Wir sind heute schon einer der führenden Anbieter von Selbstbedienungsterminals. Man muss, glaube ich, unterscheiden zwischen Selbstbedienungsterminals und einfachen Fotoautomaten. Bei den Selbstbedienungsterminals sind wir einer der führenden Anbieter und haben bereits sehr viele Behörden ausgestattet. Das werden wir auch weiterhin tun, auch ohne diesen Gesetzentwurf. Zudem – und da haben wir eine Referenz genannt – haben wir zum Beispiel 2015 ein System zur Registrierung von Flüchtlingen mit 1.500 Arbeitsplätzen deutschlandweit ausgerollt. Das war der Vorläufer des Systems, das heute auch in den Ausländerbehörden genutzt wird. Die Erfassung biometrischer Daten inklusive der Aufnahme der Lichtbilder war immer Teil dieser Ausstattung. Zum anderen muss man sagen, dass eine einheitliche Ausstattung der Behörden mit einer sicheren und medienbruchfreien Infrastruktur sowohl für kleine als auch für große Behörden eine Reihe von Vorteilen bietet Die Qualitätsstandards können einheitlich sichergestellt werden, von der Erfassung der Daten bis zur Produktion der Dokumente, die ja auch in unserer Hand liegt. Das hat für die Bürger im Übrigen auch eine ganz praktische Bedeutung, weil schlechte Lichtbilder oder Lichtbilder, die für die Produktion nicht geeignet sind, dazu führen, dass die Bürger erneut in die Behörde kommen müssen. Das will keiner. Und schlechte oder biometrisch nicht einwandfreie Lichtbilder führen auch dazu, dass es beim Grenzübertritt, zu einem Problem kommen kann, da in Zukunft mehr und mehr auf automatische Kontrollen gesetzt wird. Zudem kann für die Hard- und Software eine einheitliche Wartung und eine technische Weiterentwicklung mit regelmäßigen und zeitgerechten Updates sichergestellt werden – das ist das, was wir heute auch schon für den Rest des Systems tun – und die Behörden profitieren von einem einheitlichen Service. Wir betreiben schon heute ein Callcenter und haben ein bundesweites Servicenetzwerk, um jederzeit Probleme in den Behörden beheben und Geräte austauschen zu können und Ähnliches mehr. Die hierfür erforderlichen Infrastrukturen im

Sinne dieser Erweiterung, über die wir hier reden, sind also bereits vorhanden und können auch für diese neuen Infrastrukturkomponenten genutzt werden.

Abschließend sei noch erwähnt, dass die Bundesdruckerei als Bundesunternehmen unter staatlicher Kontrolle eine hoheitliche Aufgabe für das Pass- und Ausweiswesen wahrnimmt. Das können wir in dem Fall mithilfe eines einheitlich erweiterten Systems weiterhin tun. Bisher war es der Wunsch des Gesetzgebers, dass hier eine gewisse hoheitliche Kontrolle sichergestellt ist. Dies ist einer der wesentlichen Gründe, warum die Bundesdruckerei heute zuständig ist. Soweit zu meiner Einführung. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank. Und den Schluss in der Runde macht Herr Dr. Weichert.

SV **Dr. Thilo Weichert** (Netzwerk Datenschutzexpertise GbR, Kiel): Ja, Frau Vorsitzende, sehr geehrte Damen und Herren Abgeordnete, vielen Dank für die Einladung, eine Stellungnahme abzugeben. Meine Stellungnahme beschränkt sich auf die Regelung § 5 Absatz 9 Personalausweisgesetzentwurf, also die Regelung zu den Fingerabdrücken und der Pflicht, zwei Zeigefingerabdrücke in den Ausweis aufnehmen zu lassen. Diese Regelung nimmt Bezug auf die Verordnung von der EU 2019/1157. Und dort ist in Artikel 3 Absatz 5 vorgesehen, dass Personalausweise ein Gesichtsbild und zwei Fingerabdrücke enthalten müssten. Mehr steht da nicht drin. Außerdem ist geregelt im Artikel 11 Absatz 6 dieser Verordnung, dass diese biometrischen Daten nur verwendet werden dürfen – das ist sehr wichtig – für die Echtheitsprüfung und für die Identitätsprüfung. Das heißt also, es sind keine anderen Zwecke nach der Verordnung erlaubt als eben diese beiden Funktionen. Also es steht hier nicht Terrorismusbekämpfung oder generell Kriminalitätsbekämpfung im Raum, sondern das ist sozusagen ein nächster Schritt. Wenn die Echtheit nicht festgestellt wird, dann kann das unter Umständen relevant sein, auch für die Feststellung, ob jemand ein Terrorist oder ein anderer Krimineller ist. Diese Regelungen beziehen sich auf biometrische Identifizierungsdaten und die sind besonders geschützt im Artikel 9 Datenschutzgrundverordnung. Es gibt auch in der Datenschutzrichtlinie zu Justiz und Polizei eine entsprechende Regelung in Artikel 10. Und dort wird generell die Verarbeitung von solchen Daten verboten. Nur aufgrund einer gesetzlichen oder sonstigen normativen Regelung – also es kann auch eine europäische Verordnung sein – darf eine Verarbeitung stattfinden. Die muss dann aber ausnahmsweise erfolgen und muss einer strengen Erforderlichkeitsprüfung standhalten. Dass biometrische Identifizierungsdaten in den Artikel 9 aufgenommen wurden, das liegt daran, dass wir es hier mit ganz speziellen Daten zu tun haben wegen der Unveränderlichkeit über das ganze Leben hinweg. Dann, dass diese Daten geeignet sind als Personenkennziffer. Das heißt, die Informationen lassen sich bei den unterschiedlichsten Anlässen erheben und ermöglichen das Zusammenführen von aus unterschiedlichen Anlässen erhobenen Daten, so dass ein Profiling möglich ist, dass die Erstellung von Persönlichkeitsprofilen möglich ist und auf diese Art und Weise eine zweckübergreifende Datenzusammenführung ermöglicht wird und die damit verbundenen Risiken bestehen. Deswegen haben wir im Artikel 87 Datenschutzgrundverordnung eine Regelung zur nationalen Kennziffer, genau für solche biometrischen Daten oder im Personalausweis aufgeführten Ziffern. Diese nationalen Kennziffern dürfen nur erlaubt werden, wenn wir geeignete Garantien für die Rechte und Freiheiten der Betroffenen vorgesehen haben. Diese Anforderungen werden nach meiner Einschätzung in dem Personalausweisgesetzentwurf und auch in einigen anderen Regelungen, die jetzt nicht zur Diskussion stehen, die aber aus meiner Sicht in die Diskussion eingebracht werden müssen, nicht eingehalten.

Zuerst einmal geht es um die Frage der Erforderlichkeit. Zwei Fingerabdrücke sind meines Erachtens nicht erforderlich. Weshalb zwei? Weshalb nicht vier? Weshalb nicht zehn, wie im Ausländerrecht? Und wieso nicht nur einer? Ein Fingerabdruck müsste ausreichen, um ein hinreichendes Eins-zu-eins-Matching zwischen dem, was ich auf dem Körper trage und dem, was ich im Ausweis gespeichert habe, vorzunehmen. Es ist nicht ansatzweise nachvollziehbar, weshalb hier eine darüber hinausgehende Erfassung erfolgen soll. Dann ist für mich auch nicht erkennbar, weshalb – das wurde von Herrn Ebelt schon angesprochen – eine Erforderlichkeit generell für die Identifizierung bestehen soll angesichts des Umstandes, dass in der Regel das Lichtbild ausreicht. Ich war jetzt etwas irritiert über die Aussage von Herrn Busch, dass er den Fin-

gerabdruck sozusagen als zusätzliche Sicherheitsmaßnahme standardmäßig einführen möchte. Zumindest habe ich ihn so verstanden. Okay, ich sehe schon, er rebelliert, aber dann wäre es wichtig, klarzustellen, dass nur ausnahmsweise der Fingerabdruck genommen werden soll, wenn Zweifel bestehen bezüglich des Lichtbildes. Und gut, ich sehe, Herr Busch nickt mir zu, dann ist das richtig. Aber gerade umso weniger ist es erforderlich, zwei Finger zu haben und dann insbesondere auch den Zeigefinger zu haben. Wir haben den Daumen und den Zeigefinger als die beiden Finger, die am meisten Spuren hinterlassen, die also sozusagen kriminalistisch am relevantesten sind, die aber auch am schnellsten erfasst werden können und missbraucht werden können. Sie können aufgespielt oder anderweitig verwendet werden. Und das ist dann etwas, was ein hohes Fälschungsrisiko zur Folge hat, ein hohes Risiko einer zweckwidrigen Nutzung und letztendlich korrumpiert es auch polizeiliche Ermittlungen. Wenn diese Fingerabdrücke vom Zeigefinger oder auch vom Daumen – der ist aus meiner Sicht genauso problematisch – wenn die soweit im Umlauf sind, dann sind sie für strafrechtliche Ermittlungen für die Polizei unter Umständen nicht mehr brauchbar, weil sie anderweitig verfügbar sind. Also, es wäre spannend, mal die Polizei zu fragen, was sie davon hält, dass diese beiden Daten erfasst werden.

Der letzte Punkt von mir ist die Zweckbindungsregelung. Herr Ebelt hat es auch schon angesprochen. Ich habe es auch in meiner Stellungnahme thematisiert. In § 15 Absatz 2 Personalausweisgesetz ist geregelt, dass im Fall einer Erfassung des Fingerabdrucks eine Abspeicherung in irgendwelchen Dateien nicht erlaubt ist. Aber nach meiner Interpretation des Gesetzes – und ich habe bisher in keinem Kommentar etwas anderes lesen können – wird zum Beispiel der Datenabgleich ermöglicht. Und das hätte zur Folge, dass dann anlässlich von irgendwelchen Identitätsprüfungen sofort Abgleiche mit Fahndungsdateien zum Beispiel der Polizei und möglicherweise sogar Abgleiche bei Geheimdiensten und Ähnlichem vorgenommen werden können. Der § 15 Personalausweisgesetz enthält einen Gesetzesvorbehalt. Und gerade solche Fahndungsabgleiche sind in anderen Gesetzen vorgesehen, in der Strafprozessordnung, in irgendwelchen Polizeigesetzen, also vom BKA-Gesetz bis hin zu den Landespolizeigesetzen. Deswegen ist eine Umsetzung des europäischen Rechts vorzunehmen, das ausschließlich eine Verwendung für Echtheit- und Identitätsprüfung erlaubt. Es muss also eine Regelung zusätzlich aufgenommen werden, die ein Abgleichsverbot ausspricht. Und das gilt meines Erachtens bei dieser Regelung im europäischen Recht sowohl für den Fingerabdruck als auch für das Lichtbild, also auch für das Lichtbild und nicht nur für den Fingerabdruck. Ich komme zu dem Ergebnis, dass die Regelung europarechts- und verfassungswidrig ist und deswegen früher oder später aufgehoben werden wird. Ich hoffe, dass das dann schnell der Fall sein sollte. Einen besseren Weg würde ich darin sehen – so wie das Herr Ebelt auch schon vorgeschlagen hat –, dass man vorab klären lässt, inwieweit die europäischen Vorgaben gegen vorrangige europarechtliche Vorschriften verstoßen. Darüber hinausgehend – das will ich nur am Rande ansprechen – möchte ich darauf hinweisen, dass das Problem nicht nur im Passrecht und im Personalausweisrecht besteht, sondern in viel stärkerem Maße im Ausländerrecht, wo nicht nur zwei Fingerabdrücke, sondern zehn Fingerabdrücke, erfasst werden und das weit darüber hinausgehende Zweckänderungen eröffnet. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann kommen wir zur Fragerunde. Wir beginnen mit der Union und in dem Fall Herr Oster, bitte.

BE Abg. **Josef Oster** (CDU/CSU): Frau Vorsitzende, meine Damen und Herren, schönen guten Morgen auch von meiner Seite. Ich habe eine Frage an Herrn Dr. Hofschen und eine Frage an Herrn Professor Busch. Herr Dr. Hofschen, ich bin, bevor ich in den Bundestag gewechselt bin, viele Jahre Bürgermeister gewesen und war dort auch verantwortlich für eine Meldebehörde und weiß, wie bedeutend eine Meldebehörde für das Ansehen einer Verwaltung ist und auch für das Thema Bürgerfreundlichkeit. Deswegen hätte ich eine Frage an Sie, weil mir die besonders wichtig ist: Eine Meldebehörde muss funktionieren und die Systeme, die dort installiert sind, müssen funktionieren. Ich kann eine Meldebehörde nicht zwei Tage zumachen, weil der Service nicht funktioniert. Deswegen würde mich nochmal interessieren, wie Sie das sicherstellen wollen sozusagen, dass sehr zeitnah flächendeckend bundesweit Ihr Service greifen kann und dass Sie sozusagen längere Ausfälle am System vermeiden können. Das ist die Frage an Sie. Und Herr Professor Busch, eine Frage an Sie. Wir haben über das Thema Fingerabdrücke gesprochen. Ich hätte

gern von Ihnen nochmal eine Einschätzung: Wie schätzen Sie die Gefahr ein, dass die Fingerabdrücke, die wir im Personalausweis dann zukünftig haben, missbräuchlich ausgelesen werden könnten und dann für missbräuchliche Zwecke verwendet werden könnten. Also da vielleicht nochmal eine Einschätzung, wie Sie diese Gefahr einordnen. Danke.

Vors. **Andrea Lindholz** (CDU/CSU): Als nächstes dann Herr Dr. Baumann, bitte.

BE Abg. **Dr. Bernd Baumann** (AfD): Ich hätte zwei Fragen an Professor Busch. Sie betonen ja, dass Live Enrolment die bessere technische Alternative für die Prävention von Cyberangriffen ist. Und Sie empfehlen es für Deutschland und die EU. Mit Drittstaaten, also den Rest der Welt, blieben dann aber die alten Probleme ja bestehen. Inwieweit kann man denn auf Sicht auch mit Drittstaaten, zum Beispiel südlich des Mittelmeeres oder in Afrika, in diesem Verfahren kooperieren? Sind die Sicherheitsrisiken und der mögliche Datenmissbrauch in diesen Ländern bei diesen Verfahren zu hoch? Kann man die Länder mit besserer Technik ausstatten? Braucht es neue Abkommen? Und wie machen es eigentlich andere Länder mit großem Einwanderungsdruck wie USA, Kanada, Australien? Könnte man zum Beispiel auch mit den USA einmal in diesem Verfahren kooperieren? Das wäre eine Frage. Die zweite Frage: Sie führen ja aus, dass Zufallsfunde von gemorphten, also gefälschten Pässen, in der Regel nur durch den direkten Vergleich zweier Fingerabdrücke stattfindet in der Praxis, einmal Fingerabdruck aus dem Pass und zum zweiten Fingerabdruck des Reisenden selbst vor Ort. Das sei der beste Weg zur Feststellung von Fälschungen. Es sei derzeit aber nicht Standard bei der Grenzkontrolle in Deutschland. Sollte es Ihrer Meinung nach unbedingt bei allen Auffälligkeiten und Verdachtsfällen, zum Beispiel bei Alarm eines MRD-Verfahrens, umgehend als Standard angewendet werden, also aus Ihrer technischen Sicht? Und warum wurde das bislang aus Ihrer Sicht, so wie Sie es beobachten, nicht forciert?

Vors. **Andrea Lindholz** (CDU/CSU): Dann kommen wir zu Herrn Lindh, bitte.

BE Abg. **Helge Lindh** (SPD): Vielen Dank, Frau Vorsitzende. Ich hole etwas aus, bevor ich dann zu einer Frage an zwei Sachverständige komme. Ein Ansatzpunkt, der glaube ich ganz gut oder zumindest einen der kernstrittigen Punkte der heutigen Anhörung betrifft, ist ja glaube ich sehr gut nach meiner Einschätzung in dem schriftlichen Gutachten von Herrn Professor Busch benannt. Er nennt es die entscheidende Frage in der Anhörung, also die Frage der Anbieterlösung. Darauf möchte ich mich auch in meiner Frage primär beziehen und nehme gerade auch dieses schriftliche Gutachten jetzt als Ausgangspunkt, denn dort wird in einer ziemlich logischen Abhandlung deutlich gemacht, dass im Zuge des Entwicklungsgesetzentwurfs ja schon eine erste Entscheidung gefallen sein müsste oder gefallen ist zwischen einer Entscheidung für ein Live Enrolment oder ein alternatives Modell und dass daraufhin die Dienstleisterlösung getroffen wurde. Die Argumentation von Herrn Professor Busch geht dann dahingehend, dass, wenn wir jetzt eine zweite Entscheidungsfrage haben, nämlich in Bezug auf – ich vereinfache es jetzt – „Privileg“, „Monopol“ Bundesdruckerei oder Öffnung auch für private Anbieter, wir die gleichen Maßstäbe anlegen müssten. Also, die Frage der biometrischen Qualität und den Sicherheitsaspekt, also wie wird Sicherheit gewährleistet und er macht in seiner schriftlichen Stellungnahme deutlich, dass schon im Vergleich zu der ersten Frage, in der man sich entschieden hat, eben auch eine Öffnung für Dienstleister, also für Fotografen, vorzusehen, man dort auch noch größere Sicherheitsrisiken in Kauf nimmt, aber diese Risiken nach seiner Einschätzung – wenn ich es nicht falsch gelesen habe, aber da kann er widersprechen – in diesem Fall nicht bestehen bei einer Öffnung für andere Anbieter in Bezug auf die Gerätschaften im Behördenbereich. Deshalb haben wir also hier schon mal zwei grundlegende Fragen gesetzt. Biometrische Qualität und Sicherheitsaspekt. Wir müssen glaube ich auch noch beachten, dass wir eine Tradition haben, dass es immer schon – das ist zumindest kein Argument dafür, aber gewiss auch keins dagegen – so war, dass privatwirtschaftlich Lichtbilder geliefert wurden. Das wird auch gar nicht im Gesetzentwurf oder der Begründung in Frage gestellt. Wir haben es also mit der Sicherheitsdimension zu tun, mit der Frage der biometrischen Qualität, aber auch Rechtsgütern wie der Berufsausübungsfreiheit und der Freiheit auch in Bezug auf die Eigenständigkeit der Kommunen und ihrer Entscheidungsfähigkeit, die auch ziemlich deutlich ist in einer Stellungnahme vom 2. Oktober 2020 des Deutschen Industrie- und

Handelstages wie auch der Kommunalspitzenverbände.

Nach diesen anfänglichen Ausführungen mit dem Tableau von Kriterien daher nun meine Frage an Herrn Appel und auch an Herrn Professor Borges: Sie beide haben relativ deutlich gemacht, etwas unterschiedlich begründet aber, dass Sie die in dem jetzigen Gesetzentwurf vorgesehene Lösung in Bezug auf die Vergabe der Herstellung der Gerätschaften und die Beschaffung über die Bundesdruckerei, wie Sie das deutlich machen, als sehr problematisch erachten. Wie ließe sich aus Ihrer Sicht eine konstruktive Lösung finden, die gleichermaßen den Sicherheitsbedürfnissen entspricht, als auch die Möglichkeit der Berufsausübungsfreiheit der Privatwirtschaft, gerade auch in Zeiten der Corona-Pandemie, was ja auch für uns ein wichtiges Kriterium sein muss, gewährleistet?

Vors. **Andrea Lindholz** (CDU/CSU): Herr Höferlin, bitte.

BE Abg. **Manuel Höferlin** (FDP): Vielen Dank, Frau Vorsitzende. Ja, erstmal vielen Dank für die Stellungnahmen bisher von den Sachverständigen. Die Anhörung zeigt ja, dass bei dem wichtigen Thema Morphing – das existiert ja auch nicht erst seit Kurzem, sondern schon länger – also eigentlich nur ein kleines IT-Sicherheitsproblem – will ich jetzt mal sagen, weil das ist ja vor allen Dingen durch die IT entstanden – schon wieder große, eigentlich vier Streitpunkte entstehen. Ich bin persönlich der Ansicht, dass da einige Fragen vom BMI im Vorfeld nicht ausreichend betrachtet wurden. Man sieht das ja eigentlich auch, wenn man mal den Referentenentwurf von Anfang des Jahres sieht, da ging es ja eigentlich gar nicht mehr um die Fotografen, die wären dann draußen gewesen. Also, da hat sich schon einiges getan. Man wäre vielleicht klug beraten gewesen, vorher mehr einzubeziehen. Aber es zeigt auch, dass quasi ein gewisses Restrisiko ja zugelassen werden kann, weil offensichtlich man ja jetzt sozusagen technisch ein Stück weiter rangehen möchte mit analogen Regeln eigentlich, muss man auch sagen, wenn man diese Zertifizierung angeht. Ich frage mich, warum man dann nicht noch weitergeht und sagt, na ja, in einem modernen E-Government sollte man vielleicht auch dem Bürger/der Bürgerin ersparen, so oft immer wieder auf das Amt zu rennen. Auch jetzt läuft man ja zweimal da hin: Einmal zum Foto machen, einmal zum Abholen. Da fragt man sich, warum ist das nicht ganz in einen Prozess eingebunden worden, in dem man zum Beispiel per App den Ausweis beantragt und dort auch gleich das Foto macht und technologisch abbildet, dass da nicht gemorpht wird. Und ob das dann die Bundesdruckerei macht oder innovative Startups, das sei dann dahingestellt. Ich weiß, dass die Bundesdruckerei – sicher auch durchaus zu Recht – sich mit modernen Technologien beschäftigt und die – ich will es ganz wertneutral sagen – einkauft – zu Recht –, und auch eine große Wandlung von der Reichsdruckerei, von Pässen hin zum Digitalunternehmen gemacht hat.

Ich habe zwei Fragen an Herrn Professor Borges. Herr Professor Borges, Sie thematisieren in Ihrer Stellungnahme, dass die Qualitätssicherung bei den Lichtbildaufnahmen zum einen diese nur noch in digitaler Form vorgelegt werden dürfen und zum anderen bei der Erstellung außerhalb der Behörde eine Einschränkung auf bestimmte Dienstleister vorgenommen wird und sie kritisieren zu Recht, dass zum einen der Begriff der Dienstleister an sich und zum anderen die Anforderungen an diese Dienstleister ja nicht genauer definiert werden. Deswegen Frage eins: Wie sieht es aus, wie ist Ihre Haltung zu der Konkretisierung – wir haben an anderer Stelle hier schon mal darüber gesprochen – ist es so eine Art ZÜP (Zuverlässigkeitsüberprüfung) von Fotografen, die wir dann haben oder ist das eine Art technische Überprüfung oder irgendwie, also der Wortlaut im Gesetz, da steht ja: „… durch einen Dienstleister elektronisch zu fertigen und im Anschluss von diesem auch durch ein sicheres Verfahren an die Passbehörde zu übermitteln.“ Das ist der Wortlaut. Können da auch Startups mitmachen? Wie sehen Sie das? Und die zweite Frage, Sie kritisieren ja auch die Bestimmung des Lieferanten für Fotoautomaten und Fingerabdruckscanner durch das BMI. Ich bin da ganz interessiert, selbst Herr Hofschen hat ja gesagt, da wären ja auch Private dann drin in der Behörde, so habe ich Sie verstanden, das fand ich jetzt ein bisschen – können wir vielleicht dann nachher noch drauf eingehen. Herr Professor Borges, halten Sie so eine Veränderung auf einen Lieferanten aus Sicherheitsaspekten für notwendig? Und sehen Sie in dem Änderungsantrag der Koalitionsfraktionen eine Änderung dahingehend, dass man sich einer Zertifizierung mehrerer Hersteller öffnen würde? Danke schön.

Vors. **Andrea Lindholz** (CDU/CSU): Frau Jelpke, bitte.

BE Abg. **Ulla Jelpke** (DIE LINKE.): Danke, Frau Vorsitzende. Meine beiden Fragen gehen an Herrn Ebelt. Herr Weichert hatte ja eben auch nochmal die EU-Verordnung hier sehr ausführlich dargelegt. Da sind Sie auch ziemlich einer Meinung. Ich würde jetzt ganz gern doch nochmal von Ihnen hören, wie Sie die rechtliche Situation beurteilen. Also, Sie haben ja schon angedeutet in Ihrer Stellungnahme – aber auch heute in Ihrem Statement – dass Sie davon ausgehen, dass das Bundesverfassungsgericht und der Europäische Gerichtshof möglicherweise dieses Gesetz kippt und da würde ich aber nochmal genauere Argumente von Ihnen hören. Und die zweite Frage, die ich habe, ist nochmal: Inwiefern sehen Sie einen prinzipiellen Unterschied zwischen der bereits bestehenden Pflicht, im Reisepass Fingerabdrücke abspeichern zu lassen und der Pflicht, das jetzt eben auch im Personalausweis durchzuführen? Da würde ich aber nochmal genauer wissen von Ihnen, welche grundlegenden Kritikpunkte Sie an diesen Punkten haben.

Vors. **Andrea Lindholz** (CDU/CSU): Frau Jelpke, vielen Dank. Herr von Notz.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Frau Vorsitzende, vielen Dank. Vielen Dank für all die Stellungnahmen und die Auseinandersetzung mit diesem wichtigen Thema. Ich selbst begrüße ausgesprochen, dass wir diese Anhörung hier heute machen, denn wir halten es als grüne Bundestagsfraktion für ein extrem lebensrelevantes Thema. Erstmal relevant für alle Kommunen, die beteiligt sind, aber eben auch alle Bürgerinnen und Bürger, die ja letztlich mit diesem Verfahren sehr konkret zu tun haben. Und deswegen ist es gut, dass der Deutsche Bundestag hier nicht einfach dieses Gesetz so durchwinkt – wenn ich auf Herrn Dr. Weichert kurz Bezug nehmen darf, zu sagen, „es wird dann irgendwann aufgehoben werden – und deswegen kann man nur hoffen, dass diese Entscheidung schnell erfolgt“. Soweit sind wir gekommen, dass man in Anhörungen sitzt und sagt: „Ja, wir wissen, es gibt viele verfassungsrechtliche Bedenken, aber die Groko hat sich nun mal drauf geeinigt, wahrscheinlich geht das Gesetz genauso durch, egal, was in dieser Anhörung hier besprochen wird.“ Also Leute, soweit darf es nicht kommen. Also, wir haben schon noch einen Anspruch als Legislative, verfassungskonforme Gesetze durchs Haus zu bringen und deswegen kann ich an die Groko nur sehr appellieren, auf die fundierten Hinweise hier Bezug zu nehmen und gegebenenfalls den Vorschlag abzuändern. Dafür machen wir hier ja solche Sachen.

Ich habe zwei Fragen. Ich habe nach all den klugen Sachen, die gesagt worden sind, nicht hundertprozentig verstanden, über was für eine Dimension des Problems wir eigentlich reden. Ich habe versucht, das im Vorfeld herauszufinden, wie viele Fälle es pro Jahr gibt. Ich bin auf eine einstellige Zahl gekommen. Eine einstellige Zahl. Ich lasse mich gerne widerlegen, interessiert mich von allen sozusagen, wer das beantworten kann, aber ich richte diese erste Frage an Herrn Dr. Weichert, vor allen Dingen im Hinblick darauf, wenn es eine geringe Anzahl von Morphing-Fällen gibt, was bedeutet es dann für die Fehleranfälligkeit und die Gefahren für dieses neu zu implementierende Verfahren? In den USA ist gerade eine große biometrische Datei gehackt worden und hier im Deutschen Bundestag wissen viele, wenn so Daten von einem irgendwie raus sind, die Telefonnummer oder so, dann macht man eine neue Telefonnummer. Aber auch der Präsident dieses Hauses weiß, wenn der Fingerabdruck draußen ist, ist er den Rest seines Lebens draußen. Und den holt auch nie wieder jemand zurück, weil das ist ja gerade der Gag an biometrischen Daten, dass der Fingerabdruck halt einzigartig ist und wenn die Information draußen ist, dann ist das so. Also, wie hoch ist da der Kosten-Nutzen im Hinblick auf die Problemlage, die wir überhaupt haben?

Zweite Frage geht an Herrn Appel. Mich würde einfach interessieren, wie dieses Monopol für die Bundesdruckerei, über das wir hier faktisch reden, sich auswirkt auf die bisherigen Anbieter, auf die Wettbewerbsfreiheit und auf die Kommunen. Und wir reden jetzt immer über 170 Millionen Euro, aber das ist meiner Ansicht nach nur die oberste Schicht der Kosten, die da entsteht, vor allen Dingen, wenn die Bundesdruckerei sagt, sie hat ein Servicenetzwerk – finde ich ja gut, dass sie eins hat. Die Frage ist, ist sie dafür gerüstet, ist dieses Servicenetzwerk dafür gerüstet, was da jetzt kommt? Also, wenn ich es richtig verstehe, leisten die privaten Anbieter bisher einen sehr umfangreichen Service für die Kommunen und fahren da sehr schnell raus und reparieren die Gerätschaften

und man könnte es mit der Frage auch verbinden, wenn ich eine dritte hätte, wie viele Leute mehr planen Sie denn ein, um den Service zu leisten? Leider habe ich keine dritte Frage, insofern richte ich meine Fragen an Herrn Appel. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann würde ich auch noch selber kurz zwei Fragen stellen. Einmal an Herrn Ebelt. Habe ich es richtig verstanden, Sie wollen das Gesetz am liebsten gar nicht? Wie wäre Ihre Stellungnahme dazu, wenn wir es aber hätten – einer oder mehrere Anbieter? In dem Papier selber habe ich es auf die Schnelle jetzt nicht gefunden. Und an Herrn Professor Busch nochmal die Frage: Generalverdacht gegen Bürgerinnen und Bürger, sehen Sie das genauso, wahrscheinlich nicht, aber braucht es das alles überhaupt? Das ist ja sozusagen der Vorwurf. Dann kommen wir zur Antwortrunde und fangen im Alphabet nochmal von vorne an und würden dann mit Herrn Appel beginnen.

SV **Roland Appel** (Roa.Consult, Bornheim): Ja, Frau Vorsitzende, vielen Dank. Lassen Sie mich zunächst auf die Frage des Abgeordneten Herrn Lindh eingehen. Das war ja die Frage nach: Erstens, was muss geändert werden, und zweitens, wie sieht es eigentlich mit den Sicherheitskriterien konkret aus? Wir sind sehr dafür, die Hersteller von privaten Geräten haben bereits 2011 ein Gespräch im Bundesinnenministerium gehabt mit der damals zuständigen Fachabteilung und haben damals vorgeschlagen, lasst uns doch diese Übertragung vom Gerät elektronisch medienbruchfrei auf den Sachbearbeitungstisch verbindlich machen, das heißt sozusagen, die sicherste Lösung. Das wurde damals freundlich lächelnd zur Kenntnis genommen, es wurde uns aber gesagt, ja, da gibt es Fotografen, da trauen wir uns nicht ran. Wir sind nach wie vor der Meinung, dass diese Lösung die Beste wäre, man muss übrigens auch mal zum Verständnis sagen, wir kennen auch die Bundesdruckerei seit 2005, weil wir haben ja diese medienbruchfreie Übertragung entwickelt und da hat auch damals die Bundesdruckerei dran teilgenommen. Damals bestand aber gar kein Interesse bei der Bundesdruckerei, es hat immer wieder Gespräche gegeben, zu kooperieren zum Beispiel in der Frage. Insofern war das für uns alles sehr überraschend, dass jetzt plötzlich in diesem Gesetzentwurf die Lage ganz anders ist und man sozusagen die freien Unternehmen – ich sage es mal ein bisschen locker – vom Markt verdrängen möchte. Denn eins ist doch klar, und da komme ich auf den konkreten Gesetzentwurf, der § 1 Absatz 5 des Gesetzentwurfs im Passgesetz bestimmt, dass das BMI die Bundesdruckerei, das steht in der Begründung klar drin und das ist auch nicht anders zu erwarten, als den Anbieter bestimmt. Und das wird jede Kommune auch so lesen. Und sie werden als private kaum gehört. , Ich habe ja auch gelesen, was uns Staatssekretär Professor Krings geschrieben hat, ja, also am 02.09. schrieb er noch, die Festlegung des Herstellers bedeutet, dass nicht jede Kommune zu einer Verhandlung und Beschaffung gezwungen wird, sondern dass die vom Bund übernommen wird. Am 09.10. schreibt er dann an mich: „Lieber Herr Appel, die Privaten können Ihre Geräte im Bereich der Behörde dann aufstellen, wenn sich die Gemeinde entschieden hat, behördliche Geräte nicht in Anspruch zu nehmen.“ Behördliche Geräte, damit sind dann wohl Bundesdruckereigeräte gemeint. Da sage ich, wenn ich den Gesetzentwurf lese, dann frage ich mich, was gilt denn nun? Also, es wird in demselben Gesetzentwurf, der sich seitdem nicht verändert hat, wird einmal rein interpretiert, alle Kommunen sind verpflichtet Geräte zentral zu beschaffen, und – einen Monat später – antwortet man, ja, vielleicht doch nicht. Und daraus wird deutlich, dass, wenn dieser Artikel 1 – und da komme ich zum konkreten Vorschlag – wenn § 1 Absatz 5 Gesetzentwurf nicht geändert wird, und zwar indem man statt den Hersteller von Bildaufnahmegeräten dort durch das BMI bestimmen lässt, sondern Sicherheitskriterien, wie Zertifizierungen, die für alle gleich gelten, festlegt, so lange wird ein Eingriff in den Wettbewerb stattfinden und der wäre – das erspare ich mir jetzt auszuführen, steht in unserem Gutachten drin – verfassungswidrig. Und das müsste ganz konkret – zur Frage von Herrn Lindh – unbedingt geändert werden und natürlich muss in Artikel 2 des Gesetzentwurfs die Formulierung wortgleich auch für den Personalausweis nachgezogen werden oder angeglichen werden. Herr Professor Borges weist ja zu Recht darauf hin, dass man eigentlich sowas im Ausländerrecht auch bräuchte. Da steht komischerweise über die Sache nichts drin.

Dann bin ich gefragt worden, was wäre die Auswirkung eines Monopols, das will ich Ihnen sagen: Für die Unternehmen einer ganzen Branche heißt das das Aus die sich übrigens gewandelt hat, auch in

den letzten 15 Jahren, vom Automatenaufsteller zum Hightech-Unternehmen, zum Hightech-Serviceunternehmen, was wirklich innerhalb von sechs bis zwölf Stunden vor Ort ist und wenn es Störungen gibt, das regeln kann, und zwar bundesweit flächendeckend. Und wir kennen unsere Wettbewerber genau und wir wissen, dass die Bundesdruckerei wirklich in den Großstädten – nach unserer Kenntnis – nur in Koblenz, in Frankfurt und im Aachen sitzt, und dazu noch einige andere kleine Ämter hat und natürlich im Ausländerbereich da groß tätig ist. Aber sie sind gegenüber den privaten Anbietern – das sage ich hier nochmal klar – ein Nischenanbieter. Und der soll nun zum Generalanbieter gemacht werden. Ich kann Ihnen gerne noch eine Grafik zeigen, aus der deutlich wird, dass das System, was Herr Dr. Hofschen beschreibt, ja im Kern aus den Fachverfahren der Anbieter, AKDB und HSH heißen die, also die machen die Behördensoftware, mit denen die Pässe überhaupt erst erstellt werden und COGNITEC ist eine Tochter der Bundesdruckerei, da kaufen wir übrigens die Software auch, die stellen diese Softwareschnipsel her, die biometrische Bilder verarbeitbar und identifizierbar machen. Also, man kennt sich, das ist nichts groß Geheimes und insofern sind wir – wie gesagt – über diesen Eingriff in den Markt sehr erstaunt. Was da noch passieren kann, also es droht für die Unternehmen die existenzielle Vernichtung, das muss ich wirklich so sagen, weil es keine Alternativen gibt, man hat sich da wirklich in einem Markt spezialisiert, und insbesondere auch deswegen ist die Lage kritisch, weil Corona natürlich dafür sorgt, dass fast ein halbes Jahr die Ämter zum Teil geschlossen waren. Das heißt, die Unternehmen sind auch dadurch angeschlagen, das sage ich hier ganz offen. Und was eine Monopolstellung in der Fläche vor Ort heißt, das kann ich Ihnen auch sagen. Vor wenigen Wochen passiert, die Gemeinde Neuenhaus im Havelland, die haben etwa 2.100 Einwohner, die bekam zur Probe ein Gerät der Bundesdruckerei und nach drei Monaten wurde ihnen eröffnet, wenn sie nicht eine Mindestzahl von Bildern pro Monat machen, müssen sie Strafgebühren zahlen. Daraufhin hat sich die Gemeinde an unseren Mitanbieter FORAM Service GmbH aus Berlin gewandt und die bekommen nun ein Gerät angepasst und ohne Auflagen. Das sind die Auswirkungen, wenn man ein Monopol hat und es keinen Wettbewerb mehr gibt. Und wenn es keinen Wettbewerb mehr gibt, dann wäre diese Gemeinde dem Anbieter alternativlos ausgeliefert und insofern möchte ich wirklich darum bitten, dass der Bundestag seine Verantwortung gegenüber der freien Wirtschaft in diesem Fall annimmt. Die Menschen dort tragen das Risiko, die finanzieren die Dinge vor und die haben nicht – wie das Staatsunternehmen Bundesdruckerei – einen Bundeshaushalt im Zweifelsfall im Rücken. Dankeschön.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Appel, vielen Dank. Dann Herr Professor Borges.

SV **Prof. Dr. Georg Borges** (Universität des Saarlands, Saarbrücken): Ja, vielen Dank. Wenn ich es richtig gesehen habe, sind drei Fragen an mich adressiert worden, von denen zwei in die gleiche Richtung gehen. Ich möchte sie deswegen – wenn das in Ordnung ist, Frau Vorsitzende – zusammen beantworten.

Vors. **Andrea Lindholz** (CDU/CSU): Ja, genau.

SV **Prof. Dr. Georg Borges** (Universität des Saarlands, Saarbrücken): Es war einmal die Frage, ob es Alternativen gibt, was Lösungen wären, wenn man die Verengung auf einen Anbieter vermeiden möchte. Und die zweite Frage, die ganz ähnlich war, war die Frage, ob die Verengung auf einen Anbieter aus Sicherheitsgesichtspunkten notwendig ist. Wenn man mich als Juristen fragt, verstehe ich die Frage natürlich hinsichtlich der Regelung und nicht der technischen Umsetzung im Detail. Frage also: Wie könnte man rechtlich sicherstellen, dass ein Anbieter von Aufnahmegeräten zur Verwendung bei der Behörde auf dem optimalen technischen Stand sind oder auf dem gebotenen technischen Stand? Was wäre die richtige Lösungsoption? Und hier meine ich, ist die Antwort relativ einfach. Wir kennen in fast allen – auch sicherheitskritischen – Technikanwendungen das übliche Verfahren, dass eine Ausschreibung erfolgt und dass zur Bedingung der Ausschreibung die Erfüllung der technischen Anforderungen gehört, die zuvor gesetzlich festgelegt sind. Hier wäre der richtige Weg, wie er hier beschritten worden ist, nämlich eine gesetzliche Grundlage, wie sie jetzt geschaffen werden soll, darauf aufbauend eine Rechtsverordnung und schließlich eine technische Richtlinie des BSI. Tatsächlich haben wir für die meisten Bereiche eine technische Richtlinie, auf die Herr Kollege Busch schon hingewiesen hat, die hier insofern ausreichend erscheint. Das heißt, das Gesetz in dem jetzigen Entwurf weist eigentlich den Weg für

eine Lösung, die aus sachlicher – aber auch verfassungsrechtlicher – Sicht geboten erscheint, nämlich den Anbieter für derartige Geräte im Wege einer Ausschreibung zu gewinnen, die typischerweise wohl Ländersache wäre und nicht zwingend Bundessache. Aber jedenfalls wäre es eine Frage der Ausschreibung, die auch die Gewähr bietet, hier den Anbieter auszuwählen, der die erforderliche Sicherheit zum besten Preis gewährleistet. Eine gesetzliche Festlegung vorab würde all die nützlichen Effekte von Wettbewerb ausschließen. Das ist aus rechtlicher Sicht von vornherein keine ideale Lösung, wenn sie nicht unbedingt geboten ist. Und nun kommen wir zu dem Punkt:, Ist es tatsächlich unbedingt geboten, dass die gesamte Technik aus einer Hand kommt? Nun hat ja die Bundesdruckerei selber ein paar Dinge dazu gesagt, Einheitlichkeit vermeidet Fehler aufgrund der Verwendung verschiedener Technologien. Das ist aber kein so richtig zwingendes Argument, weil jede Kommune ja typischerweise mit einem Anbieter konfrontiert wäre. Sie hat freilich die Möglichkeit sich den Bestgeeigneten aus dem Markt auszusuchen. Kurzum, mir fällt beim besten Willen kein zwingender Gesichtspunkt ein, warum die Technik nur von einem einzigen Anbieter geliefert werden kann. Und damit ist die Lösung – meine ich – auch schon vorgegeben, das Gesetz sollte die Sicherheitsanforderungen feststellen, es sollten die Geräte einer Zertifizierung unterworfen werden, wie man das kennt. Das BSI ist ohnehin schon involviert im Gesetzentwurf, weil es die Sicherheit sicherstellen soll. Das ist der Weg, der im Gesetz schon feststeht. Man könnte also den Satz in § 1 Absatz 5 im Wesentlichen ersatzlos streichen oder eben das Erfordernis einer Ausschreibung dort festschreiben.

Ein zweiter Punkt ist genannt worden, ich habe mir das Stichwort „TÜV für Diensteanbieter“ notiert. Die Frage ist also: Wie kann man die Anforderungen an die Dienstleister, wir denken hier an die Fotografen, die solche Bilder fertigen sollen, in angemessener Weise festlegen? Mein Bedenken hier an der Stelle ist, dass das Gesetz gar nichts dazu sagt. Dazu hat auch der Änderungsantrag der CDU/CSU und SPD nichts beigetragen – meine ich – weil er diesen Punkt nicht adressiert. Festzustellen ist, dass der jetzige Gesetzentwurf zwar eine Verordnungsermächtigung enthält, aber keinerlei inhaltliche Festlegungen an den Verordnungsgeber. Ich halte das für verfassungsrechtlich problematisch. Ich gebe zu, man ist viel gewöhnt im Bereich von geringer Festlegung an den Verordnungsgeber, aber hier wird doch ohne Not eine freie Hand an den Verordnungsgeber gegeben, da frage ich mich – vielleicht im Sinne von dem, was der Herr Abgeordnete von Notz gerade geäußert hat – ob das ein ideales Vorgehen des Gesetzgebers ist. Es steht dem Parlament zu, die wesentlichen Grundsätze einer gesetzlichen Regelung festzulegen und das ist hier in Bezug auf die Fotografen schlicht und einfach nicht der Fall. Als Hochschullehrer schmerzt mich das und deswegen möchte ich diesen Punkt ausdrücklich erwähnen. Selbst, wenn es verfassungsrechtlich zulässig sein sollte, ist es nicht vorzugswürdig, im Gesetz einfach gar nichts zu dem zu sagen, was der Verordnungsgeber regeln soll. Wie sollte es sein? Sollten wir tatsächlich einen TÜV für Fotografen haben? Ich habe in meinem Eingangsstatement schon darauf hingewiesen, dass Zertifizierungen – etwa wenn sie durch das BSI erfolgen – sehr aufwendig und teuer sind. Ich habe das in meiner Tätigkeit früher kaum glauben können, als ich damit konfrontiert wurde, dass mittelständische Unternehmen zigtausende pro Jahr für Zertifizierungen ausgeben. Was erwarten wir denn, was eine Fotografenlizenz für die Fertigung von Ausweisbildern kosten soll, wenn sie vom BSI oder von einem TÜV oder vergleichbare Organisation zertifiziert werden soll? Wir sind sofort bei etlichen Tausend Euro in solchen Zertifizierungsverfahren und da frage ich mich, wie ein Fotograf das sinnvoll leisten kann. Das heißt, wenn man mit der Anforderung an eine Zertifizierung, die im Gesetz nicht im Mindesten angesprochen ist, sondern in einem einzigen Wort nur erwähnt worden ist, wird letztlich nicht festgelegt, ob es Personalausweisbilder von freien Fotografen geben wird oder nicht. Das ist bedenklich, weil ein wesentlicher Aspekt der gesetzlichen Regelung, nämlich die Fertigung von Bildern außerhalb der Behörde, hier vollständig in die Hand des Verordnungsgebers gelegt wird. Hier – meine ich – muss der Gesetzgeber/das Parlament nachbessern, um nicht Zufallsergebnisse hinsichtlich eines sehr gravierenden Aspekts der Gesetzgebung, nämlich, können wir Personalausweisbilder noch außerhalb der Behörde fertigen, zu ermöglichen. Das heißt, der wesentliche Nebeneffekt des Gesetzes wird im Gesetz nicht adressiert in dem bisherigen Entwurf, das muss unbedingt nachgebessert werden. Ich hoffe damit auf die Fragen einigermaßen eingegangen zu sein. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dürfte ich da eine kurze Rückfrage stellen? Halten Sie jetzt die Zertifizierung für wichtig oder für nicht wichtig?

SV **Prof. Dr. Georg Borges** (Universität des Saarlands, Saarbrücken): Zertifizierung kann ja auch eine Selbstzertifizierung sein, das heißt, wenn der Fotograf angeben muss, ja, ich verwende ein Gerät, das die Anforderungen der technischen Richtlinie erfüllt. Wenn das Zertifizierung sein soll, und wenn daran zum Beispiel eine Haftungsfolge gebunden ist, dann wäre das ein sehr preisgünstiger Weg ohne Marktauswirkung. Der Teufel steckt hier in dem Wort „Zertifizierung". Ich persönlich halte es nicht für erforderlich, einen Fotografen, der ein Ausweisbild macht, einer sehr teuren Zertifizierung zu unterwerfen, wenn es einen Satz später im Gesetz heißt, dass die Personalausweisbehörde in Zweifelsfällen die erneute Fertigung des Fotos verlangt. Wir haben hier im Gesetz angelegt eine „zweite Linie" – wenn ich soweit die Worte von Herrn Kollegen Busch aufgreifen darf – denn in allen Zweifelsfällen wird ein Passfoto in der Behörde unter Aufsicht gefertigt. Das ist der wesentliche Sicherheitsanker hier und deswegen meine ich, ist es nicht unbedingt erforderlich, dass die gleiche Sicherheit bei jedem einzelnen Fotografen durch eine Zertifizierung sichergestellt wird. Entscheidend ist, dass die Technik, die der Fotograf verwendet, den Vorgaben entspricht. Und vielleicht noch ein Aspekt, den ich eben nicht adressiert habe. Klar ist doch, dass der jetzige Wortlaut bei Dienstleistern auch den Automatenaufsteller umfasst und dem Wortlaut nach zumindest auch möglicherweise die Möglichkeit einer Fernaufnahme durch „App" oder so etwas. Wenn das möglich ist, ist doch offensichtlich, dass es auf die Zertifizierung der Technik ankommt und nicht auf die persönliche Zertifizierung eines einzelnen Fotografen. Diese Weichenstellung wird im Gesetz aber in keiner Weise angesprochen. Das ist bedenklich. Wir wissen also heute – wenn das Gesetz verabschiedet wird – nicht, ob das Bundesinnenministerium in der Verordnung es zulässt, dass Fotografen das machen oder ob der Schwerpunkt auf die Zertifizierung von Technik gemacht wird. Konkret: Wenn der Fotograf eine Technik verwenden muss, die von der Bundesdruckerei entwickelt ist und vom BSI zertifiziert ist, dann brauchen wir keine großen Anforderungen an diesen Fotografen, denn er muss in Grunde nur schauen, ob der Bürger sich ordentlich gekämmt hat und er muss auf den Auslöser drücken und abkassieren. Dafür wäre eine Zertifizierung, die viele Tausend Euro kostet, schlicht und einfach unverhältnismäßig. Das aber können wir heute überhaupt nicht beurteilen, weil der Gesetzentwurf nichts dazu sagt, deswegen mein wesentlicher Einwand: Der Gesetzentwurf stellt nicht – wie er eigentlich soll – die maßgeblichen Grundsätze klar. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Ja, vielen Dank. Herr Professor Borges. Es kommt Herr Professor Busch, der Techniker, vielleicht kann er noch etwas zum Thema Zertifizierung mit dranhängen.

SV **Prof. Dr. Christoph Busch** (Hochschule Darmstadt): Ja, das werde ich gerne tun. Der Reihe nach würde ich eigentlich gerne erst nochmal betonen – als Rückantwort auf Herrn Höferlin – eine Tatsache: Wir haben es hier nicht mit einem IT-Problem zu tun, zumindest klang das aus Ihren Worten heraus. Ich habe des Thema Morphing-Attacks schon jetzt eine lange Zeit in verschiedenen Fachgremien diskutiert, mitunter kann dann die Rückmeldung, na ja, hätten wir damals keine automatische Biometrie-Grenzkontrolle eingeführt, hätten wir dieses Problem nicht. Diese Annahme ist falsch. Genauso wie die biometrischen Algorithmen verwundbar sind, im gleichen Maße sind geschulte Experten, die an unseren Grenzen Dienst leisten, ebenso verwundbar. Also was ich betonen möchte, es ist kein IT-Problem, sondern es ist ein prinzipielles Problem. Wenn Sie ein gemorphtes Lichtbild einem langjährig dienenden Beamten der Bundespolizei vorlegen, wird er nur selten richtig sagen können, ob das jetzt wirklich gemorpht wurde oder ob es ein echtes Bild ist. Das ist wichtig festzuhalten.

Als zweiten Punkt möchte ich ein bisschen über Risiken sprechen. Es wurden in vielen Kommentaren und Fragen Risiken aufgeworfen, es wird nach Risiken gefragt, Marktrisiken, Anbieterrisiken, rechtliche Risiken, Verfassungskonformität. Ich sehe ein operatives Risiko hier und damit möchte ich eingehen auf den Punkt von Herrn von Notz, wie viele Fälle gibt es überhaupt. In meinem Gutachten habe ich verwiesen auf eine Umfrage, die wir im vergangenen Oktober bei der Security Printing Conference in Kopenhagen durchgeführt haben. Dort waren Druckereien und es waren Vertreter von Grenzbehörden vor Ort. Die Umfrage hat ergeben, dass wir über 1.000 Fälle detektieren konnten, also nach unserer Kenntnis. Jetzt kann man sagen, das ist eine kleine Zahl, das Risiko ist nicht groß. Ich sehe das ganz anders. Wir haben in dieser Legislaturperiode.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): In Deutschland? Kurze Zwischenfrage, 1.000 Fälle in Deutschland, in Europa, weltweit oder wovon reden Sie?

SV **Prof. Dr. Christoph Busch** (Hochschule Darmstadt): Das war jetzt Europa. Aber jetzt kommt eigentlich mein entscheidender Punkt. Wir haben keine Möglichkeit, gemorphte Pässe zu detektieren heute, weder algorithmisch – ich verweise auf die Tests, die wir durchgeführt haben. Wir haben momentan eine geringe Detektionsleistung, wir machen das jeweils mit false positiv und false negativ. Wenn Sie annehmen, dass Sie sozusagen ein System so konfigurieren, dass es maximal ein gemorphtes Lichtbild von 100 Fällen durchlässt, dann haben wir bei unserem besten Algorithmus, und der ist weltweit unübertroffen, eine Situation, dass in fünf von 100 Fällen fälschlich ein Alarm ausgelöst wird. Das kann man operativ noch nicht ausrollen. Also wir sagen, momentan können wir anhand des Bild selbst nicht zuverlässig detektieren. Warum ist das trotzdem ein großes Risiko? Aus meiner Sicht haben wir momentan eines der drängendsten Probleme überhaupt, das „Global Warming“ in den Griff zu bekommen. Was hat das mit dem Thema heute zu tun? Das hat damit zu tun, wenn wir den Globus weiter aufheizen, wenn wir in Afrika Temperaturen haben mit 50 Grad oder höher, was werden die Menschen denn machen? Die werden nach Norden emigrieren. Was hat das mit Morphing zu tun? Die Menschen werden sich überlegen, ob sie weiterhin in ein Schlauchboot steigen und unsicher nach Malta oder Italien rüber rudern oder ob sie sich über das Internet einen gemorphten Pass besorgen und dann komfortabel, vielleicht noch kostengünstiger oder auf alle Fälle sicherer nach Europa einreisen. Das wird passieren, da bin ich ganz sicher. Und das ist ein großes Risiko. Gut, jetzt möchte ich bei dem Risiko bleiben…

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Also, wenn sowas gesagt wird, darf ich eine Zwischenfrage stellen. Sie meinen, die Leute besorgen sich einen deutschen Pass mit einem gemorphten Bild oder was ist Ihre These? Sie meinen, da aus Westafrika, die holen sich einen deutschen Pass mit einem gemorphten Bild und dann reisen die einfach über die Grenze ein.

SV **Prof. Dr. Christoph Busch** (Hochschule Darmstadt): Genau, das ist meine These. Das ist das Szenario. Das ist eine These und es ist auch in Einzelfällen schon aufgedeckt worden. Wie gesagt, es ist aufgedeckt worden nicht dadurch, dass ein Morphing-Detektionsverfahren an der Grenze installiert war, sondern dass diese Personen sich durch andere Auffälligkeiten bei der Einreise so verhalten haben, dass eben die Pässe dann genauer inspiziert wurden und dann eben deutlich wurde, dass das ein Pass ist, der nicht für den Reisenden ausgestellt wurde.

Und damit komme ich auch zu der Frage: Machen Fingerabdrücke Sinn und besteht dort ein Risiko? Ich möchte mit Herrn Weichert – mit dem ich ja viele Meinungen teile, wir haben uns in vielen Diskussionen schon getroffen, aber auch unterschiedliche Positionen habe – antworten. Er hat gesagt, Fingerprint als Standardverfahren. Das ist nicht das, was ich vorgeschlagen habe, ich habe gesagt, wenn wir eine Zunahme von gemorphten Pässen an den Grenzen beobachten werden – und dazu wird es kommen – und wenn unsere Morphing-Detektionsverfahren, sagen wir mit einer Falschalarmrate von fünf Prozent, die Leute aus dem ABC-Gate hinausschleusen in eine second line inspection und dann eben mit dem Beamten diskutieren, ob das jetzt der eigene Pass ist oder nicht, dann ist die technische Möglichkeit, diese Frage zu klären, der Abgleich der Fingerbilder. Es ist also eine Fallback-Strategie, falls der Lichtbildvergleich Zweifel aufwirft.

Ich erkenne die Gedanken von Herrn Weichert und anderen, dass man durch biometrische Erfassung an verschiedenen Punkten in einem Prozess oder an verschiedenen Orten eine Profilbildung haben könnte. Das wollen wir nicht. Deswegen soll es keine zentrale Datenspeicherung geben, aber mit Verlaub, ob jetzt die Fingerbilderfassung an der Grenze funktioniert und, beispielsweise in Frankreich ist das ja vielerorts schon Standard, dass eben über die Fingerbilderfassung mit dem Personaldokument wir uns in der Identitätsfeststellung ausweisen müssen. Wenn also die Fingerbilderkennung durchgeführt wird, dann ist es doch unerheblich für dieses Risiko, ob jetzt der Fingerabdruck auch noch im Personaldokument ist – was nebenbei unter der vollen Kontrolle des Bürgers ist – oder ob eben der Live-Finger, der gerade frisch erfasst wurde, mit irgendwelchen Datenbanken abgeglichen wird. Wie gesagt, ich möchte das nicht, ich sehe das Risiko, aber sehr, sehr klein.

Dann war die Frage, die an mich adressiert wurde:

Gibt es eine Gefahr der missbräuchlichen Auslesung des Fingerabdrucks aus dem Personalausweis oder aus dem Reisepass? Die Antwort ist klar, nein. Da haben wir gute kryptografische Protokolle, Stichwort ist Extended Access Control, das eine hohe Sicherheit bietet, die Gefahr, dass das Fingerbild aus dem Ausweis ausgelesen wird, sehe ich nicht. Die ist nur durch hoheitlich berechtigte Institutionen auslesbar. Und mit Verlaub, wenn Sie meinen Fingerabdruck bekommen wollen, warum müssen Sie meinen Personalausweis dann brechen? Sie finden den Fingerabdruck auf meinem iPhone, Sie finden die auf einem Glas, also es ist keine so öffentliche Information wie das Gesichtsbild, aber es ist eine Information, die leider sehr flüchtig ist, wie wir sagen. Gut, das war das Thema der Risiken des Auslesens und der missbräuchlichen Verwendung. Ich sehe das Risiko nicht oder wesentlich kleiner als die anderen Risiken, die ich angezeigt habe.

Zur Frage der Kooperation mit den USA. Ich bin in der Standardisierung aktiv, ich leite das Standardisierungsgremium, das für diese Datenaustauschformate in den Reisepässen zuständig ist und durch diese Standardisierungsarbeit bin ich verbunden mit den Kollegen auf der amerikanischen Seite, das ist das National Institute of Standards and Technology. Wir haben jetzt über viele Jahre – Jahrzehnte schon – Standards gemeinsam entwickelt, wir treffen uns zu technischen Konferenzen. Morgen bis Donnerstag findet eine solche virtuelle Konferenz statt, wo es um die Fragestellung der Morphingangriffe oder Detektion dieser Angriffe geht. Also die Kooperation besteht. Ich habe verwiesen auf die Testplattform im NIST, die eben die Evaluierung dieser Morphing-Tech-Verfahren durchführt. Wir haben europäisch eine weitere Testplattform aufgebaut in Kooperation mit der University of Bologna. Wir nutzen die gleichen technischen Interfaces, es gibt eine intensive Kooperation seit vielen Jahren.

Dann wurde ich gefragt von Herrn Lindh, ob ich Risiken sehe bei einer Öffnung für andere Anbieter. Ich sehe – wie in meinem Gutachten ausgeführt – operative Vorteile für den Betreiber, wenn es ein Anbieter ist, aber ein technisches Sicherheitsrisiko bei vielen Anbietern sehe ich nicht. Das muss ich so sagen. Wir haben jetzt sehr gute Argumente gehört, was passiert mit den Geräten, die in der Passbehörde aufgestellt sind, die müssen zertifiziert sein. Herr Borges hat – ich denke überzeugend – nahegelegt, dass der einzelne Fotograf nicht die Ressourcen hat, eine Zertifizierung für sein Gerät durchzuführen, insofern kann man nicht sagen, der Dienstleister muss eine Zertifizierung durchführen, aber Sie könnten sehr wohl sagen, der Fotograf soll – das ist eine Sollbestimmung – soll ein System in Betrieb haben, das Vorgaben der Gerätezertifizierung, wie sie auch in der Behörde aufgestellt wird, entspricht. Und das hätte jetzt technisch gesprochen auch den Vorteil, wir haben in dem Datenaustauschformat, also das was im Reisepass dann gespeichert wird, haben wir ein Datenfeld, das die Quelle des Bildes angibt. Man könnte also sehr wohl in dem Datenaustauschformat dann angeben, ist das ein Bild, das aus der Behörde stammt, also unter Aufsicht in der Behörde gespeichert wurde, oder ist das von einem Fotografen mit dem Gerät X Y abgespeichert worden. Das bedeutet dann, an der Grenze könnte man bei der Nutzung dieses Referenzbildes im Pass dann entsprechende Intensität der Prozesse steuern. Wenn es eine vertrauenswürdige Quelle hat, kann man vielleicht schneller den Prozess ablaufen lassen als wenn es eine Dienstleistungsquelle wäre. Ich hoffe, dass ich damit auf die Fragen geantwortet habe.

Gibt es einen Generalverdacht für alle Bürger, war noch eine weitere Frage gewesen, ich kann den Generalverdacht nicht sehen. Es ist aus meiner Sicht zwingend notwendig, dass man diese strenge Bindung, ein Bürger, ein Personaldokument, dass man das sicherstellt. Ich sehe damit keinen Generalverdacht für mich als Bürger.

Vors. **Andrea Lindholz** (CDU/CSU): Habe ich Sie jetzt gerade nochmal richtig verstanden bei der Zertifizierung, dass Sie im Prinzip gesagt haben, es ist gar kein unbedingtes Muss aus Ihrer Sicht, gegebenenfalls kann man das kenntlich machen, woher das stammt? Oder habe ich das jetzt missverstanden und würde es dann hinterher möglicherweise anders behandeln?

SV **Prof. Dr. Christoph Busch** (Hochschule Darmstadt): Nein, wir haben ja zwei Wege. Wir haben die Geräte, die in der Passbehörde aufgestellt sind, ja? Die haben wahrscheinlich auch ein hohes – ich sag jetzt mal – Angriffsrisiko. Vielleicht machen sich Hacker irgendwann zu schaffen und nehmen diese Geräte auseinander. Dort, sage ich, diese Geräte müssen zertifiziert sein. Das ist naheliegend.

Vors. **Andrea Lindholz** (CDU/CSU): Genau. Und dann beim Fotografen das Thema?

SV **Prof. Dr. Christoph Busch** (Hochschule Darmstadt): Und beim Fotografen teile ich die Meinung von Herrn Borges. Der Fotograf hat nicht die finanziellen Mittel, sich selber ein Gerät zu bauen und dieses zertifizieren zu lassen. Deswegen würde ich an dieser Stelle sagen, der Fotograf soll, also eine Sollbestimmung, ein sicheres Gerät erwerben und betreiben, von dem dann abgespeichert wird, welches Produkt es war, aus dem dieses Bild erstellt wurde.

Vors. **Andrea Lindholz** (CDU/CSU): Okay, vielen Dank. Dann haben wir Herrn Ebelt.

SV **Friedemann Ulrich Ebelt** (Digitalcourage e.V., Bielefeld): Vielen Dank für die Fragen. Ich fange an mit der ersten Frage. Da geht es um die grundrechtliche Einschätzung und die Frage, ist denn die geplante Fingerabdruckpflicht verhältnismäßig? Von unserer Seite ist das ein ganz, ganz, ganz, ganz klares Nein! Es ist jetzt aber so, das ist ein weites Feld und mildere Mittel und Alternativen müssen ausführlich und systematisch geprüft werden. Das lässt sich nicht in fünf Minuten machen, auch nicht in fünf Tagen. Grundsätzlich geht es um die Frage, welche Ziele müssen erreicht werden oder sollen erreicht werden und was sind die mildesten Mittel, um diese Ziele zu erreichen? Aus unserer Sicht müsste der Gesetzgeber den Bürgerinnen und Bürgern ganz klar sagen können, aus welchem Grund jede Person zwei Fingerabdrücke abgeben soll, das heißt, um wie viele Menschen es jährlich geht, die im Schnitt ein, zwei Stunden vielleicht bei einer Grenzkontrolle für die Überprüfung ihrer Identität vielleicht nicht weiterreisen können. Das ist das einzige Konkrete, was wir aus der Kleinen Anfrage aus dem Bundestag, die in der Stellungnahme auch verlinkt ist, herausfinden konnten. Das ist das einzige Anwendungsszenario, das einzige konkrete Anwendungsszenario. Und wenn es das ist, ist die anlasslose generelle Fingerabdruckpflicht komplett unverhältnismäßig. Dann gibt es aber weitere Ziele und Dinge, die erreicht werden sollen, beispielsweise Terror wird genannt, auch in der zugrundeliegenden Verordnung. Hier sagt die Bundesregierung in der Kleinen Anfrage genau auf diese Frage – ich lese das mal vor, das ist Frage 14 –, Zitat: „Es sind keine konkreten Fälle von als terroristisch eingestuften Straftaten bekannt, in denen das Nichtvorhandensein gespeicherter Fingerabdrücke auf Personalausweisen sowie anderen Ausweisdokumenten mutmaßlich dazu geführt hätten, dass die Tat nicht verhindert beziehungsweise nicht aufgeklärt und die Täter ermittelt werden konnten.“ Also, es gab ja jetzt schon die eine Klimaanalogie. Also die Faktenlage ist aus unserer Sicht so dünn wie mittlerweile leider das Eis auf dem Weißen See im Winter, also quasi nicht vorhanden. Ja.

Zweiter Punkt: Die Identifizierung, das Ziel also, Personen identifizieren zu können. Im Grunde ist durch eine gute, solide Kontrollpraxis der konkrete Anwendungsfall so minimal, dass wir wirklich nur noch über seltene Einzelfälle sprechen. Und wir müssen ja auch immer schauen, also jetzt war von Dr. von Notz ein Fall im Raum pro Jahr.

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

SV **Friedemann Ulrich Ebelt** (Digitalcourage e.V., Bielefeld): Einstellig. Entschuldigung. Genau. Einstellig. Also sprich, wir wissen gar nicht, worüber wir zahlenmäßig überhaupt reden. Und unserer Ansicht nach können Beamt*innen, wenn sie im Verdacht Zweifel haben, die Identität prüfen. Vielleicht nicht innerhalb von fünf Minuten, aber es ist möglich. Überprüfung der Echtheit: Da sagen wir, es ist nicht notwendig, Fingerabdrücke in den Personalausweis aufzunehmen. Es gibt andere, bessere Sicherheitsmerkmale, die grundrechtsverträglich sind und privatsphärenfreundlich, haptische, optische. Und letztendlich ist auch die Verschlüsselung an sich mehr wert als die Daten dahinter, also dann die Daten des Fingerabdrucks. Das sind letztendlich auch nur Nullen und Einsen. Und, ja, im Zweifel lassen sich auch Fingerabdrücke fälschen, das ist auch soweit bekannt. Und dann, ja, das Hauptziel, oder das ist der Eindruck, den wir gewonnen haben nach der Lektüre dessen, was wir vorfinden konnten, ist die Haltung wohl: ja, es geht eigentlich ja nur darum, der zugrundeliegenden EU-Verordnung zu entsprechen. Das heißt, es muss gar nicht diskutiert werden. Es muss ja einfach nur ausgeführt werden, was da beschlossen wurde. Und da sagen wir: Natürlich ist eine Verordnung bindend, aber nur, solange sie grundrechtskonform ist. Und die Verordnung, das ist das eine und das ist das Wichtigste und das ist aus meiner Sicht die wichtigste Frage im Raum. Und der andere Punkt

ist, die Verordnung erlaubt andere Handlungsoptionen. Die Verordnung sagt nicht, jedes Land in der Europäischen Union braucht einen Personalausweis mit zwei Fingerabdrücken. Das sagt es überhaupt nicht. Sondern sie sagt eben auch, die Fingerabdruckpflicht und alle anderen Regelungen in der Verordnung gelten zum Beispiel nicht für Aufenthaltskarten, die allen im Hoheitsgebiet ansässigen Personen, unabhängig von ihrer Staatsbürgerschaft, ausgestellt werden. Das – habe ich eingangs schon erwähnt – wäre vielleicht auch ein deutlich diskriminierungsärmerer Weg, weil ich, wenn ich mit einem Duldungspapier, meinetwegen in einem Hostel einchecke, übermittle ich eine Information, die dafür überhaupt nicht notwendig ist. Insofern, aber ich möchte es nochmal betonen, also diese Grundrechtsabwägung muss deutlich systematischer und ausführlicher gemacht werden und am besten von einem Gericht, ja, so wie es aussieht.

Die zweite Frage betrifft den Unterschied zwischen dem Reisepass und dem Personalausweis. Wir sagen, da es die Fingerabdrücke im Reisepass schon gibt, und auch das ist grundrechtlich umstritten, da verweise ich in der Stellungnahme auf die Rechtssache Schwarz. Auch da gibt es sehr gute Argumente dagegen. Jedenfalls hat aber der Reisepass die Hauptfunktion des Reisens. Der Personalausweis ist ein gänzlich anderes Dokument, das ist ein Dokument des Alltags. Und die Hauptfunktionen und die Hauptanwendungsweise sind eben Hotels, Autovermietungen, ich reise in der Deutschen Bahn, ich habe einen Verkehrsunfall, ich gehe auf das Bürgeramt und so weiter und so fort. Für all diese Dinge brauche ich definitiv unter keinen Umständen einen Fingerabdruck. Das heißt, es ist einfach nicht notwendig. Außerdem sind wir der Meinung, dass jede Bürgerin und jeder Bürger in Deutschland, am besten jede Person, die in Deutschland lebt, ein ID-Dokument hat genau für diese Zwecke ohne Fingerabdruck. Das folgt dann einfach den Grundsätzen der Datenminimierung. Und was bedacht werden muss – und das ist ganz entscheidend –, einerseits langfristig zu denken. Wir reden einerseits über zehn Jahre, die so ein Dokument gültig ist und andererseits über Daten, die lebenslang verknüpft sind mit meiner Identität, mit meiner Person. Das heißt, es ist unmöglich, jetzt zu sagen, ob ein Chip in zehn Jahren noch sicher ist oder nicht. Also ich würde da auf keine Prognose viel wetten im Zweifelsfall. Grundsätzlich können oder gelangen die Daten früher oder später in Datenbanken. Sie gelangen auf Behörden in Backups, sie können bei Hackerangriffen gestohlen werden – wir wissen, wie mächtig Geheimdienste sind. Das ist eine sehr, sehr risikoreiche Wette und die Risiken übersteigen aus unserer Sicht komplett jeden Nutzen. Und wir hatten erst im September ein Hack. Da wurden 12.000 sensible Passdaten von Deutschen aus der Argentinischen Einwanderungsbehörde entwendet. Da waren noch keine biometrischen Daten dabei, soweit ich das weiß, aber das Szenario ist natürlich denkbar.

Langfristigkeit ist das eine, was beachtet werden muss. Das andere ist, das zusammenhängend zu betrachten. Die Speicherung von Fingerabdrücken in Personalausweisen, das ist nicht das einzige Sicherheitsgesetz und das ist nicht das einzige personenbezogene Datum, was mich identifizierbar, bewertbar und im Zweifel auch verfolgbar und auffindbar macht, sondern es gibt eine ganze Reihe, das heißt, was wir einfordern, wäre eine Überwachung des Gesamtrechners, die Gesamtschau aller meiner oder aller biometrischen Daten über mich, auch in einer langfristigen Betrachtung. Also, wir schauen halt immer nur punktuell Regelungen an. Selbst wenn sie im Einzelfall dann doch verhältnismäßig sein sollten, sind sie es, im Ganzen betrachtet, in ihrer Vernetzung, in ihrer Tragweite dann eben definitiv nicht mehr. Das heißt, wir brauchen eine Inventur und insofern haben wir uns auch sehr gefreut über die Forderung des Bundesdatenschutzbeauftragten, ein Sicherheitsgesetzmoratorium einzulegen, um überhaupt erst mal einen Sachstand oder eine Inventur aufzuarbeiten.

Die dritte Frage zum Thema „Ein oder mehrere Anbieter?“ mache ich ganz kurz, weil es tatsächlich kein Gegenstand meiner Stellungnahme ist. Deswegen nur ein Satz: Grundrechte und IT-Sicherheit brauchen keine Monopole. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann kommen wir als nächstes zu Herrn Dr. Hofschen.

SV **Dr. Stefan Hofschen** (Bundesdruckerei GmbH, Berlin): Ich hatte die Frage von Herrn Oster zum Service. Wir beschäftigen ungefähr 200 Mitarbeiter im Service. Das sind sowohl Techniker als auch Mitarbeiter im Callcenter. Die Anforderung ist, dass Anrufe von Behörden normalerweise innerhalb von 30 Sekunden entgegengenommen werden müssen und dem Mitarbeiter in der Behörde vor Ort, der in

dem Moment wahrscheinlich aufgrund eines akuten Problems tatsächlich nicht mehr arbeiten kann, entweder telefonisch oder, wenn möglich, remote, zu helfen. Sollte sich dabei herausstellen, dass irgendein Gerät defekt ist, dann gibt es eine entsprechende dezentralisierte Serviceflotte mit Ersatzgeräten, um diese Geräte dann schnellstmöglich vor Ort zu tauschen und zu ersetzen, so dass die Funktionsfähigkeit wieder hergestellt ist. Es stehen eine Menge von Behauptungen im Raum, die ich jetzt leider nicht alle erwidern kann. Aber zumindest in diesem Punkt kann ich sagen: Es geht hier nicht bloß um 1.400 Geräte oder Behörden, sondern es geht um alle 6.115 Meldeämter, die es in Deutschland gibt beziehungsweise Örtlichkeiten, in denen Meldeämter untergebracht sind. Es geht um über 25.000 oder – wenn man alle zusammen nimmt – über 50.000 physikalische Geräte, die dieser Service auch heute schon austauschen, ersetzen, warten, pflegen muss.

Und noch ein letzter Punkt, der vorkommen kann, ist der Austausch von Geräten und Gerätegenerationen, wie z.B. 2019 geschehen. Mit der Verabschiedung einer neuen technischen Richtlinie wurde es erforderlich, gewisse Geräte, die schon eine ganze Zeit im Feld waren, auszutauschen. Auch dies wird vom Service gewährleistet und sichergestellt, dass innerhalb einer relativ kurzen Zeitspanne wirklich alle Geräte in allen Behörden auf den neuesten Stand gebracht werden. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Und Herr Dr. Weichert bitte noch.

SV **Dr. Thilo Weichert** (Netzwerk Datenschutzexpertise GbR, Kiel): Zur Gefahr der zweckwidrigen Nutzung der Fingerabdrücke: Wenn die Fingerabdrücke zum Beispiel an den Grenzen und von der Polizei erfasst werden sollen als Fallback-Strategie, so wie es Herr Busch dargestellt hat, dann ist es notwendig, dass man Fast-ID-Geräte installiert. Wenn solche Fast-ID-Geräte mal vorhanden sind, dann werden sie auch gebraucht. Das heißt, aus dem Fallback wird sehr, sehr schnell ein Standard und man wird sich immer mehr nicht mehr auf das Lichtbild oder auf irgendwelche visuellen Abgleiche verlassen, sondern man wird dann auf diese ID-Sicherung per Fingerabdruck zurückgreifen. Und das hat dann zwangsläufig zur Folge, dass diese Daten massenhaft erfasst werden. Das ist unsere Erfahrung. Wenn mal eine Technologie da ist, dann wird sie auch tatsächlich genutzt. Und dann wird ein Abgleich vorgenommen. Dann ist es im Prinzip nur noch eine Frage der Datensicherheit, ob diese Daten zum Beispiel in den Abgleich mit irgendwelchen anderen Dateien gebracht werden oder ob sie abgespeichert werden. Das heißt, ich sehe in der Installierung dieses Fingerabdrucks im Personalausweis sozusagen das erste Mosaikstück einer weitergehenden Erfassung von Fingerabdrücken, die letztendlich dazu führt, dass der Fingerabdruck wirklich zur nationalen Kennziffer wird, von dem ich ja schon gesprochen habe mit der weiteren Folge, dass dann ein hohes Fälschungsrisiko, ein hohes Missbrauchsrisiko und insbesondere ein hohes Zweckveränderungsrisiko besteht. Aus diesem Grund ist es absolut wichtig, dass wir also von vornherein die Erforderlichkeitsprüfung durchführen. Und zu dieser Erforderlichkeitsprüfung – ist der Fingerabdruck auf dem Ausweis tatsächlich notwendig? – habe ich nichts gefunden. Ich kenne die Angabe, dass eine einstellige Zahl von Missbrauch aufgedeckt werden müsste, nicht, aber ich habe auch keine andere wissenschaftliche Untersuchung gefunden, die wirklich belegt, dass es erforderlich ist, dass Fingerabdrücke auf dem Ausweis notwendig sind, um eine Identität in einem Massenverfahren – und die Nutzung von Personalausweisen ist ein Massenverfahren – um diese zu rechtfertigen. Wir müssen davon ausgehen, dass diese Personalausweise nicht nur von 80 Millionen Deutschen, sondern von 300 Millionen EU-Bürgern erstellt werden und dass die Fingerabdrücke, wenn wir dieses Fast-ID-Verfahren haben, das zum Beispiel im Ausländerbereich schon genutzt wird, und wenn das bei der Polizei etabliert wird, dass dann der Fingerabdruck nicht nur bei Apple oder bei irgendwelchen privaten Anbietern, sondern dass das die Standardmaßnahme in der Meldebehörde, bei der Polizei oder anderswo gespeichert wird. Und dann müssen wir auf das Missbrauchsrisiko hinweisen. Ich weiß nicht, ob Sie Babylon Berlin gesehen haben, die letzte Staffel? Da ist schon in den 30er Jahren mit dem Fingerabdruck Schindluder getrieben worden. Und genau die gleiche Maßnahme, die man damals schon genutzt hat, lässt sich heute eben beim Fingerabdruck auch nutzen, Das heißt also, das Missbrauchsrisiko ist sehr, sehr, sehr groß.

Vielleicht noch zu einem Argument von Herrn Busch, das er in seinem Eingangsstatement gebracht hat. Die ICAO hat keine Festlegung auf irgendeinen Finger gemacht, zumindest ist es mir

nicht bekannt. Die ICAO ist auch kein Gesetzgeber. Es wäre problemlos möglich, aufgrund nationaler Gesetzgebung in Deutschland zu sagen, der neue Standard ist der kleine Finger oder von mir aus auch der Ringfinger. Der Ringfinger wird erheblich weniger genutzt als irgendwelche anderen Finger, insbesondere Zeigefinger und Daumen. Der Ringfinger hat mindestens die Breite, ja, meiner ist sogar größer als der Zeigefinger. Im Prinzip wird sich die Qualität der Minutien bestimmt nicht unterscheiden.

Vors. **Andrea Lindholz** (CDU/CSU): Die Frage war allerdings in dem Zusammenhang, Herr Dr. Weichert, wenn ansonsten überall in Europa ein anderer Finger genutzt wird, eben nicht der kleine, sondern der Zeigefinger, ob das eben ein Problem darstellen könnte. Das war der Punkt.

SV **Dr. Thilo Weichert** (Netzwerk Datenschutzexpertise GbR, Kiel): Standards kann man ändern und verfassungskonforme Standards ändern sich manchmal schneller, wenn der Europäische Gerichtshof sagt: Das ist nicht erforderlich mit dem Zeigefinger, weil Datensparsamkeit ein Grundsatz ist, der im Artikel 8 Europäische Grundrechtecharta vorgesehen ist.

Vors. **Andrea Lindholz** (CDU/CSU): Die Frage war nach der praktischen Gleichheit. Ich hatte das so verstanden, ob das praktischer ist, wenn alle das Gleiche benutzen innerhalb Europas und nicht unterschiedlich. Das ist die Frage.

SV **Dr. Thilo Weichert** (Netzwerk Datenschutzexpertise GbR, Kiel): Das wäre es sicher. Und praktisch ist es, den kleinen Finger dann gemeinsam zu benutzen, und dann möglichst auch nur einen und nicht gleich zwei.

Vors. **Andrea Lindholz** (CDU/CSU): Also Sie sagen, im Prinzip ist es egal. Wenn alle unterschiedliche Finger benutzen würden, wäre das auch unschädlich?

SV **Dr. Thilo Weichert** (Netzwerk Datenschutzexpertise GbR, Kiel): Genau.

SV **Roland Appel** (Roa.Consult, Bornheim): Nein, die werden ja nicht zentral gespeichert, sondern es dient ja nur der 1:1 Verifizierung: Ist der Betreffende Ausweisinhaber der Richtige, sein Fingerprint identisch mit dem gespeicherten? Und insofern ist es eigentlich egal.

Vors. **Andrea Lindholz** (CDU/CSU): Das ist egal. Das war ja vorher das Argument. Es macht nur Sinn, wenn alle den gleichen Finger benutzen. Wenn Sie sagen, das ist eigentlich egal, jeder kann das nehmen, was er will, das reicht, dann ist das auch eine Aussage. Vielen Dank für alle Teilnehmer der Anhörung heute.

SV **Roland Appel** (Roa.Consult, Bornheim): Darf ich, Frau Vorsitzende? Ich hatte eine Frage unterschlagen, will ich aber jetzt nichts dazu sagen, sondern verweisen, nämlich nach den Auswirkungen für die Kommunen. Das können Sie der Stellungnahme vom Deutschen Industrie- und Handelskammertag, Deutscher Landkreistag- und Städtetag vom 2. Oktober entnehmen. Diese haben dargelegt, dass Millionen Ausfälle durch die Änderungen kämen. Das liegt schriftlich vor.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank nochmal für die Ergänzung, Herr Appel. Dann darf ich mich bei allen bedanken und wünsche noch eine gute restliche Woche.

Schluss der Sitzung: 12:00 Uhr

Andrea Lindholz, MdB
Vorsitzende

Netzwerk Datenschutzexpertise GbR
Dr. Thilo Weichert
Waisenhofstr. 41
D-24103 Kiel
Tel.: +49 431 9719742
E-Mail: weichert@netzwerk-datenschutzexpertise.de

DR. THILO WEICHERT, WAISENHOFSTR. 41, 24103 KIEL

An den
Deutschen Bundestag
Ausschuss für Inneres und Heimat
Vorsitzende Frau MdB Andrea Lindholz
Platz der Republik 1
11011 Berlin

Kiel, den 12.10.2020

Stellungnahme des Netzwerks Datenschutzexpertise

zum Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen
BT-Drs. 19/21986 v. 31.08.2020 = BR-Drs. 435/20 v. 07.08.2020, BT-Drs. 19/22783 v. 23.09.2020

Sehr geehrte Frau Vorsitzende,
sehr geehrte Damen und Herren Abgeordnete,

unten stehend finden Sie die Stellungnahme des Netzwerks Datenschutzexpertise zu dem im Betreff genannten Gesetzentwurf. Darin sind zentrale Regelungen zur Verarbeitung von biometrischen Daten zum Zweck der Identifizierung enthalten, namentlich von Lichtbildern und Fingerabdrücken. Mit der gesetzlichen Regelungen soll insofern eine fälschungsfeindliche zentrale Identifizierungsinfrastruktur aufgebaut werden. Hiergegen ist grundsätzlich nichts einzuwenden. Mit der verpflichtenden Aufnahme von Fingerabdrücken in den Personalausweis und der Möglichkeit der Vornahme von Datenabgleichen zwischen biometrischen Datenbanken der Sicherheitsbehörden und den in den Ausweisen gespeicherten Daten wird aber zugleich stark in das Grundrecht der Menschen auf Datenschutz eingegriffen. Solche Regelungen müssen verhältnismäßig sein, um zu vermeiden, dass eine unangemessene Überwachungsinfrastruktur aufgebaut wird und um sicherzustellen, dass die Regelungen einer **verfassungsrechtlichen Prüfung** standhalten. Das Netzwerk Datenschutzexpertise bezweifelt, dass diesen Anforderungen genügt wird.

Wir wären Ihnen dankbar, wenn Sie die vorliegende Stellungnahme den Mitgliedern des federführenden Ausschusses wie auch der mitberatenden Ausschüsse zur Verfügung stellen würden in der Hoffnung, dass diese **bei den weiteren Beratungen Berücksichtigung** findet.

Diese Hoffnung ist angesichts der Terminplanung zu diesem Gesetzentwurf mit der Besorgnis verbunden, dass dieser Gesetzentwurf ohne ausreichende **öffentliche Debatte** und Beratung im Schnelldurchgang beschlossen werden soll.

A. Allgemeine Einordnung des Gesetzesvorschlags

Der Gesetzentwurf verfolgt die Zielrichtung, die Verfügbarkeit und Zuverlässigkeit staatlicher Identifizierungsmittel durch eine Bereitstellung von authentischen Gesichtsbildern und Fingerabdrücken zu verbessern. Dem dient die Verhinderung des sog. „Morphing“, also der Verfälschung von Gesichtsbildern zum Zweck der Identitätstäuschung und die Bereitstellung von automatisiert abgleichbaren Lichtbildern. Dem dient auch die verpflichtende Aufnahme der Fingerabdrücke der Zeigefinger in Personaldokumenten, also insbesondere in Personalausweisen, so wie dies bisher schon bei Reisepässen vorgesehen ist.

Die verpflichtende Aufnahme von authentifizierten Fingerabdrücken und Lichtbildern dient der Umsetzung der EU-Verordnung v. 20.06.2019 zur Erhöhung der Personaldokumente für in der Europäischen Union (EU) freizügigkeitsberechtigten Personen, der **VO (EU) Nr. 2019/1157**, wo es in Art. 3 Abs. 5 S. 1 heißt:

Die Personalausweise werden mit eine hochsicheren Speichermedium versehen, das ein Gesichtsbild des Personalausweiseinhabers und zwei Fingerabdrücke in interoperablen digitalen Formaten enthält.

I. Biometrische Identifizierung

Bei automatisiert auslesbaren Gesichtsbildern und Fingerabdrücken handelt es sich um „**biometrische Daten zur eindeutigen Identifizierung**“, die in Art. 4 Nr. 14 europäische Datenschutz-Grundverordnung (DSGVO)[1] und Art. 3 Nr. 13 europäische Datenschutzrichtlinie für Polizei und Justiz (DSRl-JI)[2] spezifisch definiert sind. Es handelt sich dabei um Daten, die gemäß Art. 9 Abs. 1 DSGVO und Art. 10 DSRl-JI einer „besonderen Kategorie personenbezogener Daten“ zugeordnet sind und die wegen ihrer Sensitivität unter einem besonderen Schutz stehen.

Diese biometrischen Daten sind **personenbezogene Daten** (Art. 4 Nr. 1 DSGVO, Art. 3 Nr. 1 DSRl-JI), die vom deutschen Verfassungsrecht über das Recht auf informationelle Selbstbestimmung[3] und vom europäischem Recht durch das Grundrecht auf Datenschutz nach Art. 8 GRCh geschützt sind.

Der Grund für den besonderen rechtlichen Schutz biometrischer Identifizierungsdaten liegt darin, dass mit diesen eine **Schnittstelle zwischen realer und digitaler Welt** hergestellt werden kann. Diese weitgehend unveränderlichen persönlichen Merkmale eignen sich als Identifikatoren, mit denen Daten aus unterschiedlichen Kontexten zu einer Person zusammengeführt werden können, woraus sich besondere Datenschutzrisiken ergeben. Es besteht insbesondere das Risiko einer zweckwidrigen Weiterverwendung von Daten und deren Zusammenführung in Persönlichkeitsprofilen.[4]

Sie eignen sich als **nationale Kennziffern**, also als persönliche Zuordnungsmerkmale, da die biometrischen Merkmale einheitlich in einem Staat, ja staatenübergreifend weltweit umfassend verwendet werden können.[5] Erfolgt eine solche staatliche umfassende Nutzung, so bedarf es hierfür gemäß Art. 87 S. 2 DSGVO „geeigneter Garantien für die Rechte und Freiheiten“ der Betroffenen. Dies gilt insbesondere, wenn als Kennziffer biometrische Merkmale zum Einsatz kommen (Art. 9 Abs. 2 lit. g DSGVO, Art. 10 DSRl-JI). Solche Garantien können in Beschränkungen der Nutzungsberechtigten, der Zwecke, der Art der

[1] VO (EU) 2016/679 v. 27.04.2016, ABl. L 119/1.
[2] RL (EU) 2016/680 v. 27.04.2016, ABl. L 119/89.
[3] BVerfG U.v. 15.12.1983 – 1 BvR 209/83 u.a., NJW 1984, 419
[4] Wedde in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 9 Rn. 30.
[5] Wedde in Däubler u.a. (Fn. 4), Art. 87 Rn. 8 ff.

Datenverarbeitung, in besonderen Betroffenenrechten, etwa in Bezug auf die Transparenz der Verarbeitung, sowie in technischen Vorkehrungen liegen.[6]

Tatsächlich werden die automatisiert auslesbaren **Lichtbilder und Fingerabdrücke** als solche nationalen Identifikatoren verwendet, wenn sie auf einem Ausweisdokument gespeichert werden, das für unterschiedliche Zwecke und durch unterschiedliche Stellen, insbesondere Behörden, also universell, genutzt werden. Das Personalausweisgesetz (PAuswG) regelt die Pflicht zum Mitführen des Ausweises und dessen Vorlage bei unterschiedlichen Behörden und sonstigen Stellen:

§ 1 Abs. 1 S. 1 PAuswG: *Deutsche im Sinne des Artikels 116 Abs. 1 des Grundgesetzes sind verpflichtet, einen gültigen Ausweis zu besitzen, sobald sie 16 Jahre alt sind und der allgemeinen Meldepflicht unterliegen oder, ohne ihr zu unterliegen, sich überwiegend in Deutschland aufhalten. Sie müssen ihn auf Verlangen einer zur Feststellung der Identität berechtigten Behörde vorlegen und es ihr ermöglichen, ihr Gesicht mit dem Lichtbild des Ausweises abzugleichen.*

Bzgl. der Ein- und Ausreise ins bzw. aus dem Bundesgebiet besteht in § 1 Abs. 1 PassG eine entsprechende Ausweispflicht durch Vorlage eines Passes. Die EU-Mitgliedstaaten stellen auf Basis der Verordnung (EG) 2252/2004 des Rates vom 13.12.2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten **Pässen und Reisedokumenten**, geändert durch Verordnung (EG) 444/2009 vom 28.05.2009, reguläre Reisepässe mit Chip aus, welche das Lichtbild und zwei Fingerabdrücke enthalten. Deutschland hat den elektronischen Reisepass zum 1. November 2005 und die Speicherung von Fingerabdrücken in Pässen zum 1. November 2007 eingeführt.[7]

Das Lichtbild und Fingerabdrücke werden nicht im Melderegister gespeichert, sondern im Pass (§ 4 Abs. 1 S. 1 PassG) wie im Personalausweis (§ 5 Abs. 2 Nr. 5 PAuswG), die Lichtbilder auch im **Passregister** (§ 21 Abs. 2 PassG) und im **Personalausweisregister** (§ 23 Abs. 3 PAuswG).

Die im Chip gespeicherten biometrischen Daten sind nur mit einem hoheitlichen Berechtigungszertifikat **auslesbar**, welches an explizit berechtigte Stellen ausgegeben wird. Die Daten sind durch kryptographische Maßnahmen (Extended Access Control) entsprechend den Vorgaben in der Technischen Richtlinie TR-03110 „Advanced Security Mechanisms for Machine Readable Travel Documents“ gegen unberechtigten Zugriff geschützt.[8] Gemäß Art. 11 Abs. 5 VO (EU) 2019/1157 dürfen maschinenlesbare Informationen nur gemäß dieser Verordnung oder dem nationalen Recht des ausstellenden Mitgliedsstaats aufgenommen werden. Erlaubt sind gemäß Art. 11 Abs. 6 VO (EU) 2019/1157 nur die Echtheitsprüfung des Dokuments und die Identitätsprüfung.

Eine Speicherung der Fingerabdrücke findet gemäß den Angaben der Bundesregierung in **Datenbanken** nicht statt.[9]

Der Zugriff auf das **Pass- und das Personalausweisregister** ist in den §§ 22 ff. PassG und den §§ 24 ff. PAuswG geregelt. Gemäß § 22a Abs. 2 S. 1-5 PassG u. § 25 Abs. 2 S. 1-4 PAuswG haben die Berechtigung für den automatisierten Abruf des Lichtbildes Behörden zur Verfolgung von Verkehrsordnungswidrigkeiten sowie generell zur Aufgabenerfüllung: „die Polizeibehörden des Bundes und der Länder, der Militärische Abschirmdienst, der

[6] Wedde in Däubler u.a. (Fn. 4), Art. 87 Rn. 15-18.
[7] BT-Drs. 19/22133, S. 12 f.
[8] BT-Drs. 19/22133, S. 6.
[9] BT-Drs. 19/22133, S. 6.

Bundesnachrichtendienst, die Verfassungsschutzbehörden des Bundes und der Länder, Steuerfahndungsdienststellen der Länder, der Zollfahndungsdienst und die Hauptzollämter“.

In den Jahren 2017/2018 wurde vom Bundesinnenministerium auf dem Bahnhof Berlin-Südkreuz ein Feldversuch zur automatisierten **Gesichtserkennung im öffentlichen Bereich** durchgeführt, der auf starke, auch rechtlich begründete öffentliche Kritik stieß.[10]

II. Gesichtsbilder

Die datenschutzrechtliche **Problematik der Verarbeitung von Gesichtsbildern**, die mit Lichtbildern erfasst werden, besteht darin, dass diese jederzeit ohne Beteiligung der Betroffenen aus der Ferne erstellt werden können und dass diese oft mit einer Zuordnungsmöglichkeit zu weiteren Identifizierungsdaten (Name, Adresse, Erreichbarkeitsdaten, sonstige Angaben und Merkmale) im Internet verfügbar sind. So hat z.B. die in den USA ansässige Fa, Clearview AI aus dem Internet verfügbare Informationen zum Aufbau einer weltweiten Gesichtsbilddatenbank mit angeblich 3 Mrd. Bildern erfasst, die sowohl privaten wie auch öffentlichen Stellen zur Nutzung zur Verfügung gestellt wird.[11] Ein vergleichbares Angebot mit 900 Mio. biometrisch analysierten Gesichtern wird als öffentlich nutzbare Suchmaschine von dem polnischen Unternehmen PinEyes betrieben.[12]

Im zentralen polizeilichen Informationssystem (INPOL), das vom Bundeskriminalamt (BKA) geführt wird, sind über 5,8 Millionen Lichtbilder von ca. 3,6 Millionen Personen und ca. 3,5 Millionen Personenbeschreibungen aus erkennungsdienstlichen Behandlungen gespeichert (Stand März 2020). Durch den direkten Zugriff auf INPOL stehen diese Lichtbilder sowie die Personenbeschreibungen allen deutschen Polizeidienststellen sofort und aktuell zur Verfügung. Mit dem seit 2008 im BKA betriebenen **Gesichtserkennungssystem** (GES) können einzelne Lichtbilder mit dem Lichtbild-Gesamtbestand abgeglichen werden. Das GES trifft automatisiert eine Vorauswahl aus dem Gesamtbestand. Die Treffer werden anschließend von Lichtbildexperten und -sachverständigen ausgewertet werden. Im Jahr 2019 wurden bundesweit bei ca. 54.000 Recherchen im GES über 2.100 Personen identifiziert.[13]

Die bisherige zweidimensionale Gesichtserkennung wird durch eine Weiterentwicklung der Mustererkennungsmethoden durch **dreidimensionale Techniken** ergänzt. Mit diesem multi-biometrischen System besteht die Möglichkeit, Identifizierungen auch aus partiellen Gesichtsbildaufnahmen mit minderer Bildqualität vorzunehmen.[14]

Die Verfügbarkeit von mit staatlich qualitätsgesicherten automatisiert lesbaren Lichtbildern aus Pässen und Personalausweisen mit auf dem Markt verfügbaren Zuordnungsdatenbanken oder dem GES des BKA erhöht das Risiko, dass Menschen anhand ihres Gesichts identifiziert werden, ohne dass die Betroffenen hiervon Kenntnis

[10] Dachwitz, Überwachungstest am Südkreuz: Geschönte Ergebnisse und vage Zukunftspläne, netzpolitik,org 16.10.2018.
[11] Clearview betreibt weltweite Gesichtsdatenbank mit Abgleichsangebot, DANA 1/2020, 68 f.; Nutzung von Clearviews Gesichtsdatenbank durch Private und Behörden, DANA 2/2020, 125 f.
[12] Laufer/Meineck, Eine polnische Firma schafft gerade unsere Anonymität ab, www.netzpolitik.org 10.07.2020.
[13] Bundeskriminalamt (BKA), https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Erkennungsdienst/erkennungsdienst_node.html;jsessionid=E702B9AF17BA335BBDAB6BF326F5F6DF.live2301#doc19616bodyText4.
[14] Multi-Biometrische Gesichtserkennung (GES-3D), Monroy, Gesichtserkennung: BKA will auf verbessertes System umstellen, netzpolitk.org 31.01.2018; Mehr Gesichtserkennung beim BKA, Bürgerrechte&Polizei/CILIP 115 (April 2018), S. 93; zum Datenschutz Körffer/Opel/Nouak, DuD 2013, 347 ff.

erlangen. Diesem Risiko muss mit Hilfe von **geeigneten Garantien** entgegengewirkt werden (Art. 10 DSRl-JI).

III. Fingerabdrücke

Die in Personalausweisen und Reisepässen gespeicherten **Fingerabdrücke** dienen der schnellen Identitätsfeststellung, wenn Zweifel an der Übereinstimmung der sich ausweisenden mit der auf dem Lichtbild des Dokuments abgebildeten Person bleiben.[15] Bisher war die Aufnahme von Fingerabdrücken im Personalausweis freiwillig (§ 9 Abs. 3 S. 1-4 PAuswG). Im Reisepass ist die Aufnahme von zwei Fingerbadrücken nach § 4 Ab. 3 S. 1 PassG obligatorisch (basierend auf Art. 1 Abs. 2 VO (EG) Nr. 2252/2004). Mit der Neuregelung soll nun auch eine Verpflichtung zur Aufnahme von zwei Fingerabdrücken im Personalausweis geregelt werden.

Anders als Gesichtsbilder sind Fingerabdrücke nicht so leicht zu erlangen. Um auf einfache Weise qualitativ hochwertige Fingerabdrücke zu erhalten, bedarf es einer gewissen Kooperation des Betroffenen. Fingerabdrücke lassen sich aber auch mit höherem Aufwand und ohne Beteiligung der Betroffenen erheben, z.B. indem angefasste Objekte (Gläser, Türklinken) auf Fingerabdruckspuren hin ausgewertet werden. Da solche **Spuren fast überall im täglichen Leben** eines Menschen anfallen, ist ein Erlangen von Fingerabdrücken und deren Zuordnung zu einer Person ohne deren Wissen möglich.

Die Erfassung von Fingerabdrücken hat eine lange Tradition in der polizeilichen Praxis zwecks Zuordnung von Tatortspuren.[16] Inzwischen wird das Erfassen und Abgleichen als Identifizierungsmethode auch von anderen Behörden und von privaten Stellen genutzt. Anders als die Gesichtserkennung, bei der die Zuordnungsqualität von der Bildperspektive, der Beleuchtung und dem Fehlen von störenden Einflüssen (Haare, Brille, Gesichtsbedeckung) abhängt, kann wegen der Einzigartigkeit der Fingerabdrücke allein mit einem Fingerabdruck in der Regel eine **sichere Zuordnung** vorgenommen werden.[17]

Das BKA führt seit 1951 eine zentrale Fingerabdrucksammlung. 1993 wurde ein automatisiertes **Fingerabdruck-Identifizierungs-System** (AFIS), eingeführt, das auf der Codierung der anatomischen Merkmale (Minutien) basiert.[18] Die Einführung der „Livescan"-Technologie im Jahr 2004 ermöglicht es, die Fingerabdrücke (ebenso wie die der Handflächen) digital aufzunehmen und im zentralen AFIS des BKA zu speichern. Im Rahmen des sog. Fast-ID-Verfahrens können seit 2006 digital aufgenommene Fingerabdrücke ohne Zeitverzug im AFIS recherchiert werden. So sind z.B. im polizeilichen Streifendienst, bei Großveranstaltungen (Fußballspiele, Konzerte etc.) und bei Grenzkontrollen rund um die Uhr innerhalb von wenigen Augenblicken zuverlässige, biometrisch basierte Personenidentifizierungen möglich. Das BKA verarbeitet monatlich ca. 60.000 eingehende digitale Fingerabdruckblätter, die gespeichert, ausgewertet und qualitätsüberprüft werden. Dabei wurden 2019 monatlich rund 19.300 Identifizierungen auf Basis des Abgleichs von Fingerabdrücken erzielt. Bei Fast-ID ist das Vorgangsaufkommen bisher ähnlich hoch: Auch hier führt ca. ein Drittel der Anfragen zu einem Treffer im Bestand. Zudem wurden im Jahr 2019 monatlich ca. 30.000 Tatortspuren recherchiert, die im AFIS gespeichert sind, was im Durchschnitt zu ca. 2.200 Treffern führte.[19]

[15] BT-Drs. 19/22133, S. 10.
[16] Weichert, CR 1997, 369 ff.
[17] Generell zur Zuordnungswahrscheinlichkeit Weichert in Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 4 Nr. 14 Rn. 7 f.; Gundermann/Probest in Roßnagel, Handbuch Datenschutzrecht, 2003, S. 1972 ff.
[18] Weichert, DuD 1999, 167.
[19] BKA (Fn. 12).

Derzeit errichten die Firmen IDEMIA und Sopra Steria für die EU ein biometrischen Erkennungssystem, wozu Fingerabdrücke und Gesichtsbilder aus fünf nationalen Datenbanken in einer Datei zusammengeführt werden und damit eine **europaweite Interoperabilität biometrischer Datenbanken** erreicht werden soll.[20]

B. Stellungnahme zur geplanten Regelung

I. Europarechtliche Grundlage: Verordnung (EU) Nr. 2019/1157

Gemäß Art. 11 des Gesetzentwurfes ist eine Änderung des **§ 5 Abs. 9 PAuswG** vorgesehen, wonach der folgende S. 1 eingeführt wird und in § 9 Abs. 3 die Sätze 4-7 (bisheriges Verfahren der freiwilligen Speicherung) gestrichen werden:

Die aufgrund der Verordnung (EU) Nr. 2019/1157 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben (ABl. L 188 vom 12.7.2019, S. 67), auf dem elektronischen Speichermedium zu speichernden zwei Fingerabdrücke der antragstellenden Person werden in Form des flachen Abdrucks des linken und rechten Zeigefingers im elektronischen Speicher- und Verarbeitungsmedium des Personalausweises gespeichert.

Zunächst stellt sich die Frage, ob die europarechtliche Grundlage dieser Regelung grundrechtskonform ist. Art. 3 Abs. 5 VO (EU) 2019/1157 verpflichtet zur **Erfassung von zwei Fingerabdrücken**. Diese Regelung muss gemäß Art. 52 Abs. 1 S. 2 GRCh dem Grundsatz der Verhältnismäßigkeit entsprechen. Sie muss für die Zielerreichung geeignet, erforderlich und angemessen sein. Eine Erforderlichkeit der Speicherung von zwei Fingerabdrücken ist nicht dargetan. Vielmehr wird in Erwägungsgrund 18 der Verordnung apodiktisch behauptet:

Die Speicherung eines Gesichtsbilds und zweier Fingerabdrücke (im Folgenden „biometrische Daten“) auf Personalausweisen und Aufenthaltskarten, die in Bezug auf biometrische Pässe und Aufenthaltstitel für Drittstaatsangehörige bereits vorgesehen ist, stellt eine geeignete Kombination einer zuverlässigen Identifizierung und Echtheitsprüfung im Hinblick auf eine Verringerung des Betrugsrisikos dar, um die Sicherheit von Personalausweisen und Aufenthaltskarten zu verbessern.

Die Bundesregierung hatte wegen der verpflichtenden Fingerabdruckspeicherung im Gesetzgebungsverfahren zunächst einen Prüfvorbehalt geltend gemacht. Als Argument für die **Erforderlichkeit** trägt sie nun – unter Aufgabe des Vorbehalts – Folgendes vor.

Die Speicherung des Fingerabdruckes in Identitätsdokumenten dient dem Zweck, bei Zweifeln an der Übereinstimmung der sich ausweisenden mit der auf dem Lichtbild des Dokuments abgebildeten Person die Identität dennoch unmittelbar feststellen zu können. Die derzeit in Zweifelsfällen noch teilweise notwendigen und zeitaufwändigen Nachfragen bei anderen Behörden können damit künftig entfallen.[21]

Dass derartige Zweifel an der Identität entstanden sind und wie oft dies der Fall war, nicht mitgeteilt. Es bestehen Zweifel daran, dass die behauptete Erforderlichkeit besteht. In jedem Fall würde der **Abdruck eines Fingers** genügen, um in den wohl wenigen Fällen eines Identitätszweifels eine Ausräumung des Zweifels zu ermöglichen. Durch die Speicherung nur

[20] Monroy, EU zahlt 300 Millionen Euro für Erkennung von Gesichtern und Fingerabdrücken, netzpolitik.org 05.06.2020.
[21] BT-Drs. 19/22133, S. 5 f.

eines Fingerabdrucks würde die Eingriffsintensität reduziert, da das mit zwei Abdrücken bestehende Missbrauchsrisiko angesichts der Verdoppelung der Zahl der potenziellen Abgleichsfingerabdrücke höher ist.

Es fehlt auch an der **Angemessenheit** der Verordnungsvorgabe: Angesichts einer geringen Zahl von Fällen, bei denen mit Hilfe des Fingerabdrucks eine schnelle Beseitigung von Identitätszweifeln möglich ist, kann nicht die Verpflichtung für über 300 Mio. EU-Bürgern ausgesprochen werden, zwei sensitive digital erfasste Fingerabdrücke auf dem Ausweis speichern zu lassen.

II. Nationale Gesetzgebung

Bei der Umsetzung der europäischen Vorgabe im vorliegenden Entwurf wird zudem der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) und damit der Erforderlichkeitsgrundsatz missachtet: Die in § 5 Abs. 9 PAuswG vorgesehene Speicherung der **Fingerabdrücke der Zeigefinger** betrifft für jede Hand diejenigen Finger, mit denen am meisten Spuren hinterlassen werden. Statt Fingerabdrücke des Zeigefingers zu verwenden, wären solche des Ringfingers und des kleinen Fingers weniger missbrauchsanfällig, für Identifizierungszwecke aber ebenso geeignet. Wegen des Fehlens europarechtlicher Vorgaben hätte der Gesetzgeber den Spielraum gehabt, insofern eine weniger eingreifende Maßnahme vorzusehen.

Folgende Sicherungsmaßnahmen sind vorgesehen: Ein technischer Ausleseschutz mit einer beschränkten Berechtigungsvergabe sowie die Beschränkung der Zwecke auf die Echtheits- und Identitätskontrolle sowie der Ausschluss einer zentralen Speicherung der ausgelesenen Daten (Erwägungsgrund 21 VO (EU) 2019/1157). Tatsächlich ist die europarechtlich in Art. 11 Abs. 6 der Verordnung vorgegebene **strenge Zweckbeschränkung** bei der nationalen Umsetzung nicht im vorliegenden Entwurf übernommen werden, obwohl hierzu eine Regelungsbefugnis erteilt wird. Vielmehr enthält § 15 PAuswG für Sicherheitsbehörden eine generelle automatisierte Abruf- und Speicherbefugnis „im Rahmen ihrer Aufgaben und Befugnisse“. Eine spezielle Beschränkung hinsichtlich der im Ausweis gespeicherten Fingerabdrücke ist nicht vorgesehen.

National ausgeschlossen ist lediglich die Abspeicherung der für Identifizierungszwecke abgeglichenen Fingerabdruckdaten in § 15 Abs. 2 PAuswG. Die automatisierte Speicherung der Ausweisdaten in einer Datei wird hierdurch verboten.

Nicht gesetzlich ausgeschlossen ist aber der Fahndungsabgleich. Das Fehlen einer strengen nationalen Zweckbeschränkung wird dazu führen, dass Fingerabdruckdaten aus den Ausweisen nicht nur zur Identitätsfeststellung verwendet werden, sondern auch zu **Zwecken des Fahndungsabgleichs** z.B. mit AFIS.

Um dem europarechtlichen Zweckbindungsgebot zu entsprechen, sollte daher zumindest folgende **zusätzliche Regelung in § 15 PAuswG** aufgenommen werden.

Die Nutzung der biometrischen Ausweisdaten auf Zwecke eines Abgleichs mit elektronischen Dateien, etwa für Fahndungszwecke, ist unzulässig.

Einer entsprechenden Regelung bedarf es wegen der Vergleichbarkeit der rechtlichen Situation auch in § 17 PassG, der den automatisierten Abruf von biometrischen Daten durch Sicherheitsbehörden bei **Kontrollen des Reisepasses** erlaubt, sowie für Abgleiche aus dem Personalausweis- und dem Passregister.

Mit dieser Regelung würde zugleich auch der automatisierte **Abgleich der Lichtbilddaten** mit externen Dateien, etwa dem GES des BKA ausgeschlossen. Welche Risiken insofern

bestehen, haben die polizeilichen Ermittlungen zu den im Rahmen des G-20-Gipfels im Jahr 2017 begangenen Straftaten gezeigt, wo Gesichtsbilder von vermeintlichen Straftätern mit Hilfe von automatisierter Gesichtserkennung analysiert und zur Öffentlichkeitsfahndung verwendet wurden.[22] Ohne ein Abgleichsverbot bestünde die rechtliche Möglichkeit, im Rahmen von Ausweiskontrollen biometrische Abgleiche mit Fahndungsregistern vorzunehmen. Angesichts der technisch bedingten Fehlerquote würden diese Fahndungsabgleiche dazu führen, dass zunächst viele völlig unschuldigen Personen in sicherheitsbehördliche Fahndungen einbezogen würden.

Ohne die oben vorgeschlagenen Regelungen würde gegen die europarechtliche Pflicht zur Regelung **angemessener Garantien** und spezifischer Maßnahmen verstoßen, wie diese in Art. 9 Abs. 2 lit. g, Art. 87 DSGVO sowie Art. 10 DSRl-JI festgehalten ist.

C. Ergebnis:

1. Die europarechtliche Verpflichtung zur Aufnahme von zwei Fingerabdrücken in den Personalausweis verstößt wegen des unverhältnismäßigen Eingriffs in das Grundrecht auf Datenschutz gegen das Grundrecht auf Datenschutz nach Art. 8 GRCh.
2. Wenn die nationale Verpflichtung zur Speicherung von Abdrücken erlaubt wird, dann muss an Stelle des Zeigefingers (oder des Daumens bzw. des Mittelfingers) der Ringfinger oder der kleine Finger herangezogen werden.
3. Im Personalausweisgesetz (und auch im Passgesetz) ist eine Regelung aufzunehmen, die den Abgleich der biometrischen Daten mit externen elektronischen Dateien untersagt.

Für Rückfragen und weitere Erläuterungen stehe ich gerne zur Verfügung

Mit freundlichen Grüßen
Dr. Thilo Weichert

[22] Große Öffentlichkeitsfahndung nach G-20-Gewaltverdächtigen, DANA 1/2018, 41 ff.; Datenschutzbeauftragter beanstandet polizeiliche Gesichtserkennung, DANA 4/2018, 199 f.

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)613 A

Stellungnahme zur Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages am 26.10.2020

zum Entwurf eines

"Gesetzes zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen"

durch die

Unternehmen digitaler Bildverarbeitung

Auto Photo Kiosk GmbH, Bonn

FORAM Service GmbH, Berlin

Fotofix Schnellphotoautomaten GmbH, Krefeld

Hujer & Graf Automaten GmbH, Karlsfeld

W. Lause GmbH, Schwaig

Speed Biometrics GmbH, Ratingen

Vending Concept, Bonn

Kritik am Entwurf eines "Gesetzes zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen".

Die Bundesregierung hat einen Gesetzentwurf in den Deutschen Bundestag eingebracht, der in beispielloser Weise zulasten von Privatunternehmen in die Wirtschaftsordnung der Bundesrepublik Deutschland eingreift. Das Gesetz zielt darauf ab, das Monopol eines Staatsunternehmens zu Ungunsten einer ganzen Branche kleinerer und mittlerer Unternehmen zu errichten und nimmt dabei deren existenzielle ökonomische Vernichtung in Kauf.

Die Absicht der Bundesregierung, die Bundesdruckerei GmbH als einzigen Lieferanten für Geräte zur biometrischen Bilderfassung in den Kommunen zu bestimmen, greift in den Wettbewerb ein und verletzt das Grundrecht aus Artikel 12 GG auf Berufs- und Gewerbefreiheit anderer Wirtschaftsbeteiligter.

Wir teilen ausdrücklich das proklamierte Ziel der Bundesregierung, durch wirksame technische Vorkehrungen Verfälschungen von Biometriebildern durch "Morphing" auszuschließen. Die von uns hergestellten und eingesetzten Geräte erfüllen diese Voraussetzung seit dem Jahr 2006 und somit lange bevor die Bundesdruckerei GmbH ihre Produkte zur Marktreife gebracht hat. Wir betreiben seit Jahren wirtschaftlich erfolgreiche, der Größe und Einwohnerzahl angemessene Lösungen zur sicheren biometrischen Bilderfassung in Städten und Kommunen in ganz Deutschland.

Wir verwehren uns dagegen, dass auf gesetzlichem Wege ein Staatsunternehmen, das bisher aufgrund fehlender Erfahrung und Innovationskraft keinen nennenswerten Markterfolg erzielen konnte, durch eine dem europäischen Wettbewerbsrecht widersprechende Beihilfe von 171 Mio. Euro in die Lage versetzt werden soll, Geräte zu entwickeln und in den kommunalen Ämtern aufzustellen. Dies insbesondere mit der Konsequenz, dass die seit über 15 Jahren erfolgreich tätigen, technologisch und sicherheitstechnisch führenden privaten Unternehmen aus diesem Marktsegment vollständig verdrängt werden.

Mit dem sogenannten "Betreibermodell" der Bundesdruckerei GmbH wird die Finanzhoheit und Entscheidungsfreiheit der Kommunen verletzt, denn diese werden ihrer bisherigen Möglichkeit beraubt, denjenigen Anbieter einer Lösung zur verfälschungssicheren Aufnahme eines Biometriebilds auszuwählen, der das unter Berücksichtigung der individuellen Gegebenheiten (z.B. Einwohnerzahl, Räumlichkeiten) beste Verhältnis aus Technik, Service und Kosten bzw. Einnahmen pro Bild bietet. Die Kommunen verlieren dadurch jährliche Einnahmen in Millionenhöhe.

Kritikwürdig erscheint vor diesem Hintergrund auch, dass der Gesetzentwurf, der nur in den Artikeln 9, 10 und 11 wirklich eilbedürftig zu beratende Sachverhalte enthält, im Eilverfahren vom Parlament verabschiedet werden soll, ohne dass die ökonomischen Folgen, die Auswirkungen auf die kommunale Selbstverwaltung und schließlich die verfassungs- und europarechtliche Dimension bisher hinreichend Berücksichtigung finden konnten.

Wir bitten den Innenausschuss und die mitberatenden Ausschüsse des Deutschen Bundestages, eine Beschlussempfehlung für den Deutschen Bundestag mit (u.a.) folgendem Inhalt zu fassen:

1. **Artikel 1 Nummer 1.** (Bestimmung des Geräteherstellers durch das BMI):
   Wird ersatzlos gestrichen; § 1 Abs. 5 PassG in der aktuellen Fassung bleibt damit unverändert.

2. **Artikel 2 Nummer 2.** (Bestimmung des Geräteherstellers durch das BMI):
   Wird ersatzlos gestrichen; § 4 Abs.3 PAuswG in der aktuellen Fassung bleibt damit unverändert.

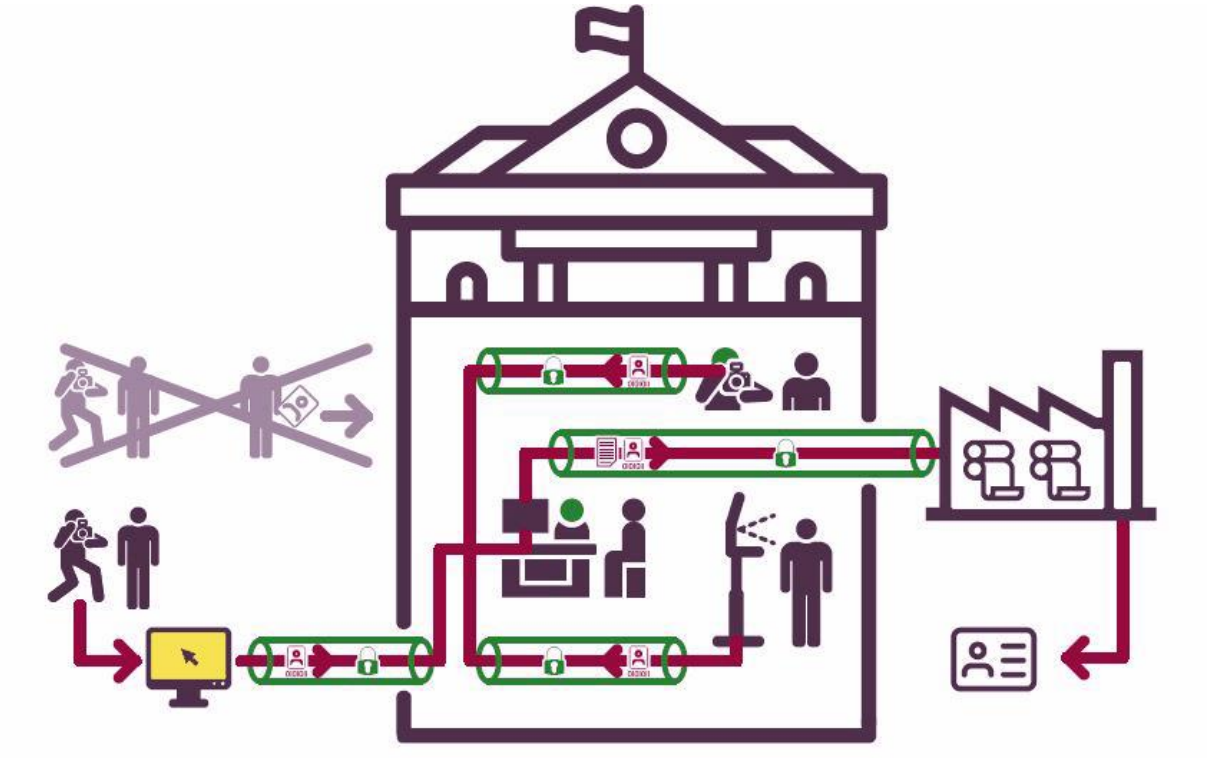
Die wichtigsten Gründe:

1. Verfälschung des Biometriebildes durch Morphing wird bereits sicher verhindert

Morphing setzt einen (unbefugten) Zugriff auf das gedruckte oder elektronische Bild voraus, um dieses verändern zu können. Deshalb sieht der Gesetzentwurf (richtigerweise!) vor, dass das Passfoto zukünftig ausschließlich digital zu erstellen und zu übermitteln ist. Die in den Behörden genutzten Fotokabinen, "Small Business"-Aufnahmegeräte für kleine Bürgerämter und Multifunktionsgeräte der Biometriedienstleister erfüllen diese Anforderung bereits seit vielen Jahren. Die Übertragung der Bilder erfolgt ausschließlich innerhalb des kommunalen Netzes und ist damit gegen unbefugte Zugriffe gesichert. Darüber hinaus erfüllen die vorgenannten Geräte die einschlägigen Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), der International Civil Aviation Organization (ICAO) u.a..

Fotokabinen sind physisch gesichert, andere Geräte stehen immer im Innenbereich der Bürgerbüros, haben keine offen zugänglichen Schnittstellen und sind softwareseitig abgesichert. Zudem gehen die Geräte mit Datenschutz- und Datensicherheitszertifikaten des ULD Schleswig-Holstein über die zwingenden Anforderungen weit hinaus. Seit der Einführung der direkten digitalen Bildübertragung durch die privaten Biometriedienstleister haben die Hersteller gemeinsam mit den Entwicklern der Kommunalsoftware alle Normen und Anforderungen mitentwickelt und umfassend erfüllt.

System der Aufnahme, Übermittlung und Verarbeitung biometrischer Passbilder in Behörden



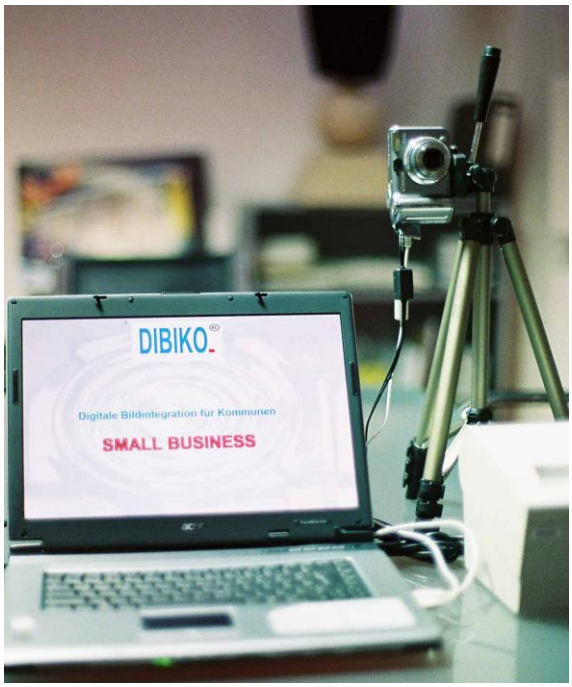
:© Speed Biometrics

2. Private Hightech-Biometriedienstleister technologisch führend

Seit Anfang der 1990er Jahre sind die Hersteller und Aufsteller von Fotoautomaten Partner der Kommunen. 2006 entwickelte die Bonner Firma Vending Concept die digitale, medienbruchfreie Übertragung von Biometriefotos und stellte sie auf dem Stand des damaligen Bundesinnenministers Schäuble auf der CEBIT 2006 vor.

©Foto Grafik Rühmekorf

2007 folgte das DIBIKO® Small Business für kleine Bürgerämter, das die Funktionen der Biometriebildaufnahme in Kamera und Laptop minimiert. Dadurch wurden angepasste Lösungen für kleine, finanz- oder einwohnerschwache Kommunen ermöglicht. (Bild unten links)



©Foto Grafik Rühmekorf

©W.Lause GmbH

Die digitale Übertragungstechnik wurde ab 2009 auch in den Geräten des größten Herstellers, der Fotofix Schnellphotoautomaten GmbH, Krefeld, eingesetzt. 2012 brachte das Ratinger Unternehmen Speed Biometrics GmbH ein Multifunktionsterminal auf den Markt, das neben dem

Foto auch Unterschrift und Fingerabdruck erfasst (oben rechts). Alle privaten Biometriedienstleister setzen die Geräte dieser drei Hersteller ein. Seit der Einführung biometrischer Fotos sind alle technischen Innovationen durch diese privaten KMU erfolgt. Die notwendigen Schnittstellen in den Fachverfahren der Kommunalsoftware wurden ebenfalls auf Initiative der KMU geschaffen.

Die Anwendung einheitlicher technischer Standards, auch im Detail, wird bereits heute in vielen Bereichen und insbesondere für hoheitliche Dokumente dadurch sichergestellt, dass u.a. das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Anforderungen umfassend definiert und deren Einhaltung durch Zertifizierungen testiert.

Die Bundesdruckerei GmbH verfügt keineswegs über besondere Expertise in der biometrischen Bild- und Datenerfassung. So trat z.B. zum 01.11.2019 die Technische Richtlinie BSI TR-03121-3.2 in Version 4.4 in Kraft, die das Verfahren für die Aufnahme, Echtheitsbewertung und Qualitätssicherung des Lichtbilds und der Fingerabdrücke präzisiert. Die Bundesdruckerei GmbH hat diese Anforderungen bis dato nicht umgesetzt, weshalb deren in den Behörden befindliche Self-Service-Terminals (SST) nur noch eingeschränkt genutzt werden.

KoKomm 2006: Mitarbeiter einer bayerischen Gemeinde (Wolfratshausen) testen die Leistungsfähigkeit der Biometriesoftware

3. Private Dienstleister bundesweit tätig

Die Biometriebild-Dienstleister der Privatwirtschaft sind rund 1.500-fach in Personalausweis-, Pass- und Ausländerbehörden (sowie Fahrerlaubnisbehörden) in ganz Deutschland vertreten. Zu ihren Kunden zählen zahlreiche Mittel- und Großstädte, viele Städte und Gemeinden aus der großen Gruppe mit 5.000 bis 20.000 Einwohnern und schließlich auch solche mit nur rund 1.000 bis 5.000 Einwohnern. Das zeigt eindrucksvoll, dass die Privatwirtschaft bereits heute passende Lösungen für Kommunen aller Größenordnungen und aller Regionen anbietet.
Die Verbreitung dieser Lösungen ist nur deshalb nicht bereits weiter fortgeschritten, weil die Vorlage eines Papierbilds aktuell der gesetzliche Standardfall ist und sich viele Kommunen daher und in Verbindung mit anderen Gründen (Platzknappheit, Schutz von lokalem Einzelhandel und Handwerk etc.) bisher nicht für den Einsatz von Selbstbedienungsterminals, Fotoautomaten oder Kameras entscheiden konnten/wollten. Interessant sind dabei erhebliche regionale Unterschiede bezüglich des Interesses und der Nachfrage seitens der Kommunen.

Die privaten Dienstleister Auto Photo Kiosk GmbH, Alpha Concept, Cornelius, FORAM Service GmbH, Fotofix Schnellphotoautomaten GmbH, Foto Select, Hujer & Graf Automaten GmbH, W. Lause GmbH, Foto-Schwarz, Speed Biometrics GmbH, Vending Concept, sowie weitere kleine selbständige Fotoautomatenaufsteller sind (unternehmensübergreifend) bundesweit in allen

Bundesländern und dabei in den Ballungsräumen wie auch in strukturschwachen Räumen mit geringer Einwohnerzahl vertreten.

Bundesland	**Stand-orte**	**Städte (Auswahl, Beispiele)**	**Auswahl, Beispiele Gemdn. 2-20 Tsd (Einwohnerzahl)**
Baden-Württemberg	37	Freiburg, Heidelberg, Heilbronn, Karlsruhe, Pforzheim, Radolfzell, Stuttgart	Plankstadt, Aulendorf, Dossenheim
Bayern	148	Augsburg, Erlangen, München, Nürnberg, Regensburg, Würzburg	Affing (5.476), Bad Tölz, Baunach (8.159), Loiching (3.590), Niederviehbach (2.611), Röthenbach, Siegsdorf (8.355)
Berlin	127	Alle Bezirke	- -
Brandenburg	132	Falkensee, Ludwigsfelde, Teltow	Brieselang, Dallgow-Döberitz (9.931), Ketzin (6.498), Nauen, Nennhausen (4.626), Oberkrämer, Premnitz (8.453), Rangsdorf, Schönefeld, Schönwalde-Glien (9.575)
Bremen	7	Alle Bürgerämter + Bremerhaven	- -
Hessen	38	Bad Homburg, Friedberg, Gießen, Hattersheim, Hofheim, Marburg, Offenbach	Ginsheim-Gustavsburg, Wehrheim (9.468)
Hamburg	27	Alle Bezirke	- -
Mecklenburg-Vorpommern	145	Crivitz, Neubrandenburg, Waren	Born am Darß (1.134), Heringsdorf (8.547), Insel Poel (2.485), Kühlungsborn (7.896), Miltzow (6.929), Neuburg (2.112) Rostocker Heide (9.759), Warnow-West, West-Rügen (9.490), Wolgast, Zingst (3.089),
Niedersachsen	163	Celle, Cloppenburg, Hannover, Leer, Lingen, Oldenburg, Osnabrück, Seevetal, Tostedt	Cappeln (7.104), Isenbüttel, Lastrup (6.970), Sassenburg
Nordrhein-Westfalen	376	Alfter, Bergheim, Bielefeld, Bochum, Bonn, Bornheim, Dortmund, Dülmen, Düsseldorf, Essen, Euskirchen, Hamm, Heiligenhaus, Heinsberg, Herford, Hilden, Hörstel, Kerpen, Köln, Langenfeld, Meckenheim, Minden, Münster, Nettetal, Remscheid, Recklinghausen, Rheinbach, Soest, Würselen, Wuppertal, Wülfrath	Balve, Gangelt, Herscheid (6.977), Kirchlengern, Merzenich (9.778), Niederzier, Odenthal, Reichshof, Schermbeck Selfkant, Tüddern, Wassenberg
Rheinland-Pfalz	35	Kaiserslautern, Römerberg-Dudenhofen, Worms	Bad Dürkheim, Bad Hönningen, Böhl-Iggelheim, Dannstadt-Schauernheim, Freinsheim, Simmern
Saarland	16	Saarlouis	Mettlach, Perl (8.566), Quierschied
Sachsen	45	Dresden, Grimma, Leipzig, Torgau	Flöha, Lichtenberg/Erzgebirge (5.198), Mulda (2.479)
Sachsen-Anhalt	34	Dessau, Halle, Merseburg	Bördeland (7.523), Calbe (8.609), Flechtingen, Hohe Börde
Schleswig-Holstein	44	Flensburg, Geesthacht, Kiel, Neumünster, Norderstedt, Pinneberg, Reinbek	Ammersbek (9.825), Bad Segeberg, Dassendorf (3.114), Horst-Herzhorn, Hürup (1.135), Leezen (8.754), Ratzeburg, Schönberg (6.729)
Thüringen	46	Erfurt, Suhl, Weimar,	Bad Frankenhausen/ Kyffhäuser, Leinetal (6.746), Ohrdruf, Straußfurt (2.105)
	1.420		

4. Gesetzentwurf mit "heißer Nadel" gestrickt?

Der Gesetzentwurf, in welchem sich die Zahl der Meldebehörden zwischen Referentenentwurf und Kabinettsbeschluss ebenso wundersam erhöhte, wie sich eine nicht konkret nachvollziehbare Anzahl von Aufnahmegeräten veränderte, wirft erhebliche Fragen auf. So war im Referentenentwurf noch von 5.500 Pass- und Ausweisbehörden und 11.000 sogenannten "Selbstbedienungsterminals" die Rede, während in der vorliegenden Drucksache für 6.115 Behörden von 9.500 "Aufnahmegeräten", 7.500 am Arbeitsplatz, 2.000 "Selbstbedienungsterminals" die Rede ist.

Diese offensichtlichen Fehler bei der Einschätzung des Marktes bestätigen unsere Erfahrung, dass die Realität vor Ort nicht vom "grünen Tisch" und mit einer Standardlösung bewältigbar ist. Es bedarf umfangreicher Erfahrung und Kenntnisse über Beleuchtung, räumliche Verhältnisse, flexible Geräte und einfache Bedienbarkeit, um angepasste und kundengerechte Lösungen anbieten zu können. Die Privaten bringen dabei entscheidende Wettbewerbsvorteile mit. Damit sind den Autoren des Entwurfs essentielle Wettbewerbsfaktoren offensichtlich entgangen. Vielmehr drängt sich der Eindruck auf, dass das BMI sich ausschließlich darauf konzentriert hat, zu prüfen, ob eine In-House-Beauftragung der Bundesdruckerei GmbH möglich ist, statt zunächst gemäß dem Subsidiaritätsprinzip eine gleichwertige oder kostengünstigere Erfüllung der Aufgabe durch Private zu prüfen.

5. Verstoss des Gesetzentwurfs gegen EU-Recht: Verbotene Beihilfe

Träte der Gesetzentwurf in Kraft, würden aus öffentlichen Mitteln etwa 171 Mio. Euro aufgewendet werden, indem der Bund Geräte durch die Bundesdruckerei GmbH beschafft und den Kommunen im "Betreibermodell" bereitstellt. Diese Investitionskosten tragen bisher fast ausschließlich die Unternehmen und Dienstleister. Da gleichzeitig die Ausweisgebühren für die Verbraucher um jeweils 6 Euro erhöht werden sollen, fließt dieser Betrag an die Bundesdruckerei, ohne die Kommunen finanziell zu beteiligen, wie dies die Geschäftsmodelle der Biometriebild-Dienstleister bisher tun. Das bedeutet nicht nur Einnahmeverluste für die Kommunen. Das Vorhaben verstößt möglicherweise sowohl gegen EU-Recht - freier Dienstleistungs- und Warenverkehr - als auch gegen die Haushaltsgrundsätze der Sparsamkeit und Subsidiarität der Bundeshaushaltsordnung (BHO).
Da der Gesetzentwurf davon ausgeht, dass die Bundesdruckerei GmbH erst durch die öffentlichen Mittel in die Lage versetzt werden soll, eine entsprechende Zahl von Geräten für alle Kommunen herzustellen oder herstellen zu lassen, um das sogenannte "Betreibermodell" überhaupt durchzuführen - und dabei die bisher in den Kommunen vorhandenen Privatanbieter zu verdrängen - ist es wahrscheinlich, dass es sich bei dem veranschlagten Haushaltstitel um eine verbotene Beihilfe nach EU-Recht handelt, konkret einen Verstoß gegen Art. 106 (1) i.V.m. Art. 102 AEUV. Denn aus eigener Investitionskraft und am freien Markt wäre die Bundesdruckerei niemals in der Lage, diese Investition profitabel vorzunehmen.

6. Eingriff in die kommunale Entscheidungs- und Finanzhoheit

Im Ergebnis brächte das Gesetz nicht unerhebliche Einnahmeausfälle für die Kommunen mit sich, die bisher zumeist an den Einnahmen der von den Biometriebild-Dienstleistern zur Verfügung gestellten Multifunktionsgeräte, Fotoautomaten und Arbeitsplatz-Bilderfassungsgeräte mit jeweils 20% bis zu 50% der Erlöse am Umsatz beteiligt sind.

Die Biometriebild-Dienstleister erbringen für die Kommunen seit vielen Jahren zeitnahe und zuverlässige Wartung und Service innerhalb von Stunden, weil sie bundesweit über ein Netz regional verankerter Mitarbeiter oder Dienstleister verfügen, die diese Leistungen vor Ort zuverlässig erbringen. Auch diese Kosten werden im Gesetzentwurf dem Bundeshaushalt auferlegt. Außerdem ist anzuzweifeln, ob die Bundesdruckerei in ihrer bisherigen Organisationsstruktur den Support zu leisten vermag und inwieweit der Aufbau einer dafür notwendigen Struktur zeit- und kostengerecht im Rahmen der vorgesehenen 171 Mio. € bewerkstelligt werden kann. Die zwangsweise Überstülpung des "Betreibermodells" der Bundesdruckerei bedeutet für die Gemeinden einen Eingriff in die Entscheidungsautonomie und finanzielle Verluste. Dies ist ein Eingriff in kommunale Selbstverwaltung und Finanzhoheit.
Des Weiteren entstehen Kommunen Kosten und Zeiteinsatz, um vorhandene Geräte abzubauen und durch neue Geräte zu ersetzen sowie die Behördenmitarbeiter entsprechend im Umgang zu schulen.

Angepasste Lösungen - in Sichweite der Mitarbeiter auch schon einmal aus Platzgründen in der Spielecke des Bürgerbüros

7. Verletzung des Grundrechts auf Gewerbefreiheit Artikel 12 Grundgesetz

Mit dem Gesetzentwurf entzieht der Gesetzgeber der gesamten privatwirtschaftlich organisierten Branche der Biometriedienstleister ihre Existenzgrundlage. Nahezu alle Unternehmen der inzwischen hoch spezialisierten Branche generieren zu 100% ihre Geschäftstätigkeit und damit ihren Gewinn aus der Tätigkeit als Biometriedienstleister. Sämtliche "Small-Business"-Geräte und Multifunktionsterminals kommen ausschließlich in kommunalen Ämtern zum Einsatz. Das trifft zwar nicht für alle, jedoch für einen nennenswerten Anteil der Fotokabinen zu. Im Übrigen sind auch die Automaten, die an öffentlichen Orten wie Einkaufszentren, Bahnhöfen und dgl. betrieben werden, vom Gesetzentwurf betroffen. Ebenfalls gravierend sind somit die Auswirkungen auf Betreiber, die nicht ausschließlich Standorte bei Behörden haben.

Da wie unter 1. dargelegt, kein übergeordneter sicherheitstechnischer Grund gegeben ist, liegt mit hoher Wahrscheinlichkeit ein verfassungswidriger Eingriff in die Gewerbefreiheit aus Artikel 12 GG vor, der in einem indirekten Entzug der wirtschaftlichen Existenzgrundlage der o.g. Unternehmen

besteht. Die Unternehmen fordern, dass stattdessen die seit Anfang der 1990er Jahre bewährte Partnerschaft mit den Kommunen erhalten bleibt. Damit die seit 2006 bestehende medienbruchfreie Übertragung von Biometriefotos in den Ämtern mit den durch private Biometriebild-Dienstleister betriebenen und gewarteten Geräte im chancengleichen Wettbewerb fortgeführt werden kann.

8. Verletzung des verfassungsrechtlichen Bestimmtheitsgrundsatzes

Der Gesetzentwurf der Bundesregierung zielt darauf ab, die Bundesdruckerei GmbH zum staatlichen Monopolunternehmen für die Herstellung von Bildaufnahmegeräten zu Pass- und Ausweiszwecken in den Kommunen zu machen. Dies geht zwar aus der Begründung des Gesetzentwurfes hervor, nicht aber aus dem Gesetzestext, der lediglich vorgibt, dass das BMI den Hersteller von Bilderfassungsgeräten bestimmt. Es werden weder Kriterien genannt und konkretisiert, noch nennt der Gesetzestext die offensichtliche Absicht der Bundesregierung, die staatseigene Bundesdruckerei zum einzigen Lieferanten für Bildaufnahmegeräte zu machen. Damit verstößt der Gesetzentwurf auch gegen das Gebot der Normenklarheit und Bestimmtheit der Gesetze.

9. Datenschutzrisiken durch Massenspeicherung biometrischer Daten in der Cloud

Darüber hinaus würden aufgrund der geplanten zahlreichen Ermächtigungen des BMI zum Erlass von Rechtsverordnungen ganz grundlegende Datenschutzfragen, auch hinsichtlich der DSGVO, offen bleiben. So verweist der Gesetzentwurf etwa auf Bilddaten-Clouds, ohne deren Gestaltung und Sicherheit zu konkretisieren. Angesichts der bekannten Risiken von zentralen Datenspeichern mit hunderttausenden Biometriefotos ist die Zielstellung des Artikelgesetzes, nämlich die gestiegene Gefahr durch "Morphing" von biometrischen Bildern auszuschließen, massiv in Frage gestellt. So kann nicht ausgeschlossen werden, dass z.B. durch Hackerangriffe erhebliche Datensicherheitslücken entstehen oder in Einzelfällen gemorphte Fotos eingestellt werden. Insofern ist die Novelle im Hinblick auf ihre zentrale Begründung mit Sicherheitserfordernissen inkonsistent und widersprüchlich.

10. Staatsmonopol statt Hilfe für Corona-geschädigte Mittelständler

Die Biometriedienstleister als kleine und mittelständische Unternehmen sind von der aktuellen Corona-Pademie wirtschaftlich schwer getroffen, da viele Einwohnerämter im "Lockdown" monatelang geschlossen waren und teilweise noch geschlossen sind oder die Nutzung der vorhandenen Geräte untersagen. Die Bundesregierung hat milliardenschwere Hilfsprogramme aufgelegt, um insbesondere für den Mittelstand und KMU die Folgen der Corona-Pandemie zu lindern und Insolvenzen zu vermeiden. Dazu passt in keiner Weise, die mittelständischen Biometriebild-Dienstleister zugunsten eines Staatsunternehmens zu verdrängen. Da es sich um unser Kerngeschäft handelt, in dem wir zudem rund zehn Jahre länger als die Bundesdruckerei erfolgreich tätig sind, helfen auch keine "Übergangsfristen". Vorschläge die darauf abzielen, "die Bundesdruckerei könne ja Unteraufträge vergeben" oder die Biometriedienstleister "als Zulieferer beauftragt werden" - so sinngemäß Parl. STS Prof. Dr. Krings in Antwortschreiben an verschiedene Abgeordnete des Deutschen Bundestages - gehen völlig an der wirtschaftlichen Realität vorbei.
Die Mehrzahl der Unternehmen sind Aufsteller, nicht Hersteller. Know-how und Kompetenz der Branche liegen in der Softwareentwicklung, Erfahrung und Servicequalität sowie der Innovationsfähigkeit und Flexibilität, kundenangepasste Lösungen zu finden. Seit 2006 hat die Privatwirtschaft innovative Lösungen entwickelt und immer wieder das Gespräch und die Zusammenarbeit mit der Bundesdruckerei gesucht, die diese jedoch stets abgelehnt hat.

Dementsprechend erscheinen Aussagen, die eine verstärkte Kooperation zwischen Bundesdruckerei und Privatwirtschaft vorsehen, wenig substantiell und glaubwürdig.

11. Gesetzentwurf: Widerspruch zu den von CIO Dr. Richter proklamierten Grundsätzen

Der CIO der Bundesregierung, Staatssekretär Dr. Markus Richter, hat im Juli 2020 den "9-Punkte-Plan für ein digitales Deutschland" der Öffentlichkeit vorgestellt. Dort bekennt sich die Bundesregierung unter Punkt 8 Absatz 1 zur Herstellerunabhängigkeit bei IT-Lösungen. Der vorliegende Gesetzentwurf verfolgt genau das Gegenteil dieser Strategie.

12. Unser Fazit:

Zusammenfassend stellen wir fest, dass der Gesetzentwurf einen unbegründeten staatlichen Markteingriff gegenüber einer leistungsfähigen und starken, technisch innovativen und kundenfreundlichen Branche darstellt.

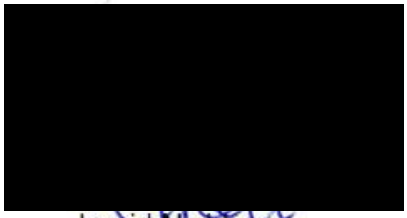
Die Bundesdruckerei GmbH verfügt unzweifelhaft über große Expertise in verschiedenen Bereichen (Dokumentenproduktion u.a.). Dies gilt jedoch nicht für die Ausstattung von Behörden mit Geräten zur Aufnahme des Lichtbilds in der Fläche und unter Berücksichtigung ganz unterschiedlicher lokaler Gegebenheiten und Anforderungen. Die Biometriebranche hingegen verfügt über langjährige Praxiserfahrung, gerade auch im Bereich des Services. Die Beauftragung der Bundesdruckerei bietet weder sicherheitstechnisch noch bei den Dienstleistungen für die Kommunen entscheidende Vorteile.

Für weitere Informationen und Gespräche stehen wir jederzeit zur Verfügung.

Alfred Freer
Geschäftsführer, Hujer & Graf Automaten GmbH
www.automatenfoto.de

Daniel Middendorf
Geschäftsführer, Fotofix Schnellautomaten GmbH
www.fotofix.de

Marcel Moser
Inhaber Vending Concept
www.vendingconcept.com



Ingrid Niebler
Geschäftsführerin W. Lause GmbH
www.ausweis-automat.de

Stefan Pahmeier
Geschäftsführer Speed Biometrics GmbH
www.speed-biometrics.de

Andreas Schramm
FORAM Service GmbH
www.foram-service-berlin.de

Kontakt:
Roa.Consult
Kirchgässchen 1
53332 Bornheim/Rhld.
t .02222-931210
f. 02222-931327
info@RoaConsult.com
www.RoaConsult.com

Deutscher Bundestag 1
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)613 A - Anlage

Dr. Uwe Günther
Rechtsanwalt
Hartmut Geil
Rechtsanwalt

Kurzgutachten zum Gesetzentwurf zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen

Gliederung

Vorbemerkung

Im nachfolgenden Gutachten beschäftigen wir uns mit dem Entwurf des Gesetzes zur Stärkung der Sicherheit im Pass- , Ausweis- und ausländerrechtlichen Dokumentenwesen, und zwar unter der eingeschränkten Perspektive der Rechte der Hersteller, Anbieter und Betreiber von Fotoautomaten und anderen Vor-Ort-Aufnahme-Lösungen. Deren wirtschaftliche Existenz wird dadurch bedroht, dass das Herstellen von Lichtbildern verlagert wird auf die im Bundeseigentum befindliche Bundesdruckerei. Wir behandeln also nicht die möglicherweise verletzten Rechte von Kommunen. Auch das Datenschutzrecht wie das Wettbewerbsrecht im engeren Sinne bleiben außerhalb unserer Betrachtung.

1. Sachverhalt

1.1 Gesetzesgeschichte

Das Bundesinnenministerium hat im Dezember 2019 den Entwurf eines Gesetzes zur Stärkung der Sicherheit im Pass- und Ausweiswesen vorgelegt. Das Gesetz dient u.a. der Erfüllung der Verordnung (EU) 2019/1157 des Rates der Europäischen Union und des Parlaments, wonach Personalausweise künftig „mit einem hochsicheren Speichermedium zu versehen sind, das ein Gesichtsbild des Personalausweisinhabers und zwei Fingerabdrücke in interoperablen digitalen Formaten enthält“.

Hintergrund ist der im Bereich der EU beobachtete Gebrauch von ge- oder verfälschten Personalausweisdokumenten. Neben den bereits verwendeten Sicherheitsmerkmalen sollen die Verwendung von Fingerabdrücken und biometrischen Bildern verbindlich festgeschrieben werden. Entsprechende Regelungen auf EU-Ebene galten in der Vergangenheit nur bei neu ausgestellten Reisepässen. In Deutschland ist das biometrische Lichtbild im Personalausweis seit 2010 verpflichtend, die Speicherung der Fingerabdrücke ist derzeit noch freiwillig.

Eine viel diskutierte Form der Verfälschungen von biometriegeeigneten Fotografien ist das sogenannte Morphing. Hierbei wird eine Bilddatei derart manipuliert, dass den biometrischen Daten einer Person das Aussehen einer anderen Person untergeschoben wird. Dies ist allerdings nur möglich, wenn das Aussehen dieser Personen gewisse Ähnlichkeiten aufweist.

In der Praxis der kommunalen Ämter werden die Fingerabdrücke und die Unterschrift der antragstellenden Person jeweils mit spezieller Hardware von der Sachbearbeitung aufgenommen, direkt digitalisiert und aus dem IT-

System der sachbearbeitenden Kommune als Bestandteil des Ausweisantrags an die Bundesdruckerei, die die Ausweisdokumente fertigt, übermittelt.

Die Fotografien werden in der Regel in analoger Form von den Antragstellern geliefert. Sie werden in einem erheblichen Umfang von mittelständischen Fotografen gefertigt. Diese haben allerdings außer der Übergabe der Bilder auch die Möglichkeit, die Bilddateien in besonderer, gesicherter Weise den Passbehörden zu übersenden. Außerdem wird ein nicht unerheblicher Teil in Fotokabinen gefertigt und ebenfalls analog oder – sofern die Kabinen innerhalb der Passbehörden betrieben werden – innerhalb des lokalen Netzes der Behörde sicher digital an die Passbehörde übermittelt.

Der Referentenentwurf sah zunächst vor, dass die Passfotos ausnahmslos in den Passbehörden mit Selbstbedienungsterminals der Bundesdruckerei aufgenommen werden sollten.

Nach erheblichen Protesten der Fotografen, für die die Ausweisfotografie einen erheblichen Teil ihres Umsatzes generiert, wurde vorgesehen, dass auch Bilder von Berufsfotografen Verwendung finden können, wenn sie auf einem besonderen sicheren Übertragungsweg digital an die Passbehörden übertragen werden.

§ 1 Abs. 5 GE PassG soll wie folgt gefasst werden:

> *„(5) Das Bundesministerium des Inneren, für Bau und Heimat bestimmt den Passhersteller sowie den Lieferanten von Geräten zur Aufnahme und elektronischen Erfassung von Lichtbildern, sofern diese in der Passbehörde gefertigt werden, und von Fingerabdrücken und macht deren Namen im Bundesanzeiger bekannt. Dies gilt nicht für Geräte zur Aufnahme und elektronischen Erfassung von Lichtbildern, die im Rahmen einer Antragstellung beim Auswärtigen Amt gefertigt werden.“*

§ 4 Abs 3 des PersonalausweisG soll wie folgt gefasst werden:

> *„(3) Das Bundesministerium des Inneren, für Bau und Heimat bestimmt*
>
> *1. …..*
>
> *2. den Lieferanten von Geräten zur Aufnahme und elektronischen Erfassung von Lichtbildern, sofern diese in der Personalausweisbehörde gefertigt werden.*
>
> *3. …*
>
> *4. …“*

Aus der Gesetzesbegründung geht hervor, dass der BMI beabsichtigt, gemäß § 1 Abs. 5 PassGE die Bundesdruckerei als Anbieter festzulegen. Es heißt in der Begründung zu Art. 1, Nr.1 GE:

> *„Die Aufgabe der Passproduktion wird seit Langem durch den Bund wahrgenommen, indem dieser den Passhersteller bestimmt, beauftragt und überwacht. Diese Aufgabe wird durch die bundeseigene Bundesdruckerei wahrgenommen. Die Vorgaben aus dem Vergaberecht finden derzeit wegen § 108 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) keine Anwendung. Die Ergänzung des § 1 Absatz 5 PassG stellt klar, dass diese Aufgabe auch die Bereitstellung von Geräten zur Aufnahme und elektronischen Erfassung von Fingerabdrücken und Lichtbildern als Annex umfasst, sofern diese vor Ort in der Passbehörde erstellt werden.“*

1.2 Technische und Marktlage

Die im Ausweiswesen verwendeten Fotografien werden derzeit zu etwa 50 % von Berufsfotografen gefertigt. Etwa 30 % stammen von den Fotokabinen freier Anbieter. Es gibt drei große Hersteller, eine ähnliche Anzahl großer

Betreiber (mit einer Vielzahl von Geräten im Markt) und einige kleinere Betreiber von Fotokabinen und ähnlichen Geräten.

Ein großer Teil der verwendeten Fotokabinen steht in den Bürgerämtern und in deren unmittelbarer Nähe. Das Aufstellen der Fotokabinen wird von den Kommunen ausgeschrieben, es werden Verträge mit einer Laufzeit von 2-4 Jahren abgeschlossen. Zu den vertraglichen Pflichten der Aufsteller gehört die Gewährleistung einer dauerhaften Betriebsbereitschaft der Kabinen. Diese wird durch die Tätigkeit eines vom Aufsteller beauftragten Wartungspersonals gewährleistet. Für das Aufstellen der Geräte haben die Aufsteller ein Entgelt zu entrichten, das in aller Regel pro aufgenommenem Bild berechnet wird. Die Kommune erhält einen Anteil von bis zu 50 % des für das Foto entrichteten Preises.

Diese Fotokabinen arbeiten digital. Das Aufnahmegerät wird entsprechend der Größe und Blickrichtung der aufgenommenen Person ausgerichtet. Die Bilddatei wird mithilfe einer Biometriesoftware auf Eignung überprüft und innerhalb des lokalen Netzwerks sicher direkt digital an die Ausweisbehörde übertragen. Es besteht keine Möglichkeit für Dritte, an die Bilddateien zu gelangen und diese zu verfälschen – es sei denn, die Täter hackten sich in die Datenverarbeitung der Kommune ein und wären zugleich in der Lage, die verschlüsselten Dateien zu entschlüsseln.

Aus historischen Gründen gibt es im Detail unterschiedliche Schnittstellen. Die Ausweisbehörden setzen für die Antragsbearbeitung diverse Softwareprodukte ein, diese bieten jeweils Schnittstellen zu allen Aufnahmelösungen. Eine Standardisierung der Schnittstellen (z.B. durch das Bundesamt für Sicherheit in der Informationstechnik) wäre problemlos möglich und würde die Unterstützung der Hersteller finden.

Es gibt auch noch Fotokabinen, in denen ein analoges Bild erzeugt wird, das die Antragsteller der Ausweisbehörde übergeben, wie oben dargelegt.

Im Angebot der Unternehmen der Biometriewirtschaft sind auch sogenannte Small Business-Anlagen für kleinere Behörden. Hier wird das Foto der Antragsteller mithilfe einer auf einem Stativ angebrachten Digitalkamera aufgenommen, dieses wird direkt von der Digitalkamera in einen Laptop

Computer übertragen und dort geprüft. Die Übertragung erfolgt dann direkt aus dem Laptop in das IT-System der Ausweisbehörde.

Diese beiden modernen Varianten sind von der Biometriewirtschaft entwickelt und auf den Markt gebracht worden. Die Bundesdruckerei hat jeweils erst deutlich später als die privatwirtschaftlichen Anbieter ähnliche Lösungen entwickelt und auf den Markt gebracht.

Die Fertigung von Ausweisfotos macht bei den drei Herstellern sowie den diversen Betreibern einen erheblichen Teil ihres Umsatzes aus. Die größte Firma am Markt, die Teil eines internationalen Konzerns ist, hat daneben durch das Aufstellen von Fotokabinen in Supermärkten noch weitere Einnahmequellen. Für die beiden mittelständischen Hersteller erbringen die in Ausweisbehörden aufgestellten Geräte praktisch den gesamten Umsatz.

2.Gutachten

Es ist fraglich, ob die Regelungen des Gesetzesentwurfes mit höherrangigem Recht vereinbar sind. In Betracht kommen Verstöße gegen das Grundrecht auf Berufsfreiheit in Art. 12 GG. Fraglich ist weiter, ob die Übertragung des Rechts zur Bestimmung des Dienstleisters auf die Bundesdruckerei mit der europäischen Dienstleistungsrichtlinie in Einklang zu bringen ist. Schließlich könnte ein Verstoß gegen rechtsstaatliche Grundsätze (Art. 20 Abs 3 GG) vorliegen.

2.1. Art. 12 GG

Art. 12 GG haben alle Deutschen das Recht, den Beruf frei zu wählen. Die Berufsausübung kann durch Gesetz oder aufgrund eines Gesetzes geregelt werden.

2.1.1 Beruf

Fraglich könnte sein, ob das Gesetz in den Schutzbereich von Art. 12 GG eingreift, ob es sich also bei der Tätigkeit der Produzenten und Aufsteller und Fotokabinen um einen Beruf im Sinne dieser Norm handelt.

Nach der Rechtsprechung des Bundesverfassungsgerichts ist unter Beruf jede auf Erwerb gerichtete Tätigkeit zu verstehen, die auf Dauer angelegt ist und der Schaffung und Erhaltung einer Lebensgrundlage dient. Der Schutz der Berufsfreiheit ist nicht auf traditionell oder gesetzlich fixierten Berufsbilder beschränkt, sondern erfasst auch Berufe die aufgrund der fortschreitenden technischen, sozialen oder wirtschaftlichen Entwicklung neu entstanden sind (BVerfG, Beschluss vom 07.03.2017 – 1 BvR 1314/12 u.a. Rn. 110 mit weiteren Hinweisen, ständige Rechtsprechung).

Zweifellos handelt sich bei der Tätigkeit der Biometriewirtschaft um eine auf Dauer angelegte Erwerbstätigkeit, die der Schaffung und Erhaltung einer Lebensgrundlage dient. Insofern liegt ein Beruf im Sinne des Grundrechts aus Art. 12 GG vor. In dieses Grundrecht greift das Gesetz auch ein, weil es den Anbietern die Ausübung ihres Berufes unmöglich macht bzw. diesen wesentlich erschwert, soweit die Biometriedienstleistungen für die Ausweisbehörden nicht die einzige Erwerbsquelle sind.

2.1.2 Zulässigkeit der Beschränkung

Bei der Übertragung des alleinigen Rechts zur Ausstattung der Ausweisbehörden auf einen einzigen Anbieter, hier die Bundesdruckerei, könnte es sich um einen unzulässigen Eingriff in die Berufsfreiheit handeln.

Nach der Rechtsprechung des Bundesverfassungsgerichts handelt sich dabei um ein einheitliches Grundrecht der Berufsfreiheit, in das nur auf gesetzlicher Grundlage und unter Beachtung des Grundsatzes der Verhältnismäßigkeit eingegriffen werden darf. Der Eingriff muss zur Erreichung eines legitimen Eingriffziels geeignet sein und darf nicht weitergehen, als es die Gemeinwohlbelange erfordern; ferner müssen Eingriffszweck und Eingriffsintensität in einem angemessenen Verhältnis stehen. An objektivierte Berufszugangsregelungen sind grundsätzlich

gesteigerte Anforderungen zu stellen (BVerfG aaO. Rn. 121, mit weiteren Nachweisen, ständige Rechtsprechung).

Der Eingriff muss also nach der ständigen Rechtsprechung des Bundesverfassungsgerichts

- ein legitimes Ziel haben
- er muss für dessen Zielerreichung geeignet sein
- er muss zur Zielerreichung erforderlich sein
- er muss verhältnismäßig sein

Legitimes Ziel

Das Bundesinnenministerium nennt als Ziel des Gesetzes bereits in dessen Titel die verbesserte Sicherheit des Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesens. Mit dem Gesetz soll noch besser gewährleistet werden, dass die Personaldokumente der Bundesrepublik Deutschland zuverlässig die richtige Identität des Inhabers ausweisen. Eine solche Zuverlässigkeit der Personaldokumente ist geeignet, die öffentliche Sicherheit beispielsweise auf den Gebieten der der Kriminalitätsbekämpfung, im Kampf gegen den Terrorismus oder des Ausländerwesens zu fördern. Hierbei handelt es sich um ein legitimes Eingriffsziel.

In diesem Zusammenhang sei allerdings noch darauf hingewiesen, dass die beabsichtige Gesetzesänderung auch geeignet ist, die finanzielle Ausstattung der Bundesdruckerei zu verbessern. Ein derartiges fiskalisches Ziel stellt kein Ziel dar, das die Einschränkung der Berufsfreiheit rechtfertigen kann. Der Finanzbedarf des Staates ist auf andere Weise zu decken. (BVerfGE Beschluss vom 19.07.2000 – 1BvR 539/96).

Eignung

Die Bestimmung der Bundesdruckerei als alleiniger Lieferant der in Rede stehenden Geräte ist zur Erreichung des oben genannten legitimen Zieles

nicht ungeeignet, jedenfalls sofern die Bundesdruckerei die technischen Fähigkeiten hat oder erwirbt, um diese Aufgaben zu bewältigen. Durch die geplante Verfahrensweise ist gewährleistet, dass die Aufnahmen direkt in das IT-System der Ausweisbehörden gelangen und von dort im Wege sicherer Übertragung zur Bundesdruckerei gelangen. Die Bilddateien können nicht in die Hände Dritter kommen und von diesen verfälscht oder geändert werden. Eine solche Möglichkeit würde sich allenfalls durch ein illegales Eindringen in die EDV ergeben. Die Sicherheitssituation verbessert sich eindeutig im Vergleich zu einer Lage, in der fremd gefertigte analoge Bilder von Antragstellern eingeliefert und von der Behörde gescannt werden. Auch das Merkmal der Eignung ist also gegeben.

Erforderlichkeit

Fraglich ist jedoch, ob der Eingriff in dieser Form auch erforderlich zur Zielerreichung ist. Alle 3 privaten Anbieter liefern Systeme, die die Bilddateien auf sicherem Wege direkt in die EDV der Ausweisbehörde einspeisen. Das gilt sowohl für die Fotokabinen als auch für die Small Business Systeme. Aus der Gesetzesbegründung ergibt sich nicht, dass im gegenwärtigen System Sicherheitsmängel vorhanden sind, die die Übertragung der Aufgabe an einen einzigen, und zwar staatlichen Lieferanten erforderlich machen.

Die gegenwärtig verfügbaren Systeme erfüllen die Anforderungen, die sich aus Gesetzen, Verordnungen und Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik ergeben; teilweise gehen sie sogar darüber hinaus. Die Hersteller haben ihre Systeme in der Vergangenheit stetig weiterentwickelt. Sie werden dies auch in Zukunft tun und dabei die einschlägigen Anforderungen erfüllen sowie aus Eigeninteresse die Sicherheit ihrer Systeme weiter verbessern.

Es waren die Privatanbieter, die die Systeme, die jetzt Stand der Technik sind entwickelt und implementiert haben. Dies ist ohne staatlichen Auftrag erfolgt, lediglich aufgrund der Dynamik des Marktes. Der gegenwärtige hohe Sicherheitsstandard ist also allein auf dem Markt entstanden. Es ist nicht

ersichtlich, weshalb es in Zukunft der Fälschungssicherheit von Ausweisdokumenten förderlich wäre, wenn der Mechanismus ausgeschaltet würde, der in der Vergangenheit in der Lage war, kostengünstig die neuen Sicherheitsstandards zu entwickeln und zu implementieren.

Ein Sicherheitsgewinn besteht lediglich in dem Ausschluss selbst beschaffter analoger Aufnahmen. Soweit das Gesetz eine solche Einschränkung trifft, ist die Erforderlichkeit und Eignung zur Erreichung des legitimen Zieles Dokumentensicherheit gegeben. Dazu ist aber ein Ausschluss der bisherigen Anbieter weder erforderlich noch geeignet. § 1 Abs. 5 PassG und § 3 Abs. 4 PersonalausweisG sind daher nicht mit Art. 12 GG vereinbar.

Verhältnismäßigkeit

Der Eingriff ist zudem unverhältnismäßig. Es entspricht auch nicht dem Grundsatz der Verhältnismäßigkeit, den freien Markt auf diesem Teilgebiet abzuschaffen und ein (staatliches) Monopol zu errichten. Die privatwirtschaftliche Verfasstheit hat sich in der Vergangenheit als technisch innovativ und wirtschaftlich günstig erwiesen. Innovationen sind nicht aufgrund von Vorgaben der Sicherheitsbehörden entstanden sondern durch die Dynamik des Marktes. Auch die möglichen Probleme auf Grund der verschiedenen Schnittstellen sind gelöst, es ist nicht ersichtlich, dass es hierbei zu irgendwelchen Problemen kommt. Die Software der Ausweisbehörde ist bereits auf eine Umstellung vorbereitet, sofern die Behörde auf Grund einer Neuausschreibung den Anbieter wechselt.

Dabei hat sich diese Lösung auch als wirtschaftlich vorteilhaft erwiesen. Das Bundesinnenministerium rechnet mit einer Gebührenerhöhung um 6 € pro Ausweisdokument durch die von ihm beabsichtigten Änderungen. Diese Erhöhungen kämen allein dem Anbieter Bundesdruckerei zugute. Die Miet- oder Pachtzahlungen der Aufsteller an die Kommunen würden wegfallen.

Im Ergebnis würde also ein funktionierendes System ohne bekannte Sicherheitsmängel ersetzt durch ein erst zu entwickelndes System, das nach den Ausführungen der Gesetzesbegründung und des Ministeriums nichts bieten soll, was in den Systemen der privaten Anbieter nicht bereits

vorhanden ist, aber zusätzliche Kosten für Kommunen und Bürger verursachen würde. Dem Grundsatz der Verhältnismäßigkeit entspricht nicht, ein funktionierendes System zu ersetzen durch ein anderes System, dessen Qualität nicht höher ist, dass aber kostenintensiver ist.

Ergebnis:

Die gesetzliche Bestimmung, gemäß der ausschließlich die Bundesdruckerei Lieferant von Geräten zur Aufnahme und elektronischen Erfassung von Lichtbildern sein soll, ist mit Art. 12 des Grundgesetzes nicht vereinbar.

2.2. Dienstleistungsrichtlinie

Die Richtlinie 2006/123/EG (EU-Richtlinie über Dienstleistungen im Binnenmarkt) über Dienstleistungen im Binnenmarkt vom 12.12.2006 zielt ab auf die Verwirklichung des Europäischen Binnenmarkts.

Im Rahmen der Normprüfung haben die verpflichteten öffentlich-rechtlichen Institutionen die Vereinbarkeit des Rechts mit den Vorgaben der Richtlinie zu überprüfen.

Art.15 („zu prüfende Anforderungen“) der Richtlinie sieht u. a. vor:

„(3) Die Mitgliedstaaten prüfen, ob die in Absatz 2 genannten Anforderungen folgende Bedingungen erfüllen:

a) Nicht-Diskriminierung: die Anforderungen dürfen weder eine direkte noch eine indirekte Diskriminierung aufgrund der Staatsangehörigkeit oder – bei Gesellschaften – aufgrund des Orts des satzungsmäßigen Sitzes darstellen;

b) Erforderlichkeit: die Anforderungen müssen durch einen zwingenden Grund des Allgemeininteresses gerechtfertigt sein;

c) Verhältnismäßigkeit: die Anforderungen müssen zur Verwirklichung des mit ihnen verfolgten Ziels geeignet sein; sie dürfen nicht über das hinausgehen, was zur Erreichung dieses Ziels erforderlich ist; diese Anforderungen können nicht durch andere weniger einschneidende Maßnahmen ersetzt werden, die zum selben Ergebnis führen."

Der EuGH hatte 2018 (Urteil vom 07.11.2018, Az.: C-171/17) über ein nationales mobiles Zahlungssystem durch ein vom ungarischen Staat kontrolliertes Unternehmen zu entscheiden. Der Gerichtshof weist darauf hin, dass das in Rede stehende mobile Zahlungssytem eine „Anforderung" im Sinne der Richtlinie darstellt, da es den Zugang zur Erbringung mobiler Zahlungsdienste einem staatlichen Monopol vorbehält. Eine solche „Anforderung" muss jedoch mit den in der Richtlinie genannten kumulativen Bedingungen der Nicht-Diskriminierung, der Erforderlichkeit und der Verhältnismäßigkeit vereinbar sein.

Das in Frage stehende nationale System erfüllt nach Auffassung des Gerichts nicht die Bedingung der Verhältnismäßigkeit, denn es gäbe Maßnahmen, die weniger einschneidend seien und die Niederlassungsfreiheit weniger beschränkten als die streitigen Maßnahmen. Mit diesen könnten die von dem Mitgliedsstaat verfolgten Ziele, die u.a. im Verbraucherschutz durch eine Verbesserung des Funktionierens des Markts für mobile Zahlungssysteme bestünden, in gleicher Weise erreicht werden. So könnte ein Konzessionssystem, das auf einem für den Wettbewerb offenen Verfahren beruht, eine weniger einschränkende Maßnahme sein.

Der vom EuGH entschiedene Fall lässt sich unschwer auf den in Rede stehenden GE übertragen. Ein funktionierendes privatwirtschaftliches System wird grundlos ersetzt durch ein staatliches Monopolunternehmen, dessen besondere Sachkunde nicht ersichtlich ist und nicht erläutert wird und dessen Beitrag für ein Mehr an Sicherheit unklar bleibt. Die Schaffung eines solchen Monopols ist weder erforderlich noch verhältnismäßig.

Ergebnis: Es verstößt gegen die EU-Dienstleistungsrichlinie, gesetzlich ausschließlich die Bundesdruckerei als Lieferant von Geräten zur

Aufnahme und elektronischen Erfassung von Lichtbildern zu bestimmen

2.3. Verletzung des Rechtsstaatsprinzips

Nach der Begründung des GE soll die Bundesdruckerei der Lieferant von „Geräten zur Aufnahme und elektronischen Erfassung von Lichtbildern“ sein. Dies ergibt sich nur aus der Begründung des GE, nicht jedoch aus den Texten der §§ 1 Abs. 5 PassG, 4 Abs 3 PersonalausweisG. Eine wortgetreue Interpretation dieser Ausführungen führt zu der Feststellung, dass der Entwurf offenbar meint, dem BMI solle die Kompetenz zur Bestimmung der Lieferanten übertragen werden, um die Fälschungssicherheit der Ausweisdokumente zu erhöhen. Diese Argumentation ist in keiner Weise plausibel: Die bloße Veränderung von Zuständigkeiten verändert Zuständigkeiten und hat zunächst nichts mit Sicherheit zu tun. Wenn B statt A zuständig wird, ändert sich nur, dass nunmehr B zuständig ist, es sei denn, B wird aufgegeben, Geräte mit ganz bestimmten Eigenschaften zu liefern, die A nicht und nur B liefern kann.

Das skizzierte Problem berührt den Grundsatz der Rechtstaatlichkeit gemäß Art. 20 Abs. 3 GG. Gemäß dem allgemeinen Vorbehalt des Gesetzes muss der Gesetzgeber „in grundlegenden normativen Bereichen alle wesentlichen Entscheidungen selbst treffen“ (BVerfG, Beschluss vom 26.06.1991 – 1 BvR 779/85). Wesentliche Entscheidungen darf das Parlament „nicht anderen Normgebern überlassen“ (BVerfGE Urteil vom 08.04.1997 – 1 BvR 48/94). Es ist evident, dass mit dem GE dem Gesetzgeber angesonnen wird, nur sehr eingeschränkt zu entscheiden. Alle relevanten Fragen, wie und wer die Geräte herstellt, wo und wie sie hergestellt werden, wer die Software entwickelt, wie für Weiterentwicklung gesorgt, wie von wem die Betreuung der Geräte vor Ort gewährleistet wird, durch was ein mehr an Sicherheit garantiert ist, bleiben ungeklärt; sie werden nicht einmal erwähnt. Nicht thematisiert wird auch, warum es für Berufsfotografen und für eine Antragstellung beim Auswärtigen Amt Ausnahmen gibt und warum hier Sicherheit offenbar weniger wichtig ist.

Der Vorbehalt des Gesetzes betrifft „nicht nur die Frage, ob ein bestimmter Gegenstand überhaupt gesetzlich geregelt sein muss, sondern auch, wie weit diese Regelungen im Einzelnen zu gehen haben“ (BVerfGE Urteil vom 06.07.1999 – 2 BvF 3/90). Das förmliche Gesetz muss in diesem Sinne ausreichend bestimmt und genau sein.

Die vom BVerfG geforderte Bestimmtheit ist nicht ansatzweise gegeben. Die Bundesdruckerei ist im Normtext nicht einmal erwähnt. Was sie leisten soll, um Sicherheit zu gewährleisten, wird in keiner Weise expliziert.

Ergebnis: Indem der GE behauptet, mehr Sicherheit im Bereich der Personaldokumente zu schaffen, es aber unterlässt, dies zu begründen bzw. Maßnahmen, durch die mehr Sicherheit garantiert werden kann, nicht nennen kann, wird das Rechtsstaatsprinzip gemäß Art. 20 Abs. 3 GG verletzt.

Der Gesetzentwurf zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen verletzt die in Art. 12 GG geschützte Berufsfreiheit sowie das in Art. 20 Abs. 3 GG verankerte Rechtsstaatsprinzip und die Europäische Dienstleistungsrichtlinie in einer Weise, dass Zweifel ausgeschlossen sind. Deswegen mag dahinstehen, ob der GE im Übrigen noch unter anderen Gesichtspunkten rechtlich angreifbar ist.

Bielefeld, 18.10.2020

Dr. Uwe Günther, Rechtsanwalt
Hartmut Geil, Rechtsanwalt

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)613 B

digitalcourage

Stellungnahme zum Entwurf eines Gesetzes zur Stärkung der Sicherheit im Pass- und Ausweiswesen

22.10.2020

Zusammenfassung: Digitalcourage rät unter dem Schlagwort **#PersoOhneFinger** Bürgerinnen und Bürgern, bis **2. August 2021** Personalausweise ohne gespeicherte Fingerabdrücke zu beantragen. Denn nach Einschätzung von Digitalcourage ist die ab dann **geplante Pflicht zur Speicherung von beiden Zeigefinger-Abdrücken** auf neuen Personalausweisen unverhältnismäßig und verstößt gegen das deutsche Grundgesetz sowie gegen die EU-Grundrechtecharta. **Digitalcourage hält eine gerichtliche Überprüfung der geplanten Regelung für unausweichlich.** Die folgende Stellungnahme begründet diese Einschätzung.

Inhalt

Hauptkritikpunkte:

- Die geplante Pflicht kommt einem Generalverdacht gegen Bürgerinnen und Bürger gleich.
- Die seltenen Einzellfällen zeitlich schnellere Überprüfung der Identität einer Person steht in keinem Verhältnis zu einer anlasslosen generellen Fingerabdruck-Pflicht.
- Personalausweise haben andere Funktionen als Reisepässe.
- Es existieren bessere Alternativen, die nicht geprüft wurden.

1. Der Gesetzentwurf und Kritik von Digitalcourage

Am 3. Juni 2020 hat die Bundesregierung einen **Gesetzesentwurf zur Stärkung der Sicherheit im Pass- und Ausweiswesen**[1] beschlossen und dem Bundestag zur Beratung[2] und Verabschiedung zugeleitet. Der Gesetzentwurf verfolgt mit mehreren geplanten Regelungen *„das Ziel, die öffentliche Sicherheit und die Bürgerfreundlichkeit von Verwaltungsdienstleistungen zu stärken“*. Grundlage für die geplante generelle und anlasslose **Pflicht zur Speicherung von zwei Fingerabdrücken** im Speichermedium des Personalausweises ist die 2019 beschlossene EU-Verordnung 2019/1157 [3]. Praktisch bedeutet die Verordnung: Bis zu 370 Millionen Bürgerinnen und Bürger der Europäischen Union[4] müssen in den nächsten Jahren zwangsweise zwei Fingerabdrücke in Personalausweisen speichern lassen. Derzeit ist die Speicherung von Fingerabdrücken auf Personalausweisen freiwillig.

Mit dem Gesetzentwurf soll das deutsche Personalausweisgesetz an die EU-Verordnung angepasst werden. Demnach sollen **ab 2. August 2021 auf den Speichermedien aller neu ausgestellten Personalausweise die Abdrücke des linken und rechten Zeigefingers in Form einer Bilddatei gespeichert** werden:

> „Das Personalausweisgesetz wird entsprechend der Vorgabe aus Artikel 3 Absatz 5 Satz 1 VO (EU) Nr. 2019/1157 so gefasst, dass die Speicherung von zwei Fingerabdrücken im Speichermedium des Personalausweises künftig verpflichtend ist.“ (im Entwurf: B. Lösung; Nutzen, Nr. 7)

Digitalcourage hat am 30. Juli 2020 unter dem Schlagwort #PersoOhneFinger begonnen, Bürgerinnen und Bürger über die geplante Pflicht zur Abgabe von Fingerabdrücken zu informieren[5] und darauf folgend eine Petition[6] gestartet, mit der bereits um 10.000 Menschen ihre Ablehnung der Pflicht zur Speicherung von Fingerabdrücken ausgedrückt haben. Bereits im März 2019 haben die Grundrechteorganisationen Digitalcourage, Privacy International (UK), Homo Digitalis (EL), ApTi (RO) und Statewatch (UK) einen offenen Brief[7] gegen die geplante Fingerabdruck-Pflicht veröffentlicht.

Digitalcourage rät allen Bürgerinnen und Bürgern, die die Pflicht zur Speicherung von zwei Fingerabdrücken ablehnen und einen Personalausweis ohne Fingerabdrücke bevorzugen, bis 2. August 2021 ein fingerabdruckfreies Dokument zu beantragen[8]. Mit Sorge musste Digitalcourage im Zuge von #PersoOhneFinger feststellen, dass ausstellende Behörden

---

1 https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/gesetz-zur-staerkung-der-sicherheit-im-pass-und-ausweiswesen.html im Bundesrat: https://www.bundesrat.de/bv.html?id=0435-20

2 Protokoll der 1. Lesung am 10. September 2020 – zu Protokoll gegebene Reden mit längeren Passagen zur Fingerabdruck-Pflicht siehe Anlage 9: https://dipbt.bundestag.de/doc/btp/19/19173.pdf#IVZd70

3 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32019R1157

4 https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_de.pdf

5 deutsch: https://digitalcourage.de/blog/2020/keine-fingerabdruecke-personalausweis-persoohnefinger englisch: https://digitalcourage.de/blog/2020/no-fingerprinting-for-id-cards

6 https://aktion.digitalcourage.de/perso-ohne-finger

7 https://digitalcourage.de/sites/default/files/2020-10/eu-id-cards-fingerprinting-open-letter.pdf

offenbar trotz der aktuell geltenden freiwilligen Speicherung von Fingerabdrücken bereits jetzt auf der Abgabe von Fingerabdrücken bestehen[9].

2. Fingerabdruck-Pflicht ist unverhältnismäßig

Angesichts des Problems der Identitätsprüfung in seltenen Einzelfällen, das mit der geplanten Fingerabdruck-Pflicht gelöst werden soll, bewertet Digitalcourage die vorgeschlagene Lösung einer anlasslosen und generellen Fingerabdruck-Pflicht als unverhältnismäßig, weil 1. zur geplanten Pflicht mildere Mittel zur Verfügung stehen (Erforderlichkeit, siehe Alternativen zur geplanten Fingerabdruck-Pflicht) und 2. die Schwere des Grundrechtseingriffs nicht im Verhältnis zum verfolgten Zweck steht (Angemessenheit). Digitalcourage teilt die Einschätzung des Netzwerks Datenschutzexpertise:

> Solche Regelungen müssen verhältnismäßig sein, um zu vermeiden, dass eine unangemessene Überwachungsinfrastruktur aufgebaut wird und um sicherzustellen, dass die Regelungen einer verfassungsrechtlichen Prüfung standhalten. Das Netzwerk Datenschutzexpertise bezweifelt, dass diesen Anforderungen genügt wird. (Dr. Thilo Weichert, Stellungnahme des Netzwerk Datenschutzexpertise vom 12.10.2020)

Artikel 52 (1) der Charta der Grundrechte erlaubt jegliche Verletzung von Grundrechten nur, *„wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen“*[10].

Nach Ansicht von Digitalcourage konnte nicht nachgewiesen werden, dass die vorgeschlagene Speicherpflicht von zwei Fingerabdrücken in Personalausweisen notwendig oder verhältnismäßig ist. Die Europäische Kommission empfahl in ihrer eigenen Folgenabschätzung gegenteilig, dass der Ausschluss der verpflichtenden Abnahme von Fingerabdrücken die **„effizienteste und verhältnismäßigste“** politische Option sei.

> Given the key objective to improve the security of ID cards as travel documents, a mandatory RFID chip including biometrics (facial image mandatory, fingerprints optional) is proposed[11]

Die Agentur der Europäischen Union für Grundrechte kommt in ihrer Einschätzung (FRA Opinion – 3/2018 [Security features ID][12]) zu folgender Schlussfolgerung:

---

8 mehr Informationen unter #PersoOhneFinger und: https://digitalcourage.de/blog/2020/keine-fingerabdruecke-personalausweis-persoohnefinger

9 https://twitter.com/digitalcourage/status/1291726405278011393 auch https://twitter.com/KeyEmCh/status/1291992934464851969 auch https://twitter.com/nelsonrr/status/1293165225856901120

10 https://dejure.org/gesetze/GRCh/52.html

11 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0110&from=EN

12 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-biometric-data-id-cards-03-2018_en.pdf

> Für Personalausweise, (…), enthält die Folgenabschätzung [der EU Kommission] keine ausreichende Begründung für die obligatorische Erfassung von Gesichtsbildern und Fingerabdrücken. Tatsächlich kommt sie zu dem Schluss, dass das Ziel mit weniger invasiven Mitteln erreicht werden könnte, nämlich indem nur die obligatorische Erfassung von Gesichtsbildern verlangt wird, während die Erfassung von Fingerabdrücken fakultativ bleibt. (FRA Opinion – 3/2018 [Security features ID] S. 20, eigene Übersetzung)

Die Regierungen der Slowakei und Tschechien haben im Rat der Europäischen Union gegen die Verordnung gestimmt. Die tschechische Regierung hat die verpflichtende Abgabe für alle Menschen als unverhältnismäßig bewertet[13]:

> Statement by the Czech Republic „The Czech Republic appreciates the development that has been made in improving the level of security of identity cards issued to Union citizens and residence documents issued to their family members. However, we cannot agree with the mandatory introduction of biometric data in identity cards and, therefore, cannot support the proposal for a regulation as it stands now. The Czech Republic could only take the opposite view if biometric data (and specifically fingerprints) were included in identity cards on a voluntary basis only. From the data protection perspective, obligatory storage of biometric data in identity cards is a very sensitive issue for the Czech Republic as the majority of the population is obliged to hold an identity card. Since only half of the Member States require their citizens to hold an identity card, the Czech Republic considers the proposal for a regulation to be disproportionate."

2.1. Nicht notwendig gegen Manipulation und Fälschung

Der Entwurf eines Gesetzes zur Stärkung der Sicherheit im Pass- und Ausweiswesen nennt in direktem Zusammenhang mit der geplanten Fingerabdruck-Pflicht kein **konkretes Problem, dass die geplante Fingerabdruck-Pflicht lösen soll**. Insgesamt soll das Gesetz unter anderem das Problem des sogenannten **„Morphing"** lösen (eine Bildbearbeitungstechnik, bei der mehrere Gesichtsbilder zu einem einzigen Gesamtbild verschmolzen werden, das die Züge der eingesetzten Gesichter in sich vereinigt). Den Problemen der

> *„Manipulationen bei der Passbeantragung und anschließenden unerlaubten Grenzübertritten wird künftig dadurch entgegengewirkt, dass das Passbild ausschließlich digital zu erstellen und zu übermitteln ist."* (siehe Entwurf: B. Lösung; Nutzen 1.)

Ein Zusammenhang zwischen der gewünschten Manipulations-, Reproduktions- und Fälschungssicherheit und der geplanten Fingerabdruck-Pflicht ist nicht zu erkennen. Hierfür wäre unserer Einschätzung nach beispielsweise die Einführung eines weiteren privatsphärefreundlichen optischen Sicherheitsmerksmals[14] zielführender. Wie der Chaos Computer Club bereits 2008 demonstrierte[15], können sich unautorisierte Dritte vergleichsweise einfach Zugang zu Fingerabdrücken fremder Personen verschaffen und diese

13 https://www.votewatch.eu/en/term9-regulation-of-the-european-parliament-and-of-the-council-on-strengthening-the-security-of-identity-c.html

14 siehe: optisch variable Zeichen (OVD) bzw. diffractive optically variable image devices (DOVID)

15 https://www.ccc.de/en/updates/2008/schaubles-finger

digitalisieren und reproduzieren. CCC-Sprecher Dirk Engling erklärte damals zum Reisepass, aus unserer Sicht auch für den Personalausweis zutreffend:

> „Fingerabdruck-Biometrie ist nicht so sicher, wie die Politik beteuert. Sie gehört in keine sicherheitsrelevante Anwendung – und erst recht nicht in den ePass."

2.2. Nicht nachvollziehbar: Sicherheit und Bürgerfreundlichkeit

Aus Sicht von Digitalcourage ist nicht nachvollziehbar, wie eine allgemeine Pflicht zur Speicherung von zwei Fingerabdrücken auf Personalausweisen die öffentliche Sicherheit und die Bürgerfreundlichkeit von Verwaltungsdienstleistungen stärken soll. **Von einer Fingerabdruck-Pflicht werden fast ausschließlich rechtstreu lebende Bürgerinnen und Bürger betroffen sein, die in keiner Weise eine Bedrohung für die öffentliche Sicherheit darstellen.** Insofern ist die Breitenwirkung der geplanten Regelung unverhältnismäßig. Aus Sicht von Digitalcourage ist auch nicht nachvollziehbar, wie durch die Fingerabdruck-Pflicht die Bürgerfreundlichkeit von Verwaltungsdienstleistungen gestärkt werden soll. Dieses Ziel ist näher zu erläutern.

In einer Kleinen Anfrage[16] der Abgeordneten Ulla Jelpke u. a. und der Fraktion DIE LINKE wurde die Bundesregierung unter Frage 6 gefragt:

> Inwiefern ist aus Sicht der Bundesregierung die Pflicht zur Abgabe von Fingerabdrücken in Personalausweisen ein verhältnismäßiger Eingriff in die Grundrechte der betroffenen Unionsbürgerinnen und Unionsbürger?

Die Antwort der Bundesregierung lautet:

> Die Speicherung des Fingerabdruckes in Identitätsdokumenten dient dem Zweck, bei Zweifeln an der Übereinstimmung der sich ausweisenden mit der auf dem Lichtbild des Dokuments abgebildeten Person die Identität dennoch unmittelbar feststellen zu können. Die derzeit in Zweifelsfällen noch teilweise notwendigen und zeitaufwändigen Nachfragen bei anderen Behörden können damit künftig entfallen.

Nach Ansicht von Digitalcourage bewertet die Bundesregierung die anlasslose Fingerabdruck-Pflicht von Millionen von Bürgerinnen und Bürgern als verhältnismäßig, weil sie in seltenen Einzelfällen einige Stunden Zeit einsparen kann. Angesichts des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung durch die **Pflicht zur digitalen Erfassung hochsensibler[17] biometrischer Körperdaten** kann mit einer unkonkret bezifferten Zeitersparnis keine Verhältnismäßigkeit für die geplante Regelung belegt werden. Der Hinweis auf zeitintensive Überprüfungsverfahren wäre Anlass, um gesetzgeberisch nach Lösungen zu suchen, um die derzeit geläufigen Verfahren zur Klärung der Identität einer Person im

16 Drucksache 19/21789; Antwort: 19/22133, zu finden via: https://dipbt.bundestag.de/dip21.web/bt

17 EDPS: „Gemäß dem EU-Rechtsrahmen, sowie dem modernisierten Übereinkommen Nr. 108, gelten biometrische Daten als sensible Daten und unterliegen besonderem Schutz. Der EDSB unterstreicht, dass sowohl Gesichtsbilder als auch Fingerabdrücke, die nach dem Vorschlag verarbeitet würden, eindeutig in die Kategorie sensibler Daten fallen würden." https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_de_0.pdf

seltenen Zweifelsfall zu optimieren (siehe weiter unten: „Alternativen zur Fingerabdruck-Pflicht“). Weiter lautet die Antwort der Bundesregierung:

> Zudem wird der betroffenen Person eine direkte Wiederinanspruchnahme ihrer vollen Freizügigkeit ermöglicht.

Im Bezug auf das Problem, dass in **Einzelfällen** beispielsweise bei Identitätsfeststellungen etwa an einer Grenze einzelne Personen unter Umständen stundenweise nicht weiterreisen können, bewertet Digitalcourage die Lösung, nämlich eine **anlasslose, massenhafte Pflicht** zur Digitalisierung und Speicherung hochsensibler biometrischer Daten als klar **unverhältnismäßig**. Die Unionsbürgerschaft verleiht allen Bürgerinnen und Bürgern der Europäischen Union das Recht auf Freizügigkeit vorbehaltlich bestimmter Beschränkungen und Bedingungen. Eine in Einzelfällen notwendige zeitliche Beschränkung ist nach Ansicht von Digitalcourage verhältnismäßig. Weiter lautet die Antwort der Bundesregierung:

> Der staatliche Schutz der Identität der Bürgerinnen und Bürger umfasst auch, den Identitätsmissbrauch mit staatlichen Ausweisdokumenten wirksam einzudämmen.

Aus Sicht von Digitalcourage ist dieser Punkt nicht belegbar. Die von der Bundesdruckerei herausgegebenen Personalausweise bieten durch zahlreiche datenschutzfreundliche technische Sicherheitsmerkmale sehr hohe Hürden vor Fälschung und Manipulation. Die **Zahl von ge- oder verfälschten Identitäts-Dokumenten ist gering und teilweise rückläufig**. Das bestätigen Zahlen[18] der EU-Grenzagentur Frontex:

> In 2019, over 7 000 fraudulent document users were detected at the EU’s external borders (entry/exit/transit), 5% fewer than in 2018. (Frontext-Risiko-Analyse 2020, mehr dazu siehe Fußnote 18)

Zum Vergleich: In Antwort auf Frage 13 zitiert die Bundesregierung die Polizeiliche Eingangsstatistik der Bundespolizei (PES). Im Zeitraum von 2010 bis 2019 wurden laut dieser **jährlich im Schnitt 360 deutsche ge- oder verfälschte Grenzübertrittsdokumente** erfasst, darunter aber nicht nur Personalausweise, sondern auch Reisepässe, Aufenthaltstitel und Visa. In den Jahren von 2010 bis 2019 wurden **jährlich zwischen 38 und 83 ver- und gefälschte ID-Karten** erfasst. Ob hierunter u.a. auch Duldungsdokumente fallen, ist nicht ausgeführt. Sowohl die Zahlen von Frontex, als auch die PES deuten insgesamt auf **Einzelfälle hin, die keine anlasslose generelle Fingerabdruck-Pflicht begründen können.** Als konkret herausgestelltes Problem nennt die Antwort das sogenannte *„Morphing“* (Erklärung siehe oben), wobei hier eine Zunahme der registrierten Fälle zu verzeichnen ist (2014: 434; 2015: 455; 2016: 598; 2017: 708; 2018; 727; 01-11 2019: 950), denen mit der geplanten Regelung zur Erstellung von Lichtbildern laut hier diskutiertem Gesetzentwurf entgegnet werden soll. Für weiterhin verbleibende Einzellfälle empfiehlt Digitalcourage u.a. Alternative 4.1.

---

18 https://frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/Annual_Risk_Analysis_2020.pdf siehe S. 28; die Frontex-Risiko-Analyse 2018 zeigt, dass deutsche Personalausweise im Vergleich selten gefälscht werden: https://frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/Risk_Analysis_for_2018.pdf S. 22, dort auch: „In 2017, Member States reported a total of about 6 700 persons from third-countries presenting themselves with fraudulent documents at BCPs on entry to the EU/Schengen area, the lowest number of detections since 2013, despite the in-creasing regular passenger flows.“

Weiter lautet die Antwort der Bundesregierung:

> Ein milderes Mittel, das Unionsbürgerinnen und Unionsbürger gleichermaßen schnell und sicher identifiziert und ihnen zugleich die zügige Wiederinanspruchnahme ihrer vollen Freizügigkeit ermöglicht, steht im Ausweiswesen nicht zur Verfügung.

Digitalcourage kann nicht nachvollziehen, warum die Bundesregierung an dieser Stelle nicht die alternativen Vorschläge des Europäischen Datenschutzbeauftragten[19] nennt. Aus Sicht von Digitalcourage ist der Eindruck, es gäbe keine **milderen Alternativen**, schlicht falsch, siehe unsere Vorschläge unten. Weiter lautet die Antwort der Bundesregierung:

> Für Reisepässe hat der europäische Gesetzgeber bereits im Jahr 2004 eine vergleichbare Regelung getroffen. Die Verordnung (EU) 2019/1157 weitet dies nunmehr auch auf Personalausweise aus, welche innerhalb der EU und zu ausgewählten Nachbarstaaten ebenfalls als Reisedokument dienen.

Digitalcourage erinnert, dass **Reisepässe und Personalausweise grundsätzlich verschiedene Dokumente** sind (insbesondere mit Blick auf die sehr unterschiedlichen praktischen Verwendungszwecke durch Behörden, Bürgerinnen und Bürger und private Stellen, siehe dazu auch S. 2 Drucksache 19/22133[20] sowie[21]) und eine bestehende Fingerabdruck-Pflicht des einen Dokuments keine Fingerabdruck-Pflicht des anderen Dokuments begründet. Das Gegenteil ist der Fall: Im Sinne einer **Überwachungsgesamtrechnung**[22], also der Gesamtbetrachtung aller Maßnahmen zur Erfassung persönlicher Daten von Bürgerinnen und Bürgern und im Sinne des **Grundsatzes der Datensparsamkeit**, und angesichts der Tatsache, dass Reisepässe und Personalausweise in der Praxis unterschiedlich genutzt werden, begründet die existierende Fingerabdruck-Pflicht in Reisepässen die Freiwilligkeit von Fingerabdrücken in Personalausweisen. Vor diesem Hintergrund erscheint Digitalcourage die vom Bundesdatenschutzbeauftragten Ulrich Kelber im Juni 2019 aufgeworfene Überlegung eines sogenannten **Sicherheitsgesetz-Moratoriums**[23] im Sinne einer überprüfenden Inventur von Sicherheitsgesetzen, die Grundrechte von Bürgerinnen und Bürgern immer weiter beschränken, ein notwendiger Schritt zu sein.
Darüber hinaus ist unserer Einschätzung nach auch die Fingerabdruck-Pflicht in Reisepässen grundrechtlich fragwürdig[24].

---

19 https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_de_0.pdf

20 https://dip21.bundestag.de/dip21/btd/19/221/1922133.pdf

21 „National identity cards, unlike passports, are not primarily used for crossing the external border." Einschätzung der Agentur der Europäischen Union für Grundrechte https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-biometric-data-id-cards-03-2018_en.pdf sowie darin Fußnote 45: Also the Commission pointed out in the Impact Assessment that "ID cards serve more purposes than crossing the border"

22 https://digitalcourage.de/ueberwachungsgesamtrechnung/einfuehrung

23 https://www.bundestag.de/presse/hib/649640-649640

24 siehe Vorlagefrage und Rechtfertigung in der Rechtssache C-291/12, Michael Schwarz gegen Stadt Bochum: http://curia.europa.eu/juris/document/document.jsf?text=&docid=143189&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=10055974

> Although the lawfulness of storing such data in passports was confirmed by the CJEU in Schwarz, it should be borne in mind that the Court assessed the proportionality of limiting the right to respect for private and family life and the right to data protection against the aims of preventing falsification and fraudulent use of passports and, by extension, the objective of preventing irregular entry into the EU.

2.3. Nicht wirksam gegen Terrorismus und Kriminalität

Begründet wurde die Verordnung (EU) 2019/1157 mit der Bewahrung von Sicherheit, *„insbesondere im Zusammenhang mit Terrorismus und grenzüberschreitender Kriminalität."* (siehe Erwägung Nr. 6) In der oben zitierten Kleinen Anfrage wurde die Bundesregierung unter 14. gefragt:

> In welchen konkreten Fällen von als terroristisch eingestufter Straftaten hat das Nichtvorhandensein gespeicherter Fingerabdrücke auf Personalausweisen sowie anderen Ausweisdokumenten nach Kenntnis der Bundesregierung dazu geführt, dass die Taten nicht verhindert bzw. nicht aufgeklärt und die Täter nicht ermittelt werden konnten?

Die Antwort der Bundesregierung lautet:

> Es sind keine konkreten Fälle von als terroristisch eingestufter Straftaten bekannt, in denen das Nichtvorhandensein gespeicherter Fingerabdrücke auf Personalausweisen sowie anderen Ausweisdokumenten mutmaßlich dazu geführt hätten, dass die Taten nicht verhindert bzw. nicht aufgeklärt und die Täter ermittelt werden konnten.

Digitalcourage hält gezielte Mittel zur Abwehr und Aufklärung für geeignet, nicht aber eine pauschale Fingerabdruck-Pflicht, denn von dieser werden fast ausschließlich rechtstreu lebende Bürgerinnen und Bürger betroffen sein, die in keiner Weise eine Bedrohung für die öffentliche Sicherheit darstellen. Dieselbe Ansicht vertreten wir gegenüber grenzüberschreitender Kriminalität und verweisen auf Zahlen der EU-Grenzagentur Frontex, die den Schluss nahelegen, dass Behörden bei Verdacht auf Fälschungen oder Manipulationen in Dokumenten, die wie der deutsche Personalausweis über ausreichend Sicherheitsmerkmale verfügen, dies zuverlässig erkennen können. Fakt ist, dass nicht alle Dokumente aller EU-Mitgliedsländer[25] über dieselbe technische Qualität von Sicherheitsmerkmalen verfügen. Insofern ist die von der EU-Verordnung beabsichtigte einheitliche Anhebung von Sicherheitsstandards zu begrüßen.
Allerdings hat Digitalcourage starke Zweifel, dass sich mit einer anlasslosen generellen Fingerabdruck-Pflicht, die alle Menschen trifft, Terrorismus und Kriminalität wirksam aufklären oder verhindern lassen. Stattdessen ist eine gezielte Sicherheitsgesetzgebung (siehe 4.6.) erforderlich.

2.4. Langfristige Gefahren für IT-Sicherheit und Privatsphäre

Fingerabdrücke (bzw. Minuzien oder Muster) werden bereits jetzt als Schlüssel beziehungsweise Passwörter für Smartphones (damit Zugang zu Online-Banking, privater

25 https://www.consilium.europa.eu/prado/de/prado-start-page.html

Kommunikation, privaten Dokumenten), Wohnungen[26], Arbeitsplätze oder Automobile[27] verwendet. Aus Sicht von Digitalcourage besteht bei der zukünftigen technischen Entwicklung die Gefahr, dass Fingerabdrücke zukünftig in weitere Verbreitung geraden und Missbrauch und Kriminalität ermöglichen. Vor dem Hintergrund

- der geplanten massenhaften Digitalisierung der Fingerabdrücke aller Bürgerinnen und Bürger,
- der temporären Speicherung bei den ausstellenden Behörden,
- einer möglichen Speicherung in der geplanten Ausweis-App[28] (Bitte Hinweis in der Fußnote beachten),
- des internationalen Zugriffs auf biometrischen Daten[29],
- der quantitativ zunehmenden Speicherung von Fingerabdrücken in internationalen Datenbanken,
- der Vernetzung von Datenbanken[30],
- automatisierter Grenzübergangsstellen[31],
- des internationalen Zugriffs auf Fingerabdruckdaten[32],
- der Zusammenarbeit mit externen Dienstleistern[33]

26 https://www.welt.de/sonderthemen/vernetzte-welten/article134416220/Per-Fingerprint-die-Haustuer-oeffnen.html

27 https://www.golem.de/news/hyundai-fingerabdruck-startet-auto-1812-138409.html

28 Bitte beachten: Bis Fertigstellung dieser Stellungnahme hat Digitalcourage leider keine Antwort erhalten, ob für den geplanten Personalausweis auf Smartphones auch die Fingerabdrücke gespeichert werden oder zukünftig werden sollen. https://news.samsung.com/de/sicher-und-einfach-identifizieren-mit-dem-smartphone

29 VO (EU) 2019/1157 Artikel 11 Absatz 7„Die Mitgliedstaaten halten eine Liste der zuständigen Behörden vor, die Zugang zu den biometrischen Daten haben, die auf dem in Artikel 3 Absatz 5 dieser Verordnung genannten Speichermedium gespeichert sind, und übermitteln diese Liste jährlich der Kommission. Die Kommission veröffentlicht im Internet eine Zusammenstellung dieser nationalen Listen."

30 „Derzeit errichten die Firmen IDEMIA und Sopra Steria für die EU ein biometrischen Erkennungssystem, wozu Fingerabdrücke und Gesichtsbilder aus fünf nationalen Datenbanken in einer Datei zusammengeführt werden und damit eine europaweite Interoperabilität biometrischer Datenbanken erreicht werden soll." (Dr. Thilo Weichert, Stellungnahme des Netzwerk Datenschutzexpertise vom 12.10.2020) auch Monroy, EU zahlt 300 Millionen Euro für Erkennung von Gesichtern und Fingerabdrücken, netzpolitik.org 05.06.2020

31 VO (EU) 2019/1157 Erwägungsgrund 33: „Die für das sichere Speichermedium verwendeten Formate sollten interoperabel sein, und zwar auch mit Blick auf automatisierte Grenzübergangsstellen."

32 VO (EU) 2019/1157 Artikel 3 Absatz 6: „Die Mitgliedstaaten tauschen untereinander die Informationen aus, die für die Authentifizierung des Speichermediums und den Zugriff auf und die Überprüfung der in Absatz 5 genannten biometrischen Datennotwendig sind."

33 VO (EU) 2019/1157 Erwägungsgrund 42 „Die Mitgliedstaaten sollten besondere Vorsicht walten lassen, wenn eine Zusammenarbeit mit einem externen Dienstleistungsanbieter besteht. "

- einer zunehmenden kriminellen Ausnutzung von IT-Sicherheitslücken[34], die nicht geschlossen werden,
- der Tatsache, dass Überwachungs- und Sicherheitsgesetze stetig erweitert und verschärft (schrittweise Erweiterung der Verwendung von Daten, schrittweise Hinzufügung von Datenkategorien, Analysemethoden, Datenverknüpfungen etc.), aber nahezu nie zurückgefahren werden,
- und vor dem Hintergrund weiterhin unzureichend kontrollierbarer Geheimdienste[35]

geht Digitalcourage davon aus, dass die Verfügbarkeit von Fingerabdrücken zukünftig ein **IT-Sicherheits- und Privatsphäreproblem** werden.
Weiterhin verfolgt der Entwurf allgemein das Ziel, *„die öffentliche Sicherheit und die Bürgerfreundlichkeit von Verwaltungsdienstleistungen zu stärken."* (A. Problem und Ziel)

3. Gerichtliche Prüfung notwendig

> Der [Europäische Datenschutzbeauftragte] EDSB unterstreicht, dass sowohl Gesichtsbilder als auch Fingerabdrücke, die nach dem Vorschlag verarbeitet würden, eindeutig in die Kategorie sensibler Daten fallen würden. (...). Dieser breit angelegte Anwendungsbereich sowie die höchst sensiblen Daten, die verarbeitet werden (Gesichtsbilder in Kombination mit Fingerabdrücken), verlangen eine gründliche Prüfung auf der Grundlage einer strengen Prüfung der Notwendigkeit.[36]

Nach Bewertung der einsehbaren Dokumente zu Beratungen des Gesetzesentwurfs in Bundesrat und Bundestag sowie der bisher öffentlich einsehbaren Stellungnahmen muss Digitalcourage feststellen, dass der geplante Eingriff in die Grundrechte der Bürgerinnen und Bürger durch eine generelle und anlasslose Pflicht zur Speicherung von zwei Fingerabdrücken **weder juristisch, technisch noch parlamentarisch ausreichend geprüft und hinterfragt** wurde. Insbesondere liegt unseres Wissens nach **keine ausreichende, systematische Verhältnismäßigkeitsprüfung** vor.

Keine der 15 zur 1. Lesung des Gesetzesentwurfs am 10. September 2020 öffentlich einsehbaren Stellungnahmen[37] zum Gesetzesentwurf kritisierte die geplante Pflicht zur Speicherung von zwei Fingerabdrücken. Die Position der Bundesregierung, vertreten durch den Parlamentarischen Staatssekretär Dr. Günter Krings in der 173. Sitzung des Bundestags am 10. September 2020, lautet:

---

34 Beispiel (Fingerabdruck-Daten waren hier nicht betroffen – ein entsprechendes Szenario ist allerdings realistisch): https://www.br.de/nachrichten/netzwelt/hacker-veroeffentlichen-passdaten-von-12-000-deutschen,SArrtc5 und https://www.tagesschau.de/investigativ/br-recherche/cyberattacke-passdaten-101.html

35 https://www.ccc.de/de/updates/2020/bverfg-geheimdienstkontrolle sowie https://netzpolitik.org/2020/sechs-vorschlaege-fuer-eine-bessere-geheimdienstkontrolle/

36 https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_de_0.pdf

37 https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/gesetz-zur-staerkung-der-sicherheit-im-pass-und-ausweiswesen.html

> Der Gesetzentwurf stärkt aber auch an anderer Stelle die Authentizität des Ausweisdokumentes. Ich will nur einen Punkt herausgreifen, den wir aufgenommen haben in Umsetzung der europäischen Verordnung zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern (...) Verpflichtend wird nun jedoch die Speicherung des Fingerabdrucks im Chip des Personalausweises vorgeschrieben. Das Personalausweisgesetz wollen wir an diese Vorgaben anpassen, weil europäisches Recht natürlich national anzupassen ist. (Plenarprotokoll[38] der 173. Sitzung des Bundestags, Dr. Günter Krings)

Digitalcourage versteht die Position der Bundesregierung so, dass es sich bei der Einführung einer generellen und anlasslosen Pflicht zur Speicherung von zwei Fingerabdrücken auf neuen Personalausweisen **lediglich um eine formale Anpassung des deutschen Rechts an europäisches Recht** handle.

Aus unserer Sicht ist das nicht der Fall:

Vielmehr handelt es sich bei der geplanten Pflicht um eine historische Ausweitung und Verschärfung des Personalausweisgesetzes, der Erfassung und Verarbeitung biometrischer Daten und dem Eingriff in die informationelle Selbstbestimmung aller Bürgerinnen und Bürger. **Deutschland ist laut Vertrag über die Arbeitsweise der EU verpflichtet, die EU-Verordnung umzusetzen, aber natürlich nur, wenn die Verordnung EU-rechtskonform und im Einklang mit der EU-Grundrechtecharta ist. Hieran hat Digitalcourage erhebliche Zweifel.** Zudem existieren Alternativen, die noch nicht geprüft wurden (siehe 4.). Nach Ansicht von Digitalcourage ist die geplante Pflicht einer ausführlichen Datenschutz-, Technik- und Grundrechtefolgenabschätzung[39] sowie einer gerichtlichen Verhältnismäßigkeitsprüfung zu unterziehen.

Aus Sicht von Digitalcourage ist all dies bisher nicht geschehen und muss auf schnellstem Wege nachgeholt werden. Das wirksamste Vorgehen ist zu prüfen, aus Sicht von Digitalcourage sind die folgenden Optionen gegeben:

1. Der **Gesetzgebungsprozess** um die geplante Regelung zu Fingerabdrücken im Entwurf des Gesetzes zur Stärkung der Sicherheit im Pass- und Ausweiswesen **ist auszusetzen**,
   - bis systematisch die Folgen für Datenschutz, Technik und Grundrechte bewertet sind,
   - bis die EU-Verordnung 2019/1157 gerichtlich gegen das Grundgesetz und die EU-Grundrechtecharta geprüft wurde sowie

38 http://dipbt.bundestag.de/doc/btp/19/19173.pdf#lVZd70

39 Der EDSB unterstreicht ferner, dass Artikel35 Absatz10 der Datenschutz-Grundverordnung (im Folgenden „DSGVO“) auf die hier zu prüfende Verarbeitung Anwendung finden würde. In diesem Zusammenhang weist der EDSB darauf hin, dass die Folgenabschätzung zum Vorschlag anscheinend die von der Kommission gewählte Option nicht unterstützt, nämlich die obligatorische Aufnahme sowohl von Gesichtsbildern als auch von (zwei) Fingerabdrücken in Personalausweise (und Aufenthaltsdokumente). Folglich kann nicht davon ausgegangen werden, dass die Folgenabschätzung zum Vorschlag für den Zweck der Einhaltung von Artikel 35 Absatz10 DSGVO genügt. Der EDSB empfiehlt daher, vor diesem Hintergrund die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung biometrischer Daten (Gesichtsbild in Kombination mit Fingerabdrücken) erneut zu prüfen.
https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_de_0.pdf

- bis alle milderen Alternativen zur geplanten Lösung bewertet und öffentlich diskutiert sind.

2. **Sollte der Bundestag die geplante Regelung** zur generellen und anlasslosen Pflicht zur Speicherung von zwei Fingerabdrücken **ablehnen**, kann die Kommission der Europäischen Union nach Art. 258 AEUV ein **Vertragsverletzungsverfahren**[40] vor dem Europäischen Gerichtshof einleiten, wobei die **Frage vorzulegen ist, ob die EU-Verordnung 2019/1157 im Lichte der EU-Grundrechtecharta verhältnismäßig ist**. Dazu wäre Rechtsbehelf mittels **Inzidenter Normenkontrolle** nach Art. 277 AEUV einzuholen:

   „Ungeachtet des Ablaufs der in Artikel 263 Absatz 6 genannten Frist kann jede Partei in einem Rechtsstreit, bei dem die Rechtmäßigkeit eines von einem Organ, einer Einrichtung oder einer sonstigen Stelle der Union erlassenen Rechtsakts mit allgemeiner Geltung angefochten wird, vor dem Gerichtshof der Europäischen Union die Unanwendbarkeit dieses Rechtsakts aus den in Artikel 263 Absatz 2 genannten Gründen geltend machen."

3. **Sollte der Bundestag die geplante Regelung** zur generellen und anlasslosen Pflicht zur Speicherung von zwei Fingerabdrücken **annehmen und das Gesetz in Kraft treten**, muss das entsprechende Gesetz zur Wahrung der Grundrechte der Bürgerinnen und Bürger auf geeigneten **Klagewegen** Gerichten zur Prüfung vorgelegt werden. Letztendlich bedeutet auch dieser Weg eine **Vorlage beim Europäischen Gerichtshof**.
4. Die Bundesregierung kann im Lichte neuer Kritik an der geplanten Regelung in der aktuell laufenden Ratspräsidentschaft die Kommission der Europäischen Union um ein **Aufhebungsgesetz zur EU-Verordnung 2019/1157** ersuchen, unter anderem mit Berufung auf die Folgenabschätzung der EU Kommission[41] und der im Zuge der geplanten Umsezung in deutsches Recht eingegangenen Kritik.

Digitalcourage ist der Ansicht, dass der deutsche Gesetzgeber im Sinne der Wahrung der Grundrechte der Bürgerinnen und Bürger und vor dem Hintergrund geschwächter rechtsstaatlicher Kontrollmechanismen durch strukturell massiv überlastete Verfassungsgerichte den **schnellsten und kostengünstigsten Weg zu einer gerichtlichen Verhältnismäßigkeitsprüfung** verfolgen sollte.

4. Es gibt Alternativen, die zu prüfen sind

Nach Ansicht von Digitalcourage bestehen für die Fingerabdruck-Pflicht mindestens drei Alternativen. Eine systematische und vollständige Erarbeitung von Alternativen hat allerdings, soweit Digitalcourage informiert ist, nicht stattgefunden.

---

40 zum Vergleich, die EU Kommission informierte am 25. Juli 2019: „Vertragsverletzungsverfahren: Kommission leitet in 17 Fällen rechtliche Schritte gegen Deutschland ein (...) Neben der Aufforderung, einem Urteil des Gerichtshofs über Nitrate nachzukommen, ist Deutschland mit weiteren Schritten der Kommission in den Bereichen Umwelt, Digitaler Binnenmarkt, Energie, Binnenmarkt, Justiz und Inneres, Verkehr und Steuern konfrontiert. " https://ec.europa.eu/germany/news/20190725-vertragsverletzungsverfahren_de und am 14. Mai 2020: „Kommission leitet in sechs Fällen rechtliche Schritte gegen Deutschland ein" https://ec.europa.eu/germany/news/20200514-vertragsverletzungsverfahren-deutschland_de

41 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0110&from=EN

4.1. Optimierung des bisherigen Überprüfungsverfahrens

Nach Kenntnis von Digitalcourage werden bisher Identitäten von Personen in seltenen Zweifelsfällen manuell überprüft, beispielsweise durch Anfragen bei anderen Behörden. Voraussetzung dafür ist, dass die Beamt.innen die Identität der betroffenen Person anhand der Daten auf dem Ausweisdokument und anhand des Lichtbilds nicht eindeutig bestimmen können. Dieser Fall wird durch die neuen geplanten Regelungen zur Erstellung und Übermittlung des Lichtbilds zukünftig jedoch ausgeschlossen.

> Als allgemeine Praxis sollten die Mitgliedstaaten zur Überprüfung der Echtheit des Dokuments und der Identität des Inhabers in der Regel vorrangig das Gesichtsbild überprüfen und nur darüber hinaus, falls zur zweifelsfreien Bestätigung der Echtheit des Dokuments und der Identität des Inhabers notwendig, auch die Fingerabdrücke. (EU VO 2019/1157, Erwägungsgrund Nr. 19)

Sollte es dennoch in seltenen Einzelfällen notwendig sein, Identitäten in möglichst kurzer Zeit in Zweifelsfällen zu überprüfen, sind die dazu notwendigen Abläufe zu optimieren. Beispielsweise ist die Erreichbarkeit von auskunftsbefugten Behörden sicherzustellen oder auch die Ausbildung der mit der Aufgabe vertrauten Beamt.innen weiter zu verbessern.

> Diese Verordnung hindert die Mitgliedstaaten nicht daran, für Identifizierungszwecke Dokumente anzuerkennen, bei denen es sich nicht um Reisedokumente handelt, also etwa Führerscheine, sofern das diskriminierungsfrei erfolgt. (EU VO 2019/1157, Erwägungsgrund Nr. 12)

4.2. Minuzien / Muster statt kompletter Fingerabdrücke

In der Stellungnahme 7/2018 des Europäischen Datenschutzbeauftragten (EDSB) zu dem Vorschlag für eine Verordnung zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und anderer Dokumenten[42] empfiehlt der EDPS die Verwendung von Minuzien[43] oder Mustern an Stelle kompletter Bilder von Fingerabdrücken:

> Der EDSB weist darüber hinaus darauf hin, dass nach seinem Verständnis die Speicherung von Fingerabdrücken die Interoperabilität verbessert, dass sie aber gleichzeitig die Menge verarbeiteter biometrischer Daten und das Risiko der Identitätserschleichung bei einer Verletzung des Schutzes personenbezogener Daten erhöht. Der EDSB empfiehlt daher, die im Dokument auf dem Chip gespeicherten Fingerabdruckdaten auf Minuzien oder Muster zu beschränken, also auf eine Untermenge der aus dem Fingerabdruckbild extrahierten Merkmale.

Als Beispiel für den (umstrittenen) Einsatz von Fingerabdruck-Merkmalen statt voller Fingerabdrücke kann offenbar zukünftig das Europäische Parlament dienen, wo ein System zur Aufenthaltskontrolle für Parlamentarier getestet werden soll.[44]

---

42 Zusammenfassung: https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_summary_de.pdf Langfassung: https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_de_0.pdf

43 https://de.wikipedia.org/wiki/Fingerabdruck#Merkmale

4.3. Keine Zeigefinger: Ringfinger / kleiner Finger

> Bei der Umsetzung der europäischen Vorgabe im vorliegenden Entwurf wird zudem der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) und damit der Erforderlichkeitsgrundsatz missachtet: Die in § 5 Abs. 9 PAuswG vorgesehene Speicherung der Fingerabdrücke der Zeigefinger betrifft für jede Hand diejenigen Finger, mit denen am meisten Spuren hinterlassen werden. Statt Fingerabdrücke des Zeigefingers zu verwenden, wären solche des Ringfingers und des kleinen Fingers weniger missbrauchsanfällig, für Identifizierungszwecke aber ebenso geeignet. Wegen des Fehlens europarechtlicher Vorgaben hätte der Gesetzgeber den Spielraum gehabt, insofern eine weniger eingreifende Maßnahme vorzusehen. (Dr. Thilo Weichert, Stellungnahme des Netzwerk Datenschutzexpertise vom 12.10.2020)

4.4. Engere Zweckbindung

Tatsächlich ist die europarechtlich in Art. 11 Abs. 6 der Verordnung vorgegebene strenge Zweckbeschränkung bei der nationalen Umsetzung nicht im vorliegenden Entwurf übernommen werden, obwohl hierzu eine Regelungsbefugnis erteilt wird. (…) Um dem europarechtlichen Zweckbindungsgebot zu entsprechen, sollte daher zumindest folgende zusätzliche Regelung in § 15 PAuswG aufgenommen werden. *„Die Nutzung der biometrischen Ausweisdaten auf Zwecke eines Abgleichs mit elektronischen Dateien, etwa für Fahndungszwecke, ist unzulässig." (Dr. Thilo Weichert, Stellungnahme des Netzwerk Datenschutzexpertise vom 12.10.2020)*

4.5. Reform der Ausweispflicht

Die Anforderungen der EU-Verordnung 2019/1157 sind auch in Ländern erfüllt, in denen Bürgerinnen und Bürger nicht verpflichtet sind, einen Reisepass oder Personalausweis zu besitzen, wie beispielsweise in der Tschechischen Republik. Insofern besteht mit einer Reform der Ausweispflicht eine zu prüfende mildere Alternative. Die Ausweispflicht könnte abgeschafft werden oder Personalausweise könnten ersetzt werden in *„Aufenthaltskarten, die allen im Hoheitsgebiet ansässigen Personen unabhängig von deren Staatsangehörigkeit ausgestellt werden"* um der genannten Verordnung zu entsprechen:

> Diese Verordnung verpflichtet die Mitgliedstaaten nicht, Personalausweise oder Aufenthaltsdokumente einzuführen, wenn diese nach nationalem Recht nicht vorgesehen sind; ebenso wenig berührt sie die Zuständigkeit der Mitgliedstaaten für die Ausstellung anderer Aufenthaltsdokumente nach nationalem Recht, die nicht in den Anwendungsbereich des Unionsrechts fallen, beispielsweise Aufenthaltskarten, die allen im Hoheitsgebiet ansässigen Personen unabhängig von deren Staatsangehörigkeit ausgestellt werden. (Verordnung (EU) 2019/1157) Erwägungsgrund 11)

44 Parliament documents reveal new biometric attendance system: https://www.euractiv.com/section/digital/news/exclusive-parliament-documents-reveal-new-biometric-attendance-system/

4.6. Gezielte Sicherheitsgesetzgebung

An Stelle einer, aus unserer Sicht unverhältnismäßigen, anlasslosen und generellen Fingerabdruck-Pflicht sind Optionen für eine gezielte und grundrechtsfreundliche Sicherheitsgesetzgebung zu prüfen, siehe beispielsweise Alternative 4.1. Voraussetzung dafür ist, dass die Maßnahmen verhältnismäßig sind und ihre Notwendigkeit und Wirkung empirisch nachgewiesen werden kann. Zudem sind im Sinne einer Überwachungsgesamtrechnung (siehe oben) alle Eingriffe in Grundrechte zu kompensieren.

5. Mittel und langfristige Gefahren

5.1. Lebenslange Kontrolle

Ein Fingerabdruck ist ein biometrisches Merkmal, das einen Menschen ein Leben lang kontrollierbar macht. Menschen können, wenn es sein muss, Namen und Wohnort wechseln, um sich beispielsweise vor Verfolgung oder Bedrohung zu schützen. Biometrische Daten wie Fingerabdrücke erlauben das nicht.

> Sie eignen sich als nationale Kennziffern, also als persönliche Zuordnungsmerkmale, da die biometrischen Merkmale einheitlich in einem Staat, ja staatenübergreifend weltweit umfassend verwendet werden können. (Dr. Thilo Weichert, Stellungnahme des Netzwerk Datenschutzexpertise vom 12.10.2020)

5.2. Übergriff statt Schutz

Die anlasslose und massenhafte biometrische Erfassung von Fingerabdrücken ist ein nutzloser und gefährlicher Übergriff des Staats auf die Bevölkerung. Demokratien und Rechtsstaaten haben die Aufgabe, Bürgerinnen und Bürger vor derartigen Übergriffen zu schützen.

5.3. Freiheit wird schrittweise abgeschafft

Überwachungs- und Kontrollmaßnahmen werden stets erweitert und verschärft, aber so gut wie nie zurückgefahren. Ohne politischen Kurswechsel werden in Zukunft immer mehr Arten sensibler Biometriedaten millionenfach erhoben, gespeichert und für alle möglichen Zwecke genutzt.

5.4. Risiko Zugriffserweiterung

In Deutschland dürfen[45] Polizei und Geheimdienste seit 2017 automatisch auf biometrische Passbilder von Personalausweisen zugreifen. Dabei gibt es wenig Kontrolle durch Aufsichtsbehörden. Eine Ausweitung der Zugriffsmöglichkeiten auf die Fingerabdrücke scheint nur eine Frage der Zeit.

45 https://media.offenegesetze.de/bgbl1/2017/bgbl1_2017_46.pdf#page=2

5.5. Kontrollverlust durch Drittstaaten

Durch *„weltweite Interoperabilität – auch bei der Maschinenlesbarkeit und der Sichtprüfung“* (Erwägungsgrund Nr. 23) können die biometrischen Daten auch an Behörden in Staaten, in denen Freiheitsrechte nicht geschützt sind, übermittelt werden. Spätestens hier gibt es keine Kontrolle darüber, wohin die biometrischen Daten der Bürgerinnen und Bürger gelangen.

5.6. Kontrollverlust durch Unternehmen

Bei *„Zusammenarbeit mit einem externen Dienstleistungsanbieter“* (Erwägungsgrund Nr. 42) können auch private Unternehmen Zugriff auf die Daten erhalten, siehe auch Artikel 11 *„Schutz personenbezogener Daten und Haftung“*.

5.7. Kontrollverlust durch Geheimdienste

Nach den Enthüllungen von Edward Snowden haben es die Regierungen der EU-Länder versäumt, die Macht von Geheimdiensten wirksam einzuschränken. Im NSU-Skandal hat der mit einem BigBrotherAward für sein Lebenswerk[46] ausgezeichnete sogenannte deutsche „Verfassungsschutz“ die Aufklärung von Terror behindert. Geheimdienste arbeiten unkontrolliert und grundrechtefeindlich. Es muss davon ausgegangen werden, dass Geheimdienste sich unkontrolliert Zugriff auf die biometrischen Daten der EU-Bürgerinnen und -Bürger verschaffen werden.

5.8. Risiko Datenvernetzung

Bereits jetzt arbeiten „Sicherheits“-Politiker.innen[47] an einer vernetzten, EU-weiten Datenbankstruktur mit Fingerabdrücken, Gesichtsbildern und anderen Biometriedaten[48]. Datenbanken von Verwaltungen, Polizei, Geheimdiensten und Firmen wachsen ständig. (siehe Programme: Next Generation Prüm, Polizei 2020, Ausbau des Visa-Information-Systems oder des Schengener-Informations-Systems SIS II).

5.9. Kinder betroffen

Laut EU-Verordnung werden Kinder ab 6 Jahren erfasst, wobei die einzelnen Regierungen der EU-Ländern die Möglichkeit haben, Kinder bis 12 Jahren von der Pflicht zur Abgabe von Fingerabdrücken zu befreien.

5.10. Illegitim in Demokratien

Ralf Bendrath erläutert in seinem Beitrag „Zur Geschichte der Fingerabdrücke in Ausweisen“[49]:

---

46 https://bigbrotherawards.de/2016/lebenswerk-verfassungsschutz-vs

47 https://digitalcourage.de/sicherheitstheater

48 siehe netzpolitik.org vom 17. Juli 2020 https://netzpolitik.org/2020/bundesregierung-fuer-europaeische-polizeipartnerschaft/ und unseren Artikel https://digitalcourage.de/blog/2019/eu-fingerabdruck-pflicht

49 https://netzpolitik.org/2007/zur-geschichte-der-fingerabdruecke-in-ausweisen/

> *„Ausweise gehen in Deutschland auf die von den Nazis ab 1938 eingeführte „Kennkarte“ zurück, deren Mitführen für Juden zwingend war. (…) In Spanien wurde die Erfassung von Fingerabdrücken für die nationale Identitätskarte, die bis heute gilt, 1940 während der Franco-Diktatur eingeführt. Was nun allen BürgerInnen aufgenötigt wird, steht also ganz klar in der Tradition verbrecherischer Regime.“* In Frankreich nutzte das Vichy-Regime ab 1942 den Eintrag „Jude“ auf Ausweisen für die Deportation von 76.000 Menschen im Holocaust. (mehr dazu auf lto.de vom 22.7.2018: 80 Jahre Ausweispflicht: Wie ein Nazi-Minister den Überwachungsstaat durchsetzte[50])

5.11. Datensicherheit

Die Daten der gespeicherten Fingerabdrücke auf den neuen Personalausweisen können kontaktlos ausgelesen werden. Sicherheitsmaßnahmen für ein Speichermedium, die heute ausreichend erscheinen, können möglicherweise in 10 Jahren überwunden werden. (siehe 2.4.)

6. Über Digitalcourage

Digitalcourage e.V. setzt sich seit 1987 für Grundrechte und Datenschutz ein und richtet seit 2000 die jährliche Verleihung der BigBrotherAwards aus. 2008 erhielt Digitalcourage die Theodor-Heuss-Medaille für besonderen Einsatz für die Bürgerrechte.

Mehr über Digitalcourage: https://digitalcourage.de/ueber-uns

Friedemann Ebelt M.A. friedemann.ebelt@digitalcourage.de

Digitalcourage e.V.
Marktstraße 18
33602 Bielefeld
https://digitalcourage.de

Telefon: +49 521 1639 1639
E-Mail: mail@digitalcourage.de
PGP-Key & Fingerprint: https://digitalcourage.de/kontakt

Fediverse: https://digitalcourage.social/@Digitalcourage
Twitter: @digitalcourage

50 https://www.lto.de/recht/feuilleton/f/ausweispflicht-80-jahre-identitaetsfeststellung-kennkarten/

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)613 C

BUNDESDRUCKEREI

Gesetzentwurf zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen

STELLUNGNAHME

Bundesdruckerei GmbH
Kommandantenstraße 18
10969 Berlin

Mit dem *Entwurf eines Gesetzes zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen* (Drucksache 19/21986) soll die Sicherheit und Bürgerfreundlichkeit von Verwaltungsdienstleistungen gestärkt werden.

Die Bundesregierung adressiert darin neben einer Reform der Verwendung der Seriennummer von Reisepass und Personalausweis die Aufnahme einer Versionsnummer in die MRZ (Machine Readable Zone) sowie die diskriminierungsfreie Angabe des Geschlechts im Reisepass entsprechend internationaler Regeln der Internationalen Zivilluftfahrtorganisation ICAO. Hinzu kommt die Umsetzung des Beschlusses der Justizministerkonferenz 2016 zur Personalausweispflicht für Strafgefangene drei Monate vor Haftentlassung sowie die Umsetzung der EU-Verordnungen VO (EG) Nr. 2252/2004 (Verkürzung der Geltungsdauer von Kinderreisepässen und Passersatzpapieren für Kinder) und VO (EU) Nr. 2019/1157 (verpflichtende Speicherung von Fingerabdrücken im Personalausweis). Weiterhin beinhaltet der Gesetzentwurf eine Neuregelung zur Aufnahme des Gesichtsbilds bei der Beantragung von Reisepass und Personalausweis, welche wesentliches Thema der vorliegenden Stellungnahme ist.

Die Neuregelung basiert auf den Gefahren, die aus manipulierten Gesichtsbildern resultieren können. Das Risiko einer Lichtbild-Manipulation durch sogenanntes „Morphing“, der Verschmelzung mehrerer Gesichtsbilder zu einem neuen Gesamtbild anhand digitaler Bildbearbeitungsmethoden, soll demnach vermindert werden, da *„die Funktion des Passes bzw. Personalausweises als Dokument zur Identitätskontrolle [durch Lichtbild-Manipulationen] im Kern bedroht [wird]“* (vgl. Drucksache 19/21986, S. 1).

Ausgangslage:

Die Herausforderung der Lichtbild-Manipulationen durch Morphing wird weltweit als Sicherheitsproblem angesehen und auch in der ICAO New Technologies Working Group regelmäßig thematisiert. Die zentrale Erkenntnis ist, dass das Risiko einer Lichtbild-Manipulation durch Morphing nur durch die Erfassung der Lichtbilder in einer kontrollierten Umgebung vermindert werden kann.

Dies ist jedoch wegen der weltweit unterschiedlichen Infrastrukturen nicht überall möglich: Viele Länder ohne Meldewesen in Asien und Nordamerika sind dazu übergegangen, dass Antragsteller eigene Bilder digital im Antragsprozess für neue Dokumente hochladen. Diese Bilder werden dann mit Bildern aus zentralen Datenbanken und / oder sozialen Netzwerken abgeglichen und plausibilisiert. In vielen europäischen Staaten wie u. a. der Slowakei, Dänemark, Schweden und Portugal werden die Lichtbilder für die Anträge zur Dokumentenherstellung ausschließlich in den Behörden bzw. bei der Polizei vor Ort aufgenommen.

In Deutschland wird aktuell primär mit von Fotografen aufgenommenen und ausgedruckten Lichtbildern gearbeitet, die in den Behörden digitalisiert werden. Bisher erfolgt die Digitalisierung der Lichtbilder am Behördenarbeitsplatz durch Scanner.

Lichtbilder können darüber hinaus auch digital (entsprechend der Richtlinie zur elektronischen Bildübermittlung zur Beantragung hoheitlicher Dokumente (E-Bild hD) per DE-Mail des Bundesamts für Sicherheit in der Informationstechnik (BSI)) [1] von den Fotografen an die Behörden

[1] Vgl. BSI TR-03146, abrufbar unter https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03146/TR-03146_node.html

geschickt werden. Eine weitere Option ist die Aufnahme von Lichtbildern über Kiosksysteme in den Behörden.

Rolle der Bundesdruckerei im deutschen Pass- und Ausweiswesen:

Die Bundesdruckerei verfügt über eine langjährige Erfahrung in der Bereitstellung, dem Betrieb und der Weiterentwicklung von hoheitlichen ID-Systemen, etwa für den Personalausweis, den elektronischen Aufenthaltstitel und den Reisepass, sowie der einheitlichen und flächendeckenden Versorgung der Behörden mit erforderlichen Hard- und Softwarekomponenten. Sie hat sich in den vergangenen Jahren zu einem führenden Anbieter in der Hochsicherheitstechnologie gewandelt. Neben dem klassischen Wertdruck von Banknoten, Postwert- und Steuerzeichen sowie ID-Dokumenten, dessen Tradition am Standort Berlin bis weit in das 18. Jahrhundert zurückreicht, bietet die Bundesdruckerei Produkte und Lösungen rund um sichere digitale Identitäten und Daten sowie IT-Infrastrukturen für Ministerien, Behörden und Unternehmen.

Dazu zählt neben der Erfassung und Verwaltung biografischer und biometrischer Daten auch die Herstellung und Personalisierung von ID-Dokumenten sowie Systeme zu deren Ausgabe und Verifikation. Bereits 2005 hat die Bundesdruckerei die Chip-Technologie in den EU-Reisepass integriert und darin neben den Personendaten das biometrische Lichtbild gespeichert. Im Jahr 2007 erfolgte die Ausstattung aller Pass- und Personalausweisbehörden mit Fingerabdruckscannern.

Auf Basis dieser Infrastruktur hat die Bundesdruckerei 2010 mit der Einführung des Personalausweises im Scheckkartenformat eines der damals größten IT-Projekte Deutschlands durchgeführt. Der Ausweis enthält seitdem einen kontaktlosen Chip, auf welchem die persönlichen sowie biometrischen Daten hinterlegt sind. Zudem ist der Personalausweis mit einer Qualifizierten Elektronischen Signatur (QES) und einer Online-Ausweisfunktion ausgestattet, die es dem Bürger erlaubt, sich mit seinem Ausweis im Internet zu identifizieren. Für die Produktion des Personalausweises mit Online-Ausweisfunktion wurde ein komplett neues Sicherheitskonzept für den Gesamtaufbau der Karte entwickelt, die gesamte Fertigung an die neuen technologischen Sicherheitsbedingungen angepasst und neue Maschinen konzipiert. Gleichzeitig wurde eine neue hochsichere Infrastruktur zur Erfassung und Übermittlung der Daten an die Produktion aufgebaut.

Seitdem betreibt die Bundesdruckerei im Auftrag des Bundes ein komplexes bundesweites Gesamtsystem zur Erstellung hoheitlicher Ausweisdokumente, an das die 6115 Pass- und Personalausweisbehörden, die Ausländerbehörden sowie die Botschaften und Konsulate des Auswärtigen Amts direkt angebunden sind. Es unterstützt u. a. die Erfassung der Daten des Antragstellers, das Auslesen und Ändern der Personendaten im Ausweischip, die Übermittlung der Antragsdaten an die Bundesdruckerei sowie die eigentliche Produktion der Dokumente.

Der Betrieb der für das Auslesen und Ändern der Personendaten im Ausweischip erforderlichen Änderungsterminals erfolgt auf Basis einer von der Bundesdruckerei betriebenen Public Key Infrastructure (PKI), die täglich neue Berechtigungszertifikate an die Systemkomponenten im Gesamtsystem übermittelt. Für die Nutzung der Online-Ausweisfunktion stellt die Bundesdruckerei über ihr akkreditiertes Trustcenter D-Trust das dazugehörige Hintergrundsystem (eID-Server) zur Verfügung, mit dem die auf dem Dokumentenchip gespeicherten Daten von den nach §21 des deutschen Personalausweisgesetzes (PAuswG) berechtigten Akteuren ausgelesen werden können. Die hierfür benötigten Berechtigungszertifikate werden ebenfalls

durch die D-Trust GmbH, die seit 2016 als qualifizierter Vertrauensdiensteanbieter gelistet ist, bereitgestellt.

Die in den Behörden erforderliche Systeminfrastruktur wird den Pass- und Personalausweisbehörden, den Ausländerbehörden sowie den Botschaften und Konsulaten des Auswärtigen Amts direkt bzw. über die Dienstleister dieser Behörden (Fachverfahrenshersteller im Einwohner- und Ausländerwesen sowie Rechenzentren) bereitgestellt.

Liefergegenstände umfassen heute:

- Erfassungssoftware für Lichtbilder
- Software zur Biometrieprüfung der Lichtbilder (ICAO-Kompatibilität)
- Erfassungs- und Qualitätssicherungssoftware für Fingerabdrücke
- IT-Infrastruktur zur Anbindung von Behörden an Produktionssysteme
- Software zur Signierung und Verschlüsselung der Antragsdaten inklusive Kommunikationsclient
- ca. 28.500 Fingerabdruckscanner inklusive Echtheitsbewertung
- ca. 26.000 Visualisierungs-Änderungsterminals (für PIN- und Adressänderungen im Chip)

Die Digitalisierung der Lichtbilder am Behördenarbeitsplatz erfolgt heute hauptsächlich durch Scanner, die von den Behörden selbst beschafft werden. Bezüglich der Scanner führt die Bundesdruckerei zur Qualitätsverbesserung Tests zur Nutzbarkeit in Kombination mit den Softwaremodulen zur Beantragung von Dokumenten aus. Die Testprotokolle werden den Behörden zur Verfügung gestellt.

Der Betrieb und die Ausrüstung des Gesamtsystems erfolgt unter Gewährleistung höchster Sicherheits-, Datenschutz- und Qualitätsstandards. Die Bundesdruckerei erfüllt alle gesetzlichen Anforderungen, Standards und relevanten technischen Richtlinien wie z. B. BSI TR-03121 (Biometrie in hoheitlichen Dokumenten). Soft- und Hardware werden bei Änderungen einer (Re-)Zertifizierung des BSI unterzogen. Zudem engagiert sie sich aktiv in nationalen und internationalen Gremien für die Standardisierung und Weiterentwicklung von Sicherheitstechnologien.

Die Bundesdruckerei gewährleistet für alle angeschlossenen Behörden, unabhängig vom Bestellaufkommen, der Größe und dem Ort, einen flächendeckenden Service und Support der o. g. Infrastruktur. Hierfür setzt sie rund 200 Mitarbeiter für den bundesweiten Einsatz vor Ort ein und betreibt ein eigenes Call Center für den telefonischen Support.

Sie arbeitet im Rahmen der bestehenden Verträge für den Personalausweis, Reisepass und elektronischen Aufenthaltstitel mit zahlreichen Lieferanten und Dienstleistern zusammen. Hierfür werden in Abhängigkeit vom Auftrag entsprechende Leistungen ausgeschrieben und die jeweiligen Unternehmen eingebunden.

Neuregelung der Erfassung von Lichtbildern:

Ab Mai 2025 sollen ausschließlich digitale Lichtbilder und eine medienbruchfreie Erfassung im Beantragungsprozess der hoheitlichen Dokumente zugelassen werden. Dies ist aus Sicht der Bundesdruckerei ausdrücklich zu begrüßen.

Hierzu haben Bürgerinnen und Bürger laut Gesetzentwurf zukünftig bei der Lichtbilderstellung die Wahl zwischen zwei Optionen: Sie können das Lichtbild entweder durch einen Dienstleister der Privatwirtschaft erstellen lassen, wobei der Dienstleister sicherstellen muss, „*dass eine elektronische, medienbruchfreie Übermittlung eines unbearbeiteten Lichtbilds an den Passhersteller auf sicherem Weg erfolgt*“, oder „*das Lichtbild vor Ort in der Passbehörde erstellen lassen, sofern die Behörde über Lichtbildaufnahmegeräte verfügt*“ (vgl. Drucksache 19/21986, Begründung Besonderer Teil, S. 34).

Im ersten Fall sollen private Dienstleister, im Speziellen Fotografen sowie Automaten- und Erfassungsgerätebetreiber, die Möglichkeit erhalten, von ihnen gefertigte Lichtbilder über eine offene, standardisierte Schnittstelle und eine sichere Verbindung an die Pass- oder Personalausweisbehörde übermitteln zu können. Laut Gesetzentwurf sollen die näheren Bestimmungen zum Prozess der Übermittlung durch eine Rechtsverordnung geregelt werden. Das oben beschriebene Gesamtsystem verfügt bereits über standardisierte Schnittstellen, welches die Anbindung externer Komponenten grundsätzlich ermöglichen.

Für den zweiten Fall soll eine bedarfsorientierte Ausstattung der Pass- und Personalausweisbehörden mit Geräten am Arbeitsplatz oder Selbstbedienungsterminals erfolgen, sodass die flächendeckende Verfügbarkeit einer entsprechenden Infrastruktur unter hoheitlicher Kontrolle sichergestellt werden kann. Das Bundesministerium des Innern, für Bau und Heimat plant, diese Erweiterung des bereits bestehenden Systems durch die Bundesdruckerei durchführen zu lassen.

Die Bundesdruckerei verfügt über einschlägige Erfahrung in diesem Bereich. Sie ist bereits heute einer der führenden Anbieter für Selbstbedienungsterminals im Behördenumfeld. Zudem hat sie im Jahr 2015 innerhalb weniger Monate ein ähnliches System zur Erfassung biometrischer und biografischer Daten von Asylsuchenden entwickelt und 1.500 Systeme deutschlandweit ausgerollt und in Betrieb genommen. Dieses System umfasste im Speziellen die Aufnahme biometrischer Lichtbilder an den Arbeitsplätzen der Sachbearbeiter.

Die Behörden sollen im Rahmen der geplanten Erweiterung ebenfalls mit einer sicheren, medienbruchfreien Infrastruktur mit nach BSI-Richtlinien zertifizierten Systemkomponenten zur digitalen Aufnahme, Verarbeitung und Übermittlung der Bilddateien ausgestattet werden. Durch die damit weiterhin einheitliche Systemarchitektur ergeben sich Vorteile insbesondere für die Gewährleistung hoher Standards für Hard- und Software sowie den Betrieb und die Ausfall- und Informationssicherheit. Durch die Nutzung etablierter Mechanismen kann schnell auf gesetzliche Änderungen reagiert werden. Eine einheitliche Wartung, Administration und technische Weiterentwicklung sowie ein Update-Prozess werden sichergestellt. Eine für kleine, mittlere und große Behörden gleichermaßen geeignete Systemarchitektur aus einer Hand und die enge Verbindung zur Dokumentenfertigung ermöglichen eine hohe Verlässlichkeit und Qualität sowie eine einheitliche Lichtbildqualität.

Für die Entwicklung und Bereitstellung der Systemkomponenten arbeitet die Bundesdruckerei mit einer Vielzahl von erfahrenen Lieferanten der deutschen Sicherheitsindustrie im Bereich von Biometriealgorithmen und -hardware zusammen. Durch die Einbindung führender Technologieunternehmen können gemeinsam innovative Lösungen entwickelt werden. Gleichzeitig ist mit der Bundesdruckerei als Bundesunternehmen die staatliche Kontrolle für das Pass- und Ausweiswesen als hoheitliche Aufgabe vollumfänglich gegeben.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)613 D

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Nationales Forschungszentrum
für angewandte Cybersicherheit

Prof. Dr. Christoph Busch

Hochschule Darmstadt
Haardtring 100
64293 Darmstadt
Tel. +49-6151-16-30090

christoph.busch@h-da.de

2020-10-23

An
den Ausschuss für Inneres und Heimat des
Deutschen Bundestages

Stellungnahme zum Gesetzentwurf zur Stärkung der Sicherheit im Pass-, Ausweis und ausländerrechtlichen Dokumentenwesen
BT-Drucksachen 19/21986 und 19/22783

Sehr geehrte Damen und Herren,

ich danke für die Einladung zur Anhörung am kommenden Montag und übersende Ihnen vorab meine Stellungnahme zum Gesetzentwurf.

Ich bin weitestgehend zufrieden mit dem Entwurf des Gesetzes zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen (Drucksache 19/21986) vom 31.08.2020 und freue mich über die Änderungen, die gegenüber der Vorversion vom 09.12.2019 umgesetzt wurden.

Der Entwurf ist in seinem Wesen richtig und wichtig und wird ermöglichen, dass Deutschland zu den Europäischen Vorreitern im Live-Enrolment (Schweden und Norwegen) endlich aufschließen kann.

zur Technik:
Ich kann Ihre Annahme bestätigen, dass derzeit nach meinem Wissen alle Produkte zur automatisierten Gesichtserkennung durch Morphing-Angriffe verwundbar sind. Es ergeben sich hohe Übereinstimmungswerte für beide im Lichtbild „enthaltenen“ Personen, die denen von unveränderten Lichtbildern entsprechen. Das bedeutet, dass Personaldokumente Ihren eigentlichen Wert verlieren, da die biometrische Bindung an den Inhaber nicht mehr gewährleistet ist.

Es gibt zwei Alternativen zur Prävention vor Morphing-Angriffen:
1.) Live-Enrolment in Deutschland und allen anderen EU-Ländern
2.) Elektronische Übertragung von digital signierten Lichtbildern direkt von autorisierten Photographen (Dienstleistern) an die Passbehörde (ebenfalls in allen EU-Ländern)

zu 1.): das ist die langfristig sinnvollste Lösung, die in Deutschland und allen EU-Mitgliedsstaaten umgesetzt werden sollte. Jedoch bleiben auch damit die Morphing-Angriffe von Drittstaatlern weiterhin möglich.

zu 2.): dies könnte z.B. durch De-Mail realisiert werden, wie es nun in Abschnitt E.2 in der Drucksache 19/21986 diskutiert wird. Damit sollten die vorgetragenen Bedenken der Photographen ausreichend berücksichtigt sein. Forderungen zur Beibehaltung der Verwendung ausgedruckter Lichtbilder sind nicht mehr zeitgemäß und bei Kenntnis der Morphing-Angriffe nicht zu verantworten. Zudem werden meines Wissens die Digitalisierungs-Bemühungen der Bundesregierung ja auch von den Oppositionsparteien getragen. Warum sollte man hier eine Ausnahme machen?

Im direkten Vergleich ist die Alternative 1.) klar zu favorisieren. Erstens aus Gründen der Sicherheit des Verarbeitungsprozesses, da Alternative 2.) möglicherweise Einbringpunkte für manipulierte/gemorphte Lichtbilder zulassen würde. Zweitens sind bei Alternative 2.) Kosten und logistischer Aufwand bei der Registrierung der Dienstleister anzunehmen.

Unabhängig von 1.) und 2.) ist es notwendig, Morphing-Attack-Detection (MAD) Verfahren zu entwickeln, die für den Einsatz an der Grenze zur Detektion von Pässen mit gemorphten Lichtbildern z.B. aus Drittstaaten geeignet sind. siehe:
https://christoph-busch.de/projects-mad.html

Es gibt mittlerweile etliche Forschungsaktivitäten, um gemorphte Lichtbilder zu erkennen. Die Detektionsleistung und insbesondere die Falschalarmraten solcher MAD-Verfahren sind derzeit ungenügend und für den operativen Einsatz noch nicht geeignet. siehe:
https://pages.nist.gov/frvt/html/frvt_morph.html
Dabei sei betont, dass die Alterung von biometrischen Referenzdaten im Verlauf der 10 jährigen Gültigkeitsdauer des Ausweises, in Verbindung mit einem Morphing-Angriff, die Chancen zur Detektion von gemorphten Lichtbildern weiter schmälern.

Fingerbilder im Dokumentenwesen:
Die „Zufallsfunde“ von gemorphten Pässen in polizeilichen Ermittlungen oder bei der Kontrolle an den Grenzen sind in der Regel auf andere Indizien als die Lichtbild-Analyse zurückzuführen. Selbst bei einer anzunehmenden Leistungssteigerung der MAD-Verfahren in den kommenden Jahren bleibt zum sicheren Nachweis der biometrischen Verbindung von Personaldokumenten zum Passinhaber (d.h. ein Pass = ein und **nur ein** Nutzer) bis auf Weiteres nur der biometrische Vergleich der beiden Fingerbilder aus dem Pass mit den Fingerabdrücken des Reisenden. Dieser Fingerbild-Vergleich dient somit der Zielerreichung einer sicheren

Identitätsfeststellung. Der Vergleich gehört derzeit nicht zum Standardprozess in der Grenzkontrolle, könnte jedoch in Zukunft die bisherigen Kontrollschritte im Verdachtsfall (z.B. bei Alarm eines MAD-Verfahrens) oder bei sonstigen Auffälligkeiten ergänzen. Damit ergibt sich die technische Notwendigkeit, die Fingerbilder beizubehalten – unabhängig vom rechtlichen Rahmen, der durch die EU-Verordnungen 2252/2004 und 2019/1157 ohnehin vorgegeben ist. Eine Diskussion um den etwaigen Verzicht von Fingerbildern im Pass- und Personalausweis ist meines Erachtens nicht erforderlich.

Die Sorge von Kollege Weichert, dass Fingerbilder als nationale Kennziffern genutzt werden können teile ich nicht, da eine nachhaltige Speicherung ja nur im Ausweisdokument erfolgt, die biometrischen Referenzdaten sich somit unter der vollständigen Kontrolle des Bürgers selbst befinden. Es muss sichergestellt bleiben – und darauf vertraue ich – dass weder die Passbehörden noch die Bundesdruckerei bei der Ausstellung des Ausweises eine Kopie der biometrischen Bilder erstellt. Ein nationales Register von Fingerbildern der Bundesbürger sollte es in Deutschland auch weiterhin nicht geben.

Auch die Sorge, dass Fingerbilder von Deutschen Bürgern durch Unberechtigte ausgelesen werden können, ist nicht begründet, da die Fingerbilder durch Extended Access Control (EAC) ausreichend geschützt sind.
https://www.icao.int/Security/FAL/PKD/BVRT/Pages/Document-readers.aspx

Der Vorschlag von Kollege Weichert, statt der Indexfinger den/die Ringfinger oder kleine Finger zu erfassen, ist meines Erachtens nicht im Einklang mit der EU-Verordnung 2019/1157. Auch wenn dort nicht explizit der Index-Finger gefordert wird, ist doch die Intention der Verordnung erkennbar: Auf dem Personalausweis (Identity cards of Union citizens) soll die gleiche ICAO 9303 logische Datenstruktur gespeichert werden, wie sie auch nach EU-Verordnungen 2252/2004 in den Reisepässen Verwendung findet. Wären nur in Deutschen Personalausweisen die kleinen Finger gespeichert, jedoch in allen anderen Ländern die Zeigefinger (wie erwartet), wäre die Identitätsfeststellung im Ausland zumindest behindert. Auch aus technischer Sicht, ist ein Wechsel auf den kleinen Finger nicht sinnvoll: Die Fingerabdruckfläche wäre kleiner, und lieferte weniger Minutien. Je kleiner die Fingerabdruckfläche, desto weniger Gewissheit bietet der biometrische Vergleich. Zudem ist die biometrische Erfassung der Zeigefinger durch die anatomischen Gegebenheiten wesentlich einfacher als beim Ringfinger oder beim kleinen Finger.

Alternativen und Anforderungen an den Anbieter:
Ein noch kontrovers diskutiertes Element im Gesetzentwurf ist die Regelung in Artikel 1 betreffend Passgesetz §1 (5), wonach das Gesetz genau *einen* Anbieter als Lieferanten vorsieht, wobei in E.3 explizit die Bundesdruckerei genannt ist.

Hier sind die Vor- und Nachteile für die Festlegung
auf nur einen Anbieter abzuwägen:

a) Für einen Anbieter (d.h. die Bundesdruckerei) spricht

- Es ist leichter zu erreichen, dass in der technischen Umsetzung im Detail einheitliche Lösungen zum Einsatz kommen. Die zu verwendende Technik wird einmalig geprüft, zertifiziert und dann installiert.
- Gegebenenfalls notwendige Updates zum Schließen von Sicherheitslücken, werden von der aufdeckenden Institution an *einen* Ansprechpartner weitergeleitet und hoffentlich zeitnah verteilt.
- Sofern eine einheitliche Lösung zum einheitlichen Preis für alle Passbehörden festgelegt wird, kommt es nicht zu höheren Kosten für den ländlichen Raum (in dem weniger Umsatz zu erwarten ist, als bei einer Passbehörde in einem Ballungszentrum).
- Auch in anderen föderal organisierten EU-Ländern wurde diese Option gewählt.

b) Für viele Anbieter spricht

- Während die Passproduktion selbst eindeutig eine sicherheitskritische Aufgabe ist, genügt bei der Aufnahme der Lichtbilder und Fingerbilder die Sorgfalt und der Nachweis, dass jegliche Manipulation der erfassten biometrischen Bilder ausgeschlossen werden kann. Dies lässt sich dadurch erreichen, dass die Eignung der Erfassungsgeräte durch eine Zertifizierung der Geräte eingefordert wird.
- Die Grundlage für eine solche Zertifizierung besteht bereits durch die Technische Richtlinie BSI TR-03121-3.2. Siehe:
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03121/tr-03121.html
  Einige Systemanbieter von Erfassungsgeräten wurden bereits nach BSI TR-03121 zertifiziert und sind auf der Homepage des BSI gelistet:
  https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachTR/ZertifizierteProdukte/Enrolment_Stations/Enrolment_Stations_node.html

Mit dieser Liste erfüllt das BSI schon in der aktuellen Fassung des Passgesetzes die Aufgabe nach §6a (3), nämlich die Einhaltung der Anforderungen an Geräte zur Erfassung des Lichtbildes und der Fingerabdrücke festzustellen.

- Es könnten *mehrere* Lieferanten / Betreiber unter Einsatz von verschiedenen Produkten zum Einsatz kommen, wenn diese Produkte nach TR-03121 zertifiziert wurden. Die beste Technologie kann sich im freien Wettbewerb durchsetzen.
- Das Sicherheitsniveau der Technologie verschiedener Anbieter wird immer noch höher sein als die Übermittlung von Lichtbildern durch Dienstleister nach Alternative 2.), wie oben diskutiert.

Diese Abwägung ist nach meinem Eindruck die entscheidende Frage in der Anhörung am 26. Oktober, zu der es verständlicher Weise kontroverse Meinungen gibt.

Ich kann die operativen Gründe für Option a) nachvollziehen. Aus meiner Sicht wird diese Option a) jedoch weder eine höhere biometrische Qualität von Lichtbildern oder Fingerbildern bedeuten noch eine Erhöhung der Sicherheit gegenüber Option b). Zudem ist zu bedenken, dass auch Option b) in jedem Fall eine höhere Sicherheit zur Alternative 2.) darstellt – also zur Übermittlung der Lichtbilder durch den Dienstleister per De-Mail-Übertragung. Biometrische Qualität und Sicherheit werden nur erreicht, wenn die in den Passbehörden aufgestellten Erfassungsgeräte zwingend zertifiziert sein müssen und beim Auftreten von Sicherheitslücken zur Not abgeschaltet werden, wenn der Lieferant nicht zeitnah ein Update bereitstellen kann. Die Notfallabschaltung könnte einen oder mehrere Lieferanten betreffen und sowohl bei Option a) als auch bei Option b) zum Einsatz kommen. Ersatzweise muss die Passbehörde in einem Fall der Abschaltung dann auf die Dienstleister (d.h. die Photographen) verweisen, mit denen sie (die Passbehörde) nach §6a Absatz 3 ja ohnehin über eine normierte Schnittstelle verbunden ist.

In diesem Zusammenhang der Zertifizierung finde ich für die anstehende Entscheidung a.) versus b.) drei Sachverhalte interessant:

i) Aktuell sind nach meinem Kenntnisstand ca. 1000 Geräte zur Erfassung von Lichtbildern in den ca. 6115 Pass- und Personalausweisbehörden im Einsatz.

ii) Die Bundesdruckerei hat derzeit 149 Geräte im Einsatz. Das Zertifikat für das Self-Service-Terminal (SST) ist jedoch auf der Website des BSI nicht gelistet.
iii) Ein Mitmarktteilnehmer der Bundesdruckerei hat derzeit 170 Geräte im Einsatz, wobei das von diesem Unternehmen eingesetzte Gerät nach TR-03121 zertifiziert wurde (Zertifizierungs-ID BSI-K-TR-0359-2019)

Sollte die Entscheidung für Option b) fallen, dann müsste §1(5) im Passgesetz NEU lauten:
Das Bundesministerium des Innern, für Bau und Heimat bestimmt den Passhersteller und macht seinen Namen im Bundesanzeiger bekannt. Die eingesetzten Geräte müssen nach der technischen Richtlinie TR-03121 zertifiziert sein. Die Liste der zertifizierten Geräte wird ebenfalls im Bundesanzeiger bekannt gemacht.
Die Änderung im PAuswG müsste analog erfolgen.

Abschließend - die Notwendigkeit des Gesetzes und des Live-Enrolment:
Wie im FAZ-Beitrag "Ein Pass für Zwei" von Piotr Heller am 20.01.2020 berichtet, ergab eine Umfrage unter den Experten auf der Security Printers Konferenz im Oktober 2019, dass eine relevante Anzahl von Pässen mit gemorphten Lichtbildern in den letzten 5 Jahren berichtet wurden. Darüber hinaus gibt es Hinweise auf eine hohe Dunkelziffer. Diese hohe vermutete Dunkelziffer ist auch durch die fehlenden Detektionsmöglichkeiten von gemorphten Lichtbildern zu erklären. Es gibt derzeit keine verlässliche Möglichkeit, ein gemorphtes Bild als solches zweifelsfrei zu erkennen.

Wir reden seit fünf Jahren über Migration. Ich glaube, dass das nur der Anfang von dem ist, was wir in den nächsten Jahrzehnten als Migration erleben werden. Ein Grund ist, dass der Klimawandel in Afrika viele Menschen dazu zwingen wird, ihre Länder zu verlassen.

Die Menschen in Afrika haben Zugang zum Internet. Sie lesen die Nachrichten aus Europa und sie lesen auch unsere Publikationen, die sich im Allgemeinen mit dem Thema Biometrie befassen. Das weiß ich, da ich Fragen zu unseren Publikationen bekomme. Es ist naheliegend, dass Migranten auch über Morphing-Angriffe Bescheid wissen und in Zukunft eine Flugreise (mit entsprechend manipuliertem Pass) einer Schlauchboot-Seereise vorziehen werden.

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Aus diesem Grund steht zu recht im Gesetzentwurf: "*Die Funktion des Passes als Dokument zur Identitätskontrolle ist damit im Kern bedroht*." Das ist noch eine vorsichtige Formulierung! Sollte sich die Kenntnis über die Verwundbarkeit der Gesichtserkennung bei Morphing-Angriffen ausbreiten, dann kann man die derzeitigen Prozesse an der Grenze nur noch als "Abschreckung" vor Angriffen, aber nicht mehr als "Kontrolle" und Abweisung von unerlaubten Grenzübertritten bezeichnen.

Vor dem Hintergrund der massiven Verbreitung biometrischer Systeme an den Grenzen müssen Präventionsmaßnahmen gegen Morphing sowohl die Vermeidung des Einbringens von manipulierten Lichtbildern in nationale Personaldokumente (hier: verpflichtende Aufnahme und Speicherung der Lichtbilder ohne Medienbruch *in* den Passbehörden oder bei den Dienstleistern) als auch die sichere Detektion von gemorphten Bildern in Dokumenten aus Drittstaaten (hier: Forschung und Entwicklung) umfassen.

Mit freundlichen Grüßen

Prof. Dr. Christoph Busch

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)613 E

UNIVERSITÄT DES SAARLANDES

INSTITUT FÜR RECHTSINFORMATIK

Prof. Dr. Borges · Universität des Saarlandes · Postfach 15 11 50 · 66041 Saarbrücken

Prof. Dr. Georg Borges
Lehrstuhl für Bürgerliches Recht, Rechtsinformatik, deutsches und internationales Wirtschaftsrecht sowie Rechtstheorie

Campus A5 4
66123 Saarbrücken

Telefon: +49 (0)681/302-3105
Fax: +49 (0)681/302-4469

ls.borges@uni-saarland.de
georg.borges@uni-saarland.de

23. Oktober 2020

Stellungnahme zum Entwurf eines Gesetzes zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen

Das Gesetz soll eine ganze Reihe von Änderungen mit durchaus heterogener Zielsetzung im Zusammenhang mit Ausweisen bringen. Die Stellungnahme, die ich vor dem Hintergrund meiner langjährigen Forschung zu rechtlichen Aspekten der Identifizierung und des Identitätsmissbrauchs erstelle, konzentriert sich auf die Maßnahmen zur Bekämpfung digitaler Bildbearbeitung der in Ausweisen verwendeten Lichtbilder.

I. Ausgangslage. Schutz gegen Bearbeitung von Lichtbildern in Ausweisen

Das in Ausweisdokumenten verwendete Lichtbild ist derzeit das zentrale Element der Ausweise im Rahmen der Identitätsfeststellung. Im Kern erfolgt die Identitätsfeststellung häufig durch Abgleich des Lichtbildes mit dem bildlichen Eindruck vom Gesicht der zu identifizierenden Person, der im Rahmen des Identifizierungsvorgangs entweder maschinell, etwa bei der automatisieren Grenzkontrolle, oder durch eine Person gewonnen wird. Das weitere zentrale Mittel der Identitätsfeststellung ist der Besitz des Ausweisdokuments.

Die Identitätsfeststellung durch Bildabgleich ist fehleranfällig. Zur Verbesserung der Zuverlässigkeit wurde die Pflicht zur Verwendung sog. „biometrischer" Lichtbilder eingeführt. Je weniger präzise das Lichtbild die abgebildete Person darstellt, desto schwieriger und fehleranfälliger wird der Identitätsabgleich.

Die Übereinstimmung zwischen Lichtbild und dem visuellen Eindruck einer Person kann naturgemäß bei Erstellung des Lichtbildes am besten gewährleistet werden. Wird das Lichtbild nachträglich verändert, sinkt die Zuverlässigkeit der Identifizierung. Wird das Bild durch sog. Morphing an das Bild einer anderen Person angenähert, werden Identitätstäuschungen erleichtert, insb. kann der Lichtbildabgleich diese nicht verhindern.

Dies führt dazu, dass die Integrität der für Ausweise verwendeten Lichtbilder zu schützen ist. Der Schutz sollte umso stärker sein, je größer die Gefahren aus der Fälschung des Ausweisdokuments und daran anschließenden Handlungen sind.

II. Das Schutzkonzept des Gesetzentwurfs

Der Gesetzentwurf zielt darauf ab, die Qualität der in Lichtbildern verwenden Lichtbilder zu verbessern und Bearbeitungen zu verhindern. Das Konzept des Entwurfs besteht darin, die Verwendung ausschließlich digitaler Lichtbilder vorzuschreiben und die Erzeugung und die Verwendung des Lichtbildes bis zur Übermittlung an die zuständigen Behörden zu kontrollieren.

Unterstellt man einmal, dass eine Rückkehr zu chemisch erzeugten Lichtbildern keine Option ist und dass es keine verlässlichen technische Alternativen, etwa „digitale Wasserzeichen", zum Integritätsschutz des Lichtbildes gibt, die eine Kontrolle der Übermittlung entbehrlich machen, erscheint das Konzept mir als technischem Laien schlüssig.

Das erste Element des Schutzes betrifft die Erzeugung des Lichtbildes. Hier ist sicherzustellen, dass tatsächlich der Ausweisinhaber und nicht etwa eine andere Person aufgenommen wird. Das Gesetz will dies durch zwei Maßnahmen sicherstellen: Zum einen soll die Erzeugung von Lichtbildern nur durch bestimmte „Dienstleister" (§ 6 Abs. 2 S. 3 PassG-E, § 9 Abs. 3 S. 3 PAuswG-E) oder durch Geräte der ausstellenden Behörde möglich sein, zum anderen soll die Aufnahme in Zweifelsfällen unter Aufsicht der Behörde wiederholt werden (§ 6 Abs. 3 S. 1 PassG-E, § 9 Abs. 4 S. 1 PAuswG-E).

Das Gesetz will damit dem Bürger die Möglichkeit belassen, das Lichtbild außerhalb der Behörde zu fertigen. Dies erscheint angemessen, wohl auch rechtlich geboten und ist uneingeschränkt zu begrüßen. Das grundrechtlich geschützte Interesse des Bürgers, das eigene Erscheinungsbild auf einem Ausweisdokument auch im Rahmen der eingeschränkten Möglichkeiten bei biometrischen Aufnahmen positiv zu gestalten, ist im Rahmen der

Bildaufnahme bei der Behörde unter aktuellen Bedingungen von Behördenabläufen nur sehr eingeschränkt verwirklicht.

Das zweite Element betrifft den Schutz vor Veränderungen oder gar Austausch des Lichtbildes. Dieser soll dadurch erfolgen, dass das Lichtbild bereits unter Kontrolle der ausstellen Behörde erstellt wird oder aber vom erzeugenden Dienstleister auf einem sicheren Weg an die Behörde übermittelt wird. Dieser Aspekt erscheint im Grundsatz schlüssig. Allerdings lässt der Gesetzentwurf nicht klar erkennen, welches Konzept hier verfolgt werden soll. Insoweit kann eine Stellungnahme hier nicht in die Tiefe gehen.

III. Aspekte der Umsetzung und offene Fragen

1. Die Erzeugung und Übermittlung von Lichtbildern außerhalb der Behörde

a) Beschränkung auf Dienstleister

Der Gesetzentwurf beschränkt die Erzeugung von Lichtbilder auf „Dienstleister". Damit verbindet der Gesetzgeber die Idee qualitativer Anforderungen, die im Wege der Rechtsverordnung durch das Bundesministerium des Innern, für Bau und Heimat erstellt werden sollen (§ 6a Abs. 3 S. 1 Nr. 2 PassG-E; § Abs. 3 lit. b) PAuswG-E).

Nicht geklärt ist, welche Vorstellungen das Gesetz mit dem Begriff des Dienstleisters überhaupt verbindet. Dies ist zumindest fragwürdig und rechtlich bedenklich. Dem Verfasser des Gesetzesentwurfs schwebt offensichtlich eine Pflicht zur Registrierung und Zertifizierung entsprechender Dienstleister vor. Dies ist ein erheblicher Eingriff in die Möglichkeit der Auswahl von Dienstleistern (dazu unten IV.). Verwunderlich ist, dass die grundlegenden Anforderungen an den Dienstleister (Zuverlässigkeit, Fachkunde?) im Gesetz nicht geregelt sind.

b) Qualität und Sicherheit des Aufnahmeverfahrens

Der Gesetzentwurf setzt zur Sicherung der Aufnahme auf technische Anforderungen an die eingesetzten technischen Geräte und an das Aufnahmeverfahren, die durch Rechtsverordnung (§ 6a Abs. 3 S. 1 Nr. 1 PassG-E, § 34 Nr. 3 lit. a) PAuswG-E) festgelegt werden sollen. Das Gesetz schweigt sich zu den Anforderungen aus.

Damit lässt sich nicht prüfen, welches Konzept hier verfolgt werden soll. Tatsächlich sind auf der Grundlage des Gesetzestextes extrem unterschiedliche Möglichkeiten denkbar. So

bleiben nach dem Wortlaut des Gesetzes sowohl ein Ansatz, der eine Aufnahme unter Präsenz der abgebildeten Person bei einem menschlichen Dienstleister, also Fotografen vorsieht, als auch die Aufnahme durch Automaten oder durch Lösungen an eigenen Geräten des Ausweisbewerbers, konkret Mobiltelefonen mit einer „App", denkbar. Die damit verbundene Technikneutralität der gesetzlichen Regelung ist zu begrüßen. Verwunderlich ist, dass das Gesetz keinerlei inhaltlichen Vorgaben macht. Es wird nicht einmal der Grundsatz geregelt, dass das Verfahren hinreichende Gewähr für die Qualität und Sicherheit der Aufnahme regelt.

2. Die Lieferung der Geräte für den Behördenbetrieb

Die seitens der Behörde für die Erzeugung von Lichtbildern eingesetzten Geräte sollen ausschließlich durch einen vom Bundesministerium des Innern, für Bau und Heimat zu bestimmenden Hersteller geliefert werden (§ 1 Abs. 2 S. 1 PassG-E, § 1 Abs. 3 S. 1 Nr. 2 PAuswG-E). Der zu bestimmende Hersteller steht offenbar schon fest, gemeint ist die bundeseigene Bundesdruckerei GmbH. Ausweislich der Gesetzesbegründung hat sich das Ministerium mit der Bundesdruckerei bereits über den Preis – 171 Mio. Euro für fünf Jahre– verständigt und will diesen Preis über die Gebühr für die in der Behörde gefertigten Lichtbilder gegenfinanzieren.

Diese Beschränkung ist nicht recht nachvollziehbar. Es ist kein sachlicher Grund ersichtlich, warum insoweit nur ein einziger Anbieter zum Zuge kommen soll. Die technischen Anforderungen an die Geräte sollen in einer Rechtsverordnung festgelegt werden (§ 6a Abs. 3 S. 1 PassG-E, § 34 Nr. 3 lit. a) PAuswG-E), die Einhaltung soll durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) festgestellt werden (§ 6a Abs. 2 S. 2 PassG-E, § 12 Abs. 2 S. 2 PAuswG-E). Damit besteht eine ideale Grundlage für eine offene Beschaffung der Geräte durch die Kommunen am Markt.

IV. Eingriffe des Gesetzes in die berufliche Tätigkeit der Erzeuger von Lichtbildern und entsprechenden Geräten

Das geplante Gesetz führt zu erheblichen Eingriffen in Rechtspositionen der Gewerbetreibenden, der Kommunen, mittelbar auch der Bürger.

1. Anforderungen an Dienstleister

Das Gesetz setzt Voraussetzungen für die Erstellung von Lichtbildern außerhalb der Behörde, indem nur Dienstleister zugelassen sind, an die durch Rechtsverordnung zu definierende materielle Anforderungen erfüllen. Der Inhalt dieser Anforderungen ist nicht absehbar. Da das Gesetz auch "Zertifizierung" als mögliche Anforderung nennt, kommen gravierende Eingriffe in die Berufsausübung in Betracht. Soweit durch Rechtsverordnung eine „Zertifizierung" im Sinne einer Prüfung durch eine kompetente und unabhängige Instanz verlangt werden sollte, werden die erheblichen Kosten derartiger Zertifizierung, die nur bei einer hohen Zahl an Lichtbildern für Ausweiszwecke finanziert werden können, zwangsläufig dazu führen, dass nur sehr wenige Anbieter eine solche Lizenz anstreben werden. Insbesondere für lokale Fotografen wird die Fertigung nicht möglich sein.

In diesem Fall wären erhebliche Eingriffe in die Berufsausübungsfreiheit (Art. 12 GG) der Fotografen gegeben. Selbst wenn man davon ausgeht, dass eine derart inhaltsleere Verweisung an den Verordnungsgeber den Anforderungen des Art. 80 Abs. 1 S. 2 GG genügt, erscheint eine grundlegende Regelung der Anforderungen dringend geboten.

2. Monopol der Lieferung von Aufnahmegeräten in Behörden

Der Gesetzentwurf strebt ein Monopol für die Lieferung und die Wartung der in den Behörden verwendeten Aufnahmegeräte an. Damit wird in die berufliche Tätigkeit der privaten Anbieter derartiger Geräte erheblich eingegriffen. Dieser Eingriff in die Berufsausübungsfreiheit (Art. 12 GG) bedarf einer Rechtfertigung, die nicht erkennbar ist. Die durch Rechtsverordnung zu stellenden materiellen Anforderungen die Sicherheit der Geräte, verbunden mit einer Überprüfung durch das BSI, erscheinen ausreichend. Die Erstellung von Lichtbildern für amtliche Ausweise ist nicht per se eine hoheitliche Tätigkeit, sondern traditionell eine Tätigkeit der Privatwirtschaft. Dies stellt das Gesetz ja auch nicht in Frage. Umso mehr erscheint das angestrebte Gerätemonopol zugunsten der Bundesdruckerei inkonsistent, der Eingriff in die Berufsausübungsfreiheit erscheint nicht erforderlich, erst recht nicht verhältnismäßig. Daher bestehen erhebliche Zweifel an der verfassungsrechtlichen Zulässigkeit des § 1 Abs. 5 S. 1 PassG-E, § 4 Abs. 3 S. 1 Nr. 2 PAuswG-E.

V. Aufenthaltstitel nach dem Aufenthaltsgesetz

Der Gesetzentwurf beschränkt sich auf die Sicherung der Lichtbilder im Personalausweisen und Passwesen. Lichtbilder werden jedoch auch in Aufenthaltstiteln nach dem Aufenthaltsgesetz verwendet. Das Bedürfnis nach Integrität der dort verwendeten Lichtbilder dürfte in gleicher Weise bestehen. Es ist nicht verständlich, warum die parallele Regelung des Aufenthaltsgesetzes nicht mit den für den Personalausweis und den Pass vorgesehenen Regeln koordiniert wird.

VI. Gesamtwürdigung

Es ist zu begrüßen, dass die Anforderungen an die Erzeugung und Übermittlung von Lichtbildern für Ausweisdokumente gesetzlich geregelt werden. Es ist sicher richtig, insoweit mit dem Personalausweis und dem Pass als den zentralen Ausweisdokumenten zu beginnen. Das Regelungskonzept sollte parallel aber auch für Dokumente nach dem Aufenthaltsgesetz eingesetzt werden.

Das Regelungskonzept des Gesetzes erscheint im Grundsatz schlüssig. Die konkrete Gestaltung ist jedoch fragwürdig und wirft in Einzelpunkten auch Zweifel an der Verfassungsmäßigkeit des Gesetzes auf. Insbesondere sollten die grundlegenden Anforderungen an Dienstleister im Gesetz selbst geregelt werden. Das Monopol für die Geräteerstellung zugunsten der Bundesdruckerei erscheint nicht gerechtfertigt.

- Prof. Dr. Georg Borges -