RECHTSWISSENSCHAFTLICHE FAKULTÄT
UNIVERSITÄT DES SAARLANDES

Lehrstuhl
für Rechtsinformatik

Prof. Dr. Christoph Sorge

Postfach 15 11 50
66041 Saarbrücken

Besucheranschrift:
Campus C3 1, Raum 1.25
66123 Saarbrücken

Tel. 0 681 / 302-51 22
Sekr. 0 681 / 302-51 20
E-Mail christoph.sorge@uni-saarland.de
Web www.legalinf.de

Berlin, 3. Juli 2023

Stellungnahme zum Entwurf eines Gesetzes zur Modernisierung des Pass-, des Ausweis- und des ausländerrechtlichen Dokumentenwesens

A. Vorbemerkung

Aufgrund der Kürze der zur Erstellung der vorliegenden Stellungnahme zur Verfügung stehenden Zeit beschränkt diese sich auf die Kommentierung einzelner Aspekte des Gesetzesentwurfs sowie des Entschließungsantrags der Fraktionen der SPD, BÜNDNIS 90/DIE GRÜNEN und der FDP (Ausschussdrucksache 20(4)258).

B. § 16a Abs. 3 PassG-E, § 20 Abs. 3a PAuswG-E und § 78 Abs. 7 AufenthG-E

Ich verstehe § 16a Abs. 3 PassG-E, § 20 Abs. 3a PAuswG-E und § 78 Abs. 7 AufenthG-E so, dass ein Auslesen sowohl vor Ort als auch online ermöglicht werden soll.[1] Vor Ort dürften die Vorteile in der Fälschungssicherheit durch die digitale Signatur des Lichtbildes sowie in der Möglichkeit eines automatisierten Abgleichs liegen.

Das Auslesen des Lichtbilds aus dem elektronischen Speicher- und Verarbeitungsmedium eines Personalausweises, Aufenthaltstitel oder Passes kann aber auch für die Identifikation bei der Videokommunikation jedenfalls nach heutigem Stand sinnvoll sein. Es ist aktuell in

[1] Das Auslesen des Lichtbilds aus dem Pass erfolgt nach einem anderen Protokoll als bei Personalausweis und Aufenthaltstitel, ist aber grundsätzlich mit der gleichen Hardware möglich – also auch mit den meisten aktuellen Smartphones.

§ 16c BeurkG vorgesehen, könnte aber perspektivisch auch z. B. im Rahmen der digitalen Teilnahme an Gerichtsverhandlungen zum Einsatz kommen. Das Auslesen der Gesichtsbilds erfordert seitens des Nutzers die Eingabe der CAN (Card Access Number, die auf dem Ausweis bzw. Aufenthaltstitel aufgedruckt ist) oder von Daten aus der MRZ des Passes. Soweit das Auslesen von Lichtbildern im Kontext einer Videokommunikation vorgesehen werden soll, wäre eine explizite gesetzliche Regelung bzw. Klarstellung wünschenswert.

Der Hinweis des BfDI auf die Gefahr, dass durch Deep Fakes die Identifikation von Teilnehmern einer Videoübertragung anhand eines Lichtbilds entwertet wird, ist berechtigt. Aktuell dürfte diese Gefahr noch beherrschbar sein, wenn die Empfehlungen der ENISA[2] befolgt werden und in Fällen, bei denen ein Identitätsmissbrauch besonders wahrscheinlich erscheint, auf die Videoidentifikation verzichtet wird. Auch die ENISA weist im o. g. Bericht allerdings auf den schnellen technischen Fortschritt bei der Erstellung überzeugender Deepfakes hin, so dass eine zuverlässige Erkennung solcher Fälschungen mittel- bis langfristig nicht mehr möglich sein dürfte.

Ein elektronischer Identitätsnachweis ohne Lichtbildübermittlung, in dessen Rahmen der Ausweisinhaber lediglich seine PIN eingibt, ist für viele Anwendungsszenarien ebenfalls sinnvoll und ausreichend. Das gilt jedoch nicht, wenn der Ausweisinhaber an einem Identitätsmissbrauch mitwirkt und seinen Ausweis nebst PIN weitergibt.

Ein elektronischer Identitätsnachweis kann natürlich auch mit dem Auslesen des Lichtbildes kombiniert werden.

C. Registermodernisierung

Zu dem Antrag der Fraktionen der SPD, BÜNDNIS 90/DIE GRÜNEN und der FDP auf eine Entschließung des 4. Ausschusses des Deutschen Bundestages (Ausschussdrucksache 20(4)258) möchte ich betonen, dass ich an der grundlegenden Kritik aus dem Gutachten „Registermodernisierung: Datenschutzkonforme und umsetzbare Alternativen“[3] sowie meiner Stellungnahme zum Entwurf des Registermodernisierungsgesetzes (Ausschussdrucksache 19(4)667 C) festhalte. Bereits der grundlegende Ansatz eines allgemeinen Personenkennzeichens entspricht nicht dem Stand der Technik des Identitätsmanagements. Das zeigt sich auch etwa darin, dass der Personalausweis schon seit der Einführung des elektronischen Identitätsnachweises im Jahr 2010 in der Lage ist, für jeden Diensteanbieter ausweis- und anbieterspezifische Kennzeichen zu erzeugen (sog. „Restriced Identification“). Da diese Kennzeichen an den Ausweis und nicht die Person gebunden sind, eignen

[2] Remote Identity Proofing – Attacks & Countermeasures, ENISA-Bericht vom 20. Januar 2022, online abrufbar unter `https://www.enisa.europa.eu/publications/remote-identity-proofing-attacks-countermeasures/@@download/fullReport`

[3] *Christoph Sorge, Indra Spiecker gen. Döhmann, Jörn von Lucke*: Registermodernisierung: Datenschutzkonforme und umsetzbare Alternativen, Friedrich-Naumann-Stiftung für die Freiheit, 2020

sie sich nicht unmittelbar zum Einsatz als langlebige bereichsspezifische Personenkennzeichen. Sie zeigen jedoch die Möglichkeiten aktueller datenschutzfreundlicher Technik exemplarisch auf.

Wie im genannten Gutachten bereits dargelegt, besteht eine nicht nur geringe Wahrscheinlichkeit, dass die Verwendung der Steuer-ID als allgemeines Personenkennzeichen durch das Bundesverfassungsgericht untersagt werden wird. Daher erscheint eine Vorbereitung auf diesen Fall ratsam – einschließlich einer möglicherweise notwendig werdenden Neuvergabe aller Steuer-IDs, wenn diese bis zur Entscheidung des BVerfG bereits an zahlreiche Register übermittelt worden sein sollten.

Zu den einzelnen Anträgen unter II möchte ich wie folgt Stellung nehmen:

1. Die vorgeschlagene Stärkung des Datenschutzcockpits ist grundsätzlich begrüßenswert. Insbesondere ist positiv zu werten, dass auch Übermittlungen innerhalb eines Bereichs erfasst werden und sogar Benachrichtigungen ermöglicht werden sollen. Auch die Möglichkeit von Einsichtnahme in Bestandsdaten sowie die Geltendmachung von Betroffenenrechten über das Datenschutzcockpit sind geeignet, die Transparenz der staatlichen Datenverarbeitung zu verbessern und Erwartungen der Bürger an moderne E-Government-Dienste zu erfüllen. Die Zusammenführung umfangreicher Einsichtnahme- und Steuerungsmöglichkeiten an einer zentralen Stelle erhöht aber auch das Risiko missbräuchlicher Verwendung des Datenschutzcockpits. Daher sollten technische Umsetzungen gewählt werden, die dieses Risiko weitestmöglich reduzieren. So sind beispielsweise Lösungen denkbar, bei denen Daten aus einzelnen Registern erst auf dem Endgerät des Nutzers entschlüsselt werden und nicht etwa auf einem Server im Klartext vorliegen.

2. Entsprechende Vorgaben sind, soweit nicht ohnehin de lege lata vorgesehen, zwingend notwendig und sollten (ggf. untergesetzlich) weiter konkretisiert werden.

3. Auch dies halte ich für zwingend notwendig. Um sicherzustellen, dass die Steuer-ID nicht als Authentifizierungsmerkmal verwendet wird, müsste auch jedenfalls eine praktikable Alternative für jeden Einzelfall (einschl. telefonischer Auskünfte) verfügbar sein.

4. Hierzu sollten sich unproblematisch technische Ansätze finden lassen – jedenfalls, soweit Zugriffe innerhalb der dafür vorgesehenen Systeme stattfinden. Der Vorschlag ist jedenfalls aus Sicht des Datenschutzes zu begrüßen, aus meiner Sicht sogar notwendig, um Missbrauch zu verhindern. Umgekehrt ist die Zweckbindung der durch die Auswertung von Zugriffen erzeugten Daten zu beachten, denn die Zugriffe haben auch einen Bezug zur Person des jeweiligen Bearbeiters.

5. In der Tat ist dieses Vorgehen aus zwei Gründen sinnvoll. Einerseits sollte das Konzept der Registermodernisierung für sich genommen weiterentwickelt werden, um den Datenschutz beim E-Government kontinuierlich zu verbessern und vor allem auch, um im Fall einer festgestellten Verfassungswidrigkeit des bislang verfolgten

Konzepts zeitnah auf eine verbesserte Alternative zurückgreifen zu können. Ansätze dazu, die bereits mit einfachen Mitteln ohne grundlegende Änderungen des verfolgten 4-Corner-Modells den Verzicht auf ein allgemeines Personenkennzeichen ermöglichen, liegen im oben erwähnten Gutachten bereits vor. Andererseits sollten aber auch grundlegendere Neukonzeptionen erforscht werden. Perspektivisch könnten verbesserte und effizientere Dienste im E-Government, E-Business und E-Justice erreicht werden, wenn staatliches Identitätsmanagement umfassender neu gedacht wird. So sind die fortgeschrittenen Identitätsmanagementlösungen der elektronischen Ausweisfunktion bisher nur eine Insellösung, die weder mit den Identitäten in staatlichen Registern zusammenhängt noch in nennenswertem Umfang in der Privatwirtschaft verwendet wird. Für ein umfassendes, verbessertes Identitätsmanagement sind aber auch Entwicklungen auf europäischer Ebene (z. B. EU Digital Identity Wallet) mit einzubeziehen. Denkbar ist mittel- bis langfristig auch die Einführung veränderter Betriebsmodelle, bei denen Register nicht mehr physisch dezentral geführt werden, sondern die dezentrale Struktur der Verwaltung durch verschlüsselte Datenspeicherung in staatlichen Cloud-Diensten abgebildet werden.

6. Die Registermodernisierung voranzutreiben, wird sicherlich zu Effizienzgewinnen beitragen. Eine verfassungskonforme, datenschutzgerechte Lösung auf dem Stand der Technik sollte aber Priorität genießen.

Berlin, 3. Juli 2023

Christoph Sorge