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

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)605

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.