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#IVZd70

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/