RECHTSWISSENSCHAFTLICHE FAKULTÄT
UNIVERSITÄT DES SAARLANDES

Lehrstuhl
für Rechtsinformatik

Prof. Dr. Christoph Sorge

Postfach 15 11 50
66041 Saarbrücken

Besucheranschrift:
Campus A5 4, Raum 0.25
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, 22. September 2024

Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Inneren Sicherheit und des Asylsystems, BT-Drucksache 20/12805 sowie zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, BT-Drucksache 20/12806

A. Vorbemerkung

Die Stellungnahme beschränkt sich auf einzelne Aspekte der vorliegenden Gesetzentwürfe, die die Verarbeitung personenbezogener Daten betreffen. In der Kürze der für die Stellungnahme zur Verfügung stehenden Zeit ist nur eine vorläufige Einschätzung möglich. Angesichts der umfangreichen Grundrechtseingriffe, die in den Entwürfen vorgesehen sind, wäre eine tiefgehende rechtliche Prüfung unter Berücksichtigung der technischen Rahmenbedingungen aber umso dringender geboten.

An der Stellungnahme haben meine Doktoranden Ass. iur. Nils Wiedemann, LL. M. (Dublin) und Dipl.-Jur. Maximilian Leicht, LL. M. mitgewirkt

B. Nachträglicher biometrischer Abgleich

§ 15b AsylG-E, § 10b BKAG-E, § 39a BKAG-E, § 63b BKAG-E und § 34b BPolG-E regeln nachträgliche biometrische Abgleiche mit öffentlich zugänglichen personenbezogenen Daten „aus dem Internet“.

Biometrische Abgleiche erscheinen für die vorgesehenen Zwecke nicht grundsätzlich ungeeignet. Wie auch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

(in ihrer Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, S. 3) feststellt, lässt sich dem Gesetzentwurf aber nicht entnehmen, wie ein solcher biometrischer Abgleich technisch umgesetzt werden soll. Auch die heranzuziehenden biometrischen Merkmale bzw. Eigenschaften werden in § 15b AsylG-E (anders als in § 10b BKAG-E, § 39a BKAG-E, § 63b BKAG-E und § 34b BPolG-E, die „biometrische Daten zu Gesichtern und Stimmen" benennen) nicht aufgeführt. So wird wohl die Verwendung von Gesichtsbildern vorausgesetzt, aber andere Merkmale wie z. B. Körperproportionen nicht erwähnt und insbesondere nicht ausgeschlossen. Auch § 16 Abs. 1 AsylG lässt sich eine entsprechende Beschränkung, etwa auf das Erstellen von Gesichtsbildern, nicht entnehmen.

Ob eine technische Umsetzung möglich ist, die sowohl mit den Vorgaben der DSGVO bzw. der JI-RL und der KI-Verordnung vereinbar ist als auch für die jeweiligen Anwendungszwecke einen nennenswerten Vorteil mit sich bringt, erscheint fraglich.

Konkret sei auf die folgenden Problemfelder hingewiesen:

I. Grundsätzliche Eignung biometrischer Verfahren nach Aufgabenstellung

Die Eignung biometrischer Verfahren unterscheidet sich erheblich zwischen den verschiedenen Aufgaben, für die diese Verfahren eingesetzt werden. **Dass biometrische *Verifikation* einer Identität sehr zuverlässig funktioniert, heißt gerade nicht, dass die gleiche Zuverlässigkeit für die *Identifizierung* einer Person erreicht werden kann.** Das ergibt sich bereits aus grundlegenden statistischen Überlegungen.

So ist die Verifikation einer behaupteten Identität – bei der etwa ein Gesichtsbild, das von einer sicher identifizierten Person hinterlegt oder aus einem elektronischen Identitätsdokument ausgelesen wurde, mit einem neu aufgenommenen Foto abgeglichen wird – eine vergleichsweise einfache Aufgabe, da lediglich ein 1:1–Vergleich vorgenommen werden muss. Entsprechend werden in der Literatur – abhängig vom für den Test verwendeten Datensatz – geringe Fehlerraten angegeben. Beispielsweise konnte für den Gesichtserkennungs-Datensatz „MegaFace Challenge 1" eine Quote von 97,96% korrekt bestätigten Übereinstimmungen bei einer Falsch-Positiv-Rate von 10^{-6}, also einer fälschlich bestätigten Übereinstimmung auf eine Million Versuche, erzielt werden.[1]

Ein Abgleich, mit dem eine Person erst identifiziert werden soll, erfordert dagegen ggf. Millionen Vergleiche, bei denen unterschiedlich große Übereinstimmungsgrade festgestellt werden. Eine gängige Bewertung solcher Verfahren besteht darin, die Treffer nach dem Grad der Übereinstimmung zu sortieren und das Verfahren als erfolgreich zu bewerten,

[1] *Minaee, Abdolrashidi, Su, Bennamoun, Zhang*: Biometrics recognition using deep learning: a survey, Artificial Intelligence Review (2023) 56:8647–8695, S. 8679, Tabelle 2.

wenn die tatsächliche Identität der gesuchten Person an erster Stelle (Rank-1) oder den ersten fünf Stellen (Rank-5) liegt. Nach dem „Rank-1"-Maßstab wurde unter Nutzung des gleichen Datensatzes („MegaFace Challenge 1") eine Genauigkeit von 95,023% erzielt.[2] Die Trainingsdaten des genannten Datensatzes bestehen aus 4,7 Millionen Fotos von 672 057 Personen.

Bei einem Abgleich mit einer unbestimmten Menge an öffentlich zugänglichen personenbezogenen Daten dürfte ein Vielfaches dieser Personenzahl erfasst werden, was zu einer reduzierten Genauigkeit führen dürfte. Gleichzeitig ist – im Gegensatz zu den genannten, in der wissenschaftlichen Forschung gängigen Evaluationen – nicht garantiert, dass überhaupt ein Foto der gesuchten Person über das Internet auffindbar ist. Das erschwert die Aufgabe der biometrischen Erkennung weiter, denn die bloße Ausgabe der Person mit der höchsten Übereinstimmung kann somit irreführend werden.

II. Erzielbare Genauigkeit

Realistisch erzielbare Genauigkeiten bei der Gesichtserkennung dürften trotz technischen Fortschritts in absehbarer Zeit **nicht ausreichen, um eine sichere Identifizierung allein durch Abgleich mit über das Internet öffentlich verfügbaren Daten zu ermöglichen**. Neben den oben genannten technischen Einschränkungen der biometrischen Identifikation hängt das auch damit zusammen, dass über das Internet auffindbare Fotos von Personen dort nicht zwingend mit der richtigen Identität verknüpft werden. Der Aufbau von Gesichtsdatenbanken durch staatliche Stellen dürfte dieses Problem verschärfen, da er einen Anreiz für die Betroffenen schafft, personenbeziehbare Profile zu löschen.

Ein ähnliches Bild dürfte sich für andere biometrische Daten (etwa Körperproportionen) ergeben, deren Auffindbarkeit etwa in Social Media erwartet werden kann.

Das bedeutet nicht, dass ein biometrischer Abgleich nutzlos wäre, denn er kann eines unter mehreren Indizien darstellen. **Es erscheint mir allerdings wichtig, darauf hinzuweisen, dass die Erwartungen in dieses Instrument nicht zu hoch gesetzt werden sollten.** Das dürfte sich auch auf die Verhältnismäßigkeitsprüfung auswirken, denn der vorgesehene Eingriff in die Rechte der Personen, deren Daten verarbeitet werden sollen, muss letztlich gegen den Nutzen der Maßnahme abgewogen werden.

III. Inaugenscheinnahme

Die in § 15b Abs. 2 AsylG-E vorgesehenen **Inaugenscheinnahme** im Fall eines Treffers ist sinnvoll; dass sie, wie in der Begründung des Entwurfs angegeben, durch zwei Personen erfolgen soll, sollte in den Normtext übernommen werden. **Ihr Effekt sollte aber ebenfalls**

[2] *Minaee, Abdolrashidi, Su, Bennamoun, Zhang*, S. 8679, Tabelle 2.

nicht überbewertet werden. Falsch positive Treffer des automatischen Abgleichs sind vermutlich besonders bei Personen zu erwarten, die der gesuchten sehr ähnlich sehen; gerade dann besteht aber auch für den menschlichen Betrachter eine erhöhte Irrtumswahrscheinlichkeit. Verschärft wird dieses Problem, wenn den menschlichen Betrachtern das Ergebnis des automatischen Abgleichs bekannt ist.

IV. Vereinbarkeit mit Art. 5 Abs. 1 lit. e KI-VO

Art. 5 Abs. 1 lit. e KI-VO verbietet „das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern". Diese Norm ist unklar, was auch zu einer gewissen **Unsicherheit für die vorliegenden Gesetzentwürfe** führt. Dem Wortlaut nach dürfte ein dem KI-Training vorgelagerter Prozess des Datensammelns, wenn er nicht von einem KI-System durchgeführt wird, nicht unter das Verbot fallen. Dafür spricht auch der Wortlaut des Art. 2 Abs. 8 KI-VO. Denn andernfalls würde Art. 5 Abs. 1 lit. e KI-VO ein faktisches Verbot des Scraping von Gesichtsbildern für die Entwicklung von KI-Systemen bedeuten.

Nach dieser Auslegung läuft das Verbot des Art. 5 Abs. 1 lit. e KI-VO aber de facto leer. Denn reguliert wird nur der Einsatz eines KI-Systems für das *ungezielte* Auslesen von Gesichtsbildern. Sofern aber gerade ein ungezieltes Auslesen durchgeführt wird, wäre der Einsatz eines KI-Systems hierfür gar nicht erforderlich. Diese Überlegungen werden auch durch ErwG 43 KI-VO gestützt, der als Gründe für das Verbot eine Verstärkung des Gefühls der Massenüberwachung sowie schwere Verstöße u.a. gegen das Recht auf Privatsphäre nennt. Diese Gründe dürften jedoch regelmäßig unabhängig davon vorliegen, ob für das ungezielte Auslesen ein KI-System eingesetzt wird. Geht man deshalb davon aus, dass eine solche Beschränkung – Verbot des ungezielten Auslesens nur bei Einsatz eines KI-Systems – vom Unionsgesetzgeber nicht gewollt ist, könnte man mit einer teleologischen Auslegung möglicherweise dazu kommen, dass das Verbot für das Scraping von Gesichtsbildern schon im Vorfeld des KI-Trainings anwendbar ist.

Diese Auslegung unterstellt, ist die praktische Umsetzung des biometrischen Abgleichs (wie er in § 15b AsylG-E, § 10b BKAG-E, § 39a BKAG-E, § 63b BKAG-E und § 34b BPolG-E vorgesehen ist) kaum mehr rechtskonform möglich. Gesichtsbilder stellen in den geplanten Anwendungsbereichen die wohl relevanteste bzw. einzig relevante Grundlage für den biometrischen Abgleich dar; diese müssten zudem tatsächlich ungezielt „aus dem Internet" heruntergeladen werden. Theoretisch sind zwar Gestaltungen denkbar, bei denen keine Datenbanken von im Internet aufgefundenen Bildern benötigt werden:

- Einerseits könnten die Lichtbilder der zu identifizierenden Personen gesammelt und in regelmäßigen Crawler-Durchläufen, bei denen (etwa im Monatsrhythmus) immer

wieder neu das World Wide Web durchsucht wird, mit den dort aufgefundenen Bildern abgeglichen werden.

- Andererseits könnte ein Modell mit jeweils einzeln beim Durchsuchen des World Wide Web aufgefundenen Bildern trainiert werden – wenn man davon ausgeht, dass weder das Modell noch zusätzlich zu speichernde Verknüpfungen zu den Fundstellen der aufgefundenen Bilder in ihrer Gesamtheit eine Datenbank i.S.d. Art. 5 Abs. 1 lit. e KI-VO darstellen.

Beide Ansätze erscheinen aber kaum praktikabel; sie sind zudem mit rechtlichen Risiken verbunden, da eine teleologische Auslegung des Art. 5 Abs. 1 lit. e KI-VO durchaus beide Ansätze erfassen könnte.

V. Vereinbarkeit mit Art. 9 DSGVO bzw. Art. 10 JI-RL

Sofern man eine Anwendbarkeit des Verbots aus Art. 5 Abs. 1 lit. e KI-VO ablehnt – wofür gute Gründe sprechen –, bedeutet dies aber nicht, dass der Aufbau einer Datenbank mit öffentlich zugänglichen Gesichtsbildern aus dem Internet ohne Weiteres rechtlich zulässig ist. So erlaubt zwar Art. 9 Abs. 2 lit. e DSGVO bzw. Art. 10 lit. c JI-RL die Verarbeitung offensichtlich öffentlich gemachter biometrischer Daten. Nach der – auf dem insoweit auch eindeutigen Wortlaut der Norm beruhenden – Rechtsprechung des EuGH gilt diese Ausnahme aber nur für solche Daten, die von der betroffenen Person selbst offensichtlich öffentlich gemacht worden sind und damit nicht für Daten, die andere Personen betreffen. **Öffentlich zugängliche Gesichtsbilder werden in einer Vielzahl der Fälle nicht nur das Gesicht der betroffenen Person, die das Gesichtsbild öffentlich zugänglich gemacht hat, sondern auch Gesichter anderer Personen beinhalten.** Hinsichtlich der Gesichter anderer Personen können Art. 9 Abs. 2 lit. e DSGVO bzw. Art. 10 lit. c JI-RL aber gerade nicht als Ausnahme vom grundsätzlichen Verbot der Verarbeitung biometrischer Daten dienen. Eine entsprechende Differenzierung ist im Vorschlag jedoch nicht zu erkennen.

Ferner ist auch hinsichtlich der betroffenen Person diese Ausnahme vom Grundsatz des Verbots der Verarbeitung biometrischer Daten eng auszulegen, so dass es der Absicht der betroffenen Person bedarf, die fraglichen personenbezogenen Daten ausdrücklich und durch eine eindeutige bestätigende Handlung der breiten Öffentlichkeit zugänglich zu machen.[3] Für das Vorliegen dieser Voraussetzungen kommt es gerade im Social-Media-Bereich entscheidend auf die Einstellungsmöglichkeiten oder – in Ermangelung dieser – auf die der betroffenen Person zur Verfügung gestellten Informationen an. Aufgrund dieser engen Auslegung werden daher selbst bei der betroffenen Person, die die Gesichtsbilder öffentlich gemacht hat, die Voraussetzungen des Art. 9 Abs. 2 lit. e DSGVO bzw. Art. 10 lit. c JI-RL häufig nicht vorliegen.

[3] EuGH, Urteil vom 04. Juli 2023, C-252/21, Rn. 76 f.

In der Literatur wird darüber hinaus davon ausgegangen, dass selbst die Tatsache, dass eine betroffene Person selbst ein Gesichtsbild bewusst öffentlich zugänglich gemacht hat, nicht impliziert, dass auch die daraus ableitbaren biometrischen Daten als offensichtlich öffentlich zugänglich gemacht gelten.[4] Das wird auch durch den Europäischen Datenschutzausschuss vertreten.[5] Möglicherweise wird die anstehende Entscheidung des EuGH in der Rechtssache C-446/21 zur Klärung dieser Frage beitragen.

Darüber hinaus erscheint es im Lichte der Rechtsprechung des EuGH rechtlich problematisch, die Erhebung der öffentlich zugänglichen biometrischen Daten auf allgemeine Ermittlungsbefugnisse zu stützen.[6] **Auch die geplanten Vorschriften implizieren eine umfassende Erhebung von biometrischen Daten, die durch den vergleichsweise schwach ausgeprägten Schutz äußerst problematisch erscheint. Die Normen werden daher sehr wahrscheinlich die Anforderungen des Unionsrechts nicht erfüllen.**

Zudem sei darauf hingewiesen, dass die geplanten Vorschriften mangels geeigneter Garantien **auch den Anforderungen von Art. 9 Abs. 2 lit. g DSGVO bzw. Art. 10 lit. a JI-RL nicht genügen dürften.** Die Begründung zu § 15b Abs. 1 AsylG-E stützt sich zwar auf Art. 9 Abs. 2 lit. g DSGVO. Sie führt aus, die Verarbeitung sei „aus Gründen eines erheblichen öffentlichen Interesses erforderlich“ und stehe „in angemessenem Verhältnis zu dem verfolgten Ziel“ (Drucksache 20/12805, S. 23). Für die Verarbeitung der personenbezogenen Daten der zu identifizierenden Person ist das auch durchaus plausibel. Das gilt aber nicht für die über das Internet abgerufenen Daten Dritter ohne Bezug zu dem Verfahren.

Ohnehin ist fraglich, ob die unbeschränkte Erfassung öffentlich zugänglicher Daten einer ebenfalls unbeschränkten Personenzahl den in Art. 5 Abs. 1 lit. c DSGVO bzw. Art. 4 Abs. 1 lit. c JI-RL festgelegten Grundsätzen entsprechen kann. Entsprechendes gilt auch im nationalen Recht für die Vereinbarkeit mit dem Informationellen Selbstbestimmungsrecht (Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG).

VI. Datenquellen

Der Entwurf lässt **unklar, welche Datenquellen herangezogen werden können**. Das Internet ist ein Kommunikationsnetz, auf dessen Grundlage zahlreiche Dienste (wie E-Mail, Audio- und Videokonferenzen etc.) angeboten werden. Der Entwurf kann unproblematisch so ausgelegt werden, dass wohl nur über das Internet zum Abruf für die Öffentlichkeit bereitgehaltene Daten erfasst werden sollen. Offen bleibt aber, ob Dienste, deren Inhalte nur nach Anmeldung abgerufen werden können, adressiert werden – gerade Social-Media-Dienste, bei denen das oft der Fall ist, dürften in großem Umfang die für den biometrischen

[4] Wendehorst in Martini/Wendehorst, KI-VO Art. 5 Rn. 91, im Erscheinen

[5] EDSA, Leitlinien 05/2022 über den Einsatz von Gesichtserkennungstechnologie im Bereich der Strafverfolgung, Version 2.0, angenommen am 26. April 2023, S. 6

[6] Vgl. dazu die Anmerkung von Benamor in ZD 2024, 264 (269) zu EuGH, Urteil vom 30. Januar 2024, C-118/22.

Abgleich nützlichen Bilddaten mit Personenzuordnung enthalten. Die genannten Dienste sind technisch in der Lage, den massenhaften Download von Daten zu unterbinden. Daher kann diese Datenquelle praktisch nur aufgrund einer Vereinbarung mit dem Diensteanbieter genutzt werden. Hier stellt sich auch die Frage, ob ggf. bereits vorhandene Erkenntnisse dieser Diensteanbieter durch BKA, Bundespolizei und BAMF genutzt werden könnten – denn zur Gesichtserkennung sind auch diese selbstverständlich in der Lage. Wird gezielt nach bestimmten Personen(gruppen) gesucht, ist dies für den Diensteanbieter nachvollziehbar; wie damit umzugehen ist, wäre zu regeln.

Zu prüfen wären hier auch urheber- bzw. leistungsschutzrechtliche Fragestellungen, da zum Abgleich gesammelte Bilder regelmäßig entsprechend geschützt sein dürften und unionsrechtliche Vorgaben bestehen, die den Gestaltungsspielraum des nationalen Gesetzgebers einschränken. So definiert Art. 4 Abs. 1, 2 der Richtlinie 2019/790 (Urheberrechtsrichtlinie) zwar eine Schranke für Text und Data Mining, doch gibt Art. 4 Abs. 3 der Richtlinie dem Rechteinhaber die Möglichkeit, den Schutzgegenstand mit einem Nutzungsvorbehalt zu versehen.

C. Maschinelles Lernen und Diskriminierung

§ 15b Abs. 7 Satz 2 AsylG-E und § 22 Abs. 3 Satz 2 BKAG-E enthalten Regelungen, die wohl insbesondere auf das Training maschineller Lernverfahren abzielen. Sie verpflichten das BAMF bzw. das BKA, sicherzustellen, dass „diskriminierende Algorithmen weder herausgebildet noch verwendet werden“. Die Normen sind aber völlig unklar. Selbst bereits bestehende Diskriminierungsverbote stellen die Entwickler von KI-Systemen vor Herausforderungen, da in der Informatikliteratur sehr unterschiedliche Ansätze diskutiert werden, mit denen sich die „Fairness“ bzw. umgekehrt die Diskriminierung durch Klassifikationsverfahren messbar machen lassen könnten. Ob einer dieser Ansätze die rechtlichen Anforderungen angemessen abbildet, ist aber noch ungeklärt.

§ 15b Abs. 7 Satz 2 AsylG-E und § 22 Abs. 3 Satz 2 BKAG-E benennen ebenfalls keinen Maßstab für die geforderte Diskriminierungsfreiheit; außerdem sind aber auch die geschützten Gruppen nicht benannt. Für den Anwendungsfall der Identifikation (wie in § 15b AsylG-E ausschließlich und in § 22 Abs. 3 BKAG-E wohl auch erfasst) lassen sich kaum sinnvolle Maßnahmen aus der Anforderung der Gesetzentwürfe ableiten, denn eine Nichtberücksichtigung von etwa in Art. 3 Abs. 3 GG genannten – oder mit diesen korrelierten – Merkmalen ist kaum mit einer zuverlässigen Identifikation vereinbar.

D. § 16a BKAG-E

§ 16a BKAG-E erscheint äußerst weitreichend und auch unklar. So erschließt sich nicht, welche Daten etwa nach § 16a Abs. 1 S. 2 BKAG-E konkret zusammengeführt

werden können. Wie die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (in ihrer Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, S. 7) zu Recht feststellt, ist in der Begründung des Gesetzentwurfs eine noch weiterreichende Absicht formuliert, Daten auch einzelfallunabhängig zusammenzuführen.

Wie bereits zu den Normen zum biometrischen Abgleich angemerkt, **fehlt es zudem an einer Konkretisierung, die wenigstens Kernaspekte der vorgesehenen technischen Umsetzung festlegt.** Nur mit einer solchen Konkretisierung wäre es auch möglich, zu prüfen, ob die einzelfallunabhängige Zusammenführung (wie in S. 20 der Drucksache 20/12806 angegeben), tatsächlich technisch erforderlich ist – woran zumindest Zweifel bestehen.

§ 16a BKAG-E lässt zudem völlig unklar, wann und unter welchen Bedingungen die zusammengeführten Daten wieder gelöscht werden müssen. Aus der Gesetzesbegründung zu § 16a Abs. 1 BKAG-E ergibt sich zudem, dass auch Daten aus externen Quellen, die zwar rechtmäßig erhoben, aber nur zwischengespeichert werden, für die Analysen verwendet werden können. Dies ermöglicht eine weitreichende Analyse, ohne dass ausreichende Sicherheitsvorkehrungen zum Schutz dieser Daten getroffen werden, die gerade nicht längerfristig gespeichert werden sollen.

Zudem ist nicht ersichtlich, ob die zusammengeführten Daten als „vorhandene Daten“ im Sinne des § 22 BKAG-E zu verstehen sind und entsprechend nach § 22 BKAG-E weiterverarbeitet werden können.

Insgesamt ergibt sich, dass **§ 16a BKAG-E** – insbesondere wenn die nach der Gesetzesbegründung angestrebte, einzelfallunabhängige Datenbank von der Norm umfasst sein sollte – **aufgrund der umfassenden Verarbeitungsbefugnisse weder mit Art. 4 Abs. 1 lit. c JI-RL noch mit dem Recht auf Informationelle Selbstbestimmung nach Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG vereinbar sein dürfte**.

E. § 22 BKAG-E

Auch § 22 BKAG-E erscheint zu weitreichend, da eine nahezu unbegrenzte Übermittlung personenbezogener Daten ermöglicht wird. Es besteht auch das Risiko, dass aus trainierten Modellen personenbezogene Daten ableitbar sind. Zwar wird dieses Risiko teilweise dadurch adressiert, dass für die weitere Verwendung der personenbezogenen Daten selbstverständlich die einschlägigen datenschutzrechtlichen Regeln gelten, doch sollte es dennoch bereits im Vorfeld – also bei der Übermittlung nach § 22 BKAG-E – berücksichtigt werden.

§ 22 Abs. 3 Satz 1 Nr. 1, Nr. 2 BKAG-E werfen auch aus technischer Sicht Fragen auf. So ist eine Pseudonymisierung bei größeren Datenbeständen zwar oft nur wenig wirksam, da eine Profilbildung anhand pseudonymisierter Daten in vielen Fällen selbst ohne direkte Kenntnis der Zuordnungsvorschrift Rückschlüsse auf die Identität der Betroffenen erlaubt und damit

am Personenbezug nichts ändert. Sie ist aber in den meisten Fällen mit verhältnismäßigem Aufwand möglich. Eine Anonymisierung hingegen ist bei solchen Datenbeständen in aller Regel tatsächlich schwierig.

Unklar ist auch, ob der Entwurf die Anonymisierung oder Pseudonymisierung als Veränderung (im Sinne des § 22 Abs. 3 Satz 1 Nr. 1 BKAG-E) versteht und ob die Voraussetzungen der § 22 Abs. 3 Satz 1 Nr. 1, Nr. 2 BKAG-E – angesichts der in der Regel einfachen Pseudonymisierung – nicht eher kumulativ zu verstehen sein sollten.

In der Informatikforschung wird der technische Datenschutz im maschinellen Lernen schon seit vielen Jahren untersucht; es ist anzuraten, die dort gewonnenen Erkenntnisse auch im Kontext des § 22 Abs. 3 BKAG-E in die Praxis umzusetzen.

F. Fazit

Insgesamt lässt sich feststellen, dass mit den betrachteten Regelungen legitime Ziele verfolgt werden. Sie sind jedoch insgesamt insbesondere aus zwei Gründen hochproblematisch:

1. Weder den Normtexten noch der Begründung des Gesetzentwurfs lässt sich eine auch nur ansatzweise konkretisierte technische Konzeption entnehmen. Somit kann nicht beurteilt werden, ob die angestrebte Umsetzung tatsächlich möglich sein wird; vieles deutet aber darauf hin, dass zu hohe Erwartungen in die geplanten technischen Lösungen gesetzt werden. Nur auf Basis einer Konkretisierung der geplanten Verarbeitungen ließen sich auch konkrete technische Schutzmaßnahmen ausarbeiten. Es ist denkbar, dass solche Maßnahmen eine grundrechtsschonende Umsetzung der Bedarfe des BAMF und der Sicherheitsbehörden ermöglichen könnten; auf Grundlage des vorliegenden Entwurfs ist eine Ableitung konkreter technischer Maßnahmen allerdings ausgeschlossen.
2. Damit zusammenhängend umfassen die sehr breit gefassten Normen mögliche Verarbeitungen, die weder mit nationalem Verfassungsrecht noch mit Unionsrecht vereinbar sein dürften. Dem Gesetzgeber ist daher eine wesentlich striktere Eingrenzung der geplanten Befugnisse sowie insbesondere ein Verzicht auf das Anlegen neuer, umfangreicher Datenbanken „auf Vorrat“ anzuraten.

Saarbrücken, 22. September 2024

Christoph Sorge