Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)493 H

BfDI | Postfach 1468 | 53004 Bonn

Stellvertretenden Vorsitzenden
des Ausschusses für Inneres und Heimat
des Deutschen Bundestages
Herrn Prof. Dr. Lars Castellucci
Platz der Republik 1
11011 Berlin

E-Mail: Innenausschuss@bundestag.de

Prof. Dr. Louisa Specht-Riemenschneider
Die Bundesbeauftragte

Telefon: +49 228 997799 5000

E-Mail: bfdi@bfdi.bund.de

Aktenz.: 32-642/041#1723
(bitte immer angeben)
Dok.: 86711/2024

Anlage:

Bonn, 20.09.2024

Anhörung im Ausschuss für Inneres und Heimat am Montag den 23.September 2024

Sehr geehrter Herr Abgeordneter,

anbei übersende ich meine ergänzte Stellungnahme zur Vorbereitung des Anhörungstermins.

Mit freundlichen Grüßen

Prof. Dr. Louisa Specht-Riemenschneider

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 16.09.2024

Stellungnahme

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung

Bundestagsdrucksache 20/12806

sowie

zum Entwurf eines Gesetzes zur Verbesserung der inneren Sicherheit

und des Asylsystems

Bundestagsdrucksache 20/12805

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

A. Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung

Grundsätzliche Anmerkungen

Gesetzliche Grundlagen zur automatisierten Datenanalyse und zur biometrischen Identifizierung von Personen befinden sich schon seit längerer Zeit in der Diskussion. Auf Arbeitsebene gab es eigentlich bereits eine Vielzahl konstruktiver Gesprächen zwischen meinem Haus und dem Bundesministerium des Innern, wie polizeiliche IT modern, effektiv und gleichzeitig grundrechtskonform gestaltet werden kann. Sowohl für eine effektive Polizeiarbeit als auch für die Wahrung der Grundrechte betroffener Personen ist es wichtig, dass für neue Gesetze eine gründliche Vorarbeit geleistet wird. Natürlich muss der Gesetzgeber im Blick haben, dass die Polizeibehörden sinnvolle Werkzeuge erhalten. Er muss aber ebenso die Grundrechte aller betroffener Personen wahren. **Daher sollten Ermächtigungsgrundlagen für grundrechtsintensive Maßnahmen nicht übereilt geschaffen werden.** Dies gilt hier umso mehr, als dass am 1. Oktober 2024 eine wichtige Entscheidung des Bundesverfassungsgerichts zu Kernregelungen des BKA-Gesetzes (BKAG) verkündet wird.

Ohne die künftige Entscheidung des Bundesverfassungsgerichts zu Kernvorschriften des BKAG zu kennen, möchte ich nach Durchsicht des Gesetzentwurfs aber auf einige wichtige Punkte aufmerksam machen.

1. Gesichtserkennung

Der Gesetzentwurf regelt den biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet. Sowohl die §§ 10b, 39a, 63b des Entwurfs zur Änderung des Bundeskriminalamtgesetzes (BKAG-E) als auch § 34b des Entwurfs zur Änderung des Bundespolizeigesetzes (BPolG-E) und § 98d des Entwurfs zur Änderung der Strafprozessordnung (StPO-E) beinhalten vergleichbare Regelungen. Alle Eingriffsnormen weisen zu unscharfe Tatbestandsmerkmale auf und ermöglichen erhebliche Eingriffe in die Rechte unbeteiligter Personen.

Ferner sind die Regelungen nicht mit der KI-Verordnung in Einklang zu bringen. Diese verbietet unter anderem die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsmaterial erstellen oder erweitern.[1] **Der Gesetzentwurf lässt eine Darstellung vermissen, wie der Einsatz der Gesichtserkennungstechnologie technisch ermöglicht werden soll.** Da die Polizeibehörden nach der KI-Verordnung nicht eine eigene

[1] Art. 5 Abs. 1 lit. e) KI-Verordnung

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

umfassende Datenbank zur Gesichtserkennung anlegen dürfen, aber nach allgemeiner Ansicht auch nicht Kunden etablierter kommerzieller Anbieter wie PimEyes oder Clearview AI werden sollten, müssten sie für jeden Abgleich von Gesichtsbildern den aktuellen Lichtbildbestand des Internets erheben. Dies ist unter den heutigen technischen Gegebenheiten unrealistisch.

Weiterhin besteht dadurch, dass alle Normen im BKAG auf die Weiterverarbeitungsregelungen des § 12 Abs. 2 BKAG Bezug nehmen,[2] die Gefahr, dass faktisch eine dauerhafte Spiegelung vieler Dateien des Internets beim Bundeskriminalamt vorgehalten wird. § 12 BKAG steht seinerseits in Bezug mit der Generalklausel des BKAG zur Datenverarbeitung in § 16 BKAG (Gegenstand des Verfassungsbeschwerdeverfahrens, Urteil am 1.10.2024). Durch die sukzessive Abarbeitung der Abgleiche lägen sodann in diesen Fällen die Voraussetzungen des § 12 Abs. 2 BKAG vor. Beispielhaft können nach § 10b BKAG-E dann Speicherungen der Vergleichsdaten bei gewerbsmäßigen Kontoeröffnungsbetrugstaten im Internet erfolgen. Diese Vergleichsdateien könnten sehr lange vorgehalten werden, wenn die Abgleiche nun sukzessive erfolgen.

§§ 10 b Abs. 1 Satz 2, 39 a Abs. 1 Satz 3, 63b Abs. 1 Satz 2 BKAG-E und § 34 b Abs. 1 S. 2 BPolG-E stellen klar, dass ein Abgleich mit biometrischen Daten aus im Internet öffentlich zugänglichen Echtzeit-Lichtbild und Echtzeit- Videodaten ausgeschlossen wird. Einen Ausschluss bezüglich Stimmdaten enthalten die Vorschriften nicht. Es wird davon ausgegangen, dass es sich um ein redaktionelles Versehen handelt. Anderenfalls wäre nicht zu erklären, warum diese biometrischen Daten anders behandelt werden sollen.

- **Zu § 10b BKAG-E**

Die Regelung nimmt Bezug auf den Katalog des § 100a Abs. 2 StPO. Dieser Straftatenkatalog unterliegt ständigen Erweiterungen und Neuregelungen, so dass er nicht mehr geeignet ist, um eine Maßnahme trennscharf auf schwere Taten zu beschränken. Insoweit sei beispielhaft auf die durch Nr. 1 Buchstabe n) erfassten Fälle eines über einen längeren Zeitraum und damit gewerbsmäßig begangenen Sozialhilfebetrugs oder die nach Nr. 7 Buchstabe a) erfassten Fälle regelmäßiger und damit gewerbsmäßiger „Kleindealerei“ verwiesen. **Eine Bezugnahme auf den Katalog der Bezugstaten in § 138 StGB ist eher geeignet, um eine taugliche Abgrenzung mit Blick auf schwere Taten zu schaffen.**

Auch der Adressatenkreis der Neuregelung ist zu weit gefasst. Nach § 10 Abs. 2 BKAG-E in Verbindung mit § 19 Abs. 1 Satz 1 Nr. 1 und 2 BKAG können sich Maßnahmen auch gegen Zeugen und Opfer künftiger Straftaten richten. Die Suche nach einem Opfer einer künftigen Straftat zur Verhinderung derselben im Bereich der Verhütung schwerer Straftaten ist

[2] siehe §§ 10 b Abs. 3, 39 a Abs. 6, 63b Abs. 6 BKAG-E

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

der Kernbereich der Gefahrenabwehr. Sollte die unbeteiligte Person allerdings „nur“ Zeuge sein, so liegt ein unverhältnismäßiger Eingriff in die Rechte einer unbeteiligten Person vor. Zum Beispiel könnten hier mit Blick auf die Zentralstellenfunktion bereits bei einer gewerblichen Hehlerei die biometrischen Daten eines gutgläubigen Kunden eines kriminellen Pfandhausbetreibers mit öffentlich zugänglichen Daten aus dem Internet abgeglichen werden. **Der Verweis auf § 19 Abs. 1 Nr. 1 BKAG ist meines Erachtens zu streichen.**

Die Vorschrift des § 10b Abs. 7 ist zu unbestimmt. Zwar fordert die Vorschrift, dass die Daten zu löschen sind, soweit sie keinen konkreten Ermittlungsansatz für den Ausgangssachverhalt aufweisen. Die Auslegung des Rechtsbegriffs ist zu unbestimmt, um eine rechtssichere Datenlöschung zu ermöglichen. Es besteht die Gefahr, dass Daten missbräuchlich vorgehalten werden, in dem auf den Abschluss von Ermittlungen in einem größeren Kontext verwiesen wird. **Es bedarf einer klaren Regelung, dass die Daten, sofern sie nicht als Beweismittel in einem Strafverfahren dienen können, sofort zu löschen sind.**

Einer genaueren verfassungsrechtlichen Prüfung bedürfte auch die Gesetzgebungskompetenz. Auf die Zentralstellenkompetenz nach Art. 73 Nr. 10 GG wurden bislang nur Datenerhebungen des BKA von geringer Eingriffsintensität gestützt, die für die von der Zentralstelle zu erledigenden Koordinierungsaufgaben konzentriert war.

- **Zu § 39a BKAG-E**

In Satz 2 der Vorschrift wird auf die Begehung von Straftaten und nicht mehr auf das Vorliegen einer Gefahr abgestellt. Zu beachten ist, dass das Bundesverfassungsgericht die Verschiebung vom Gefahrenbegriff zu einem Blick auf schwere Taten zulässt, aber dann auch Anlasstaten, die im Höchstmaß mit einer Freiheitsstrafe von mindestens 10 Jahren bedroht sind, fordert.[3] Diesen Anforderungen wird § 39a BKAG-E durch die Bezugnahme auf § 5 Abs. 1 Satz 2 BKAG und § 129a Abs. 2 StGB nicht gerecht, weil letzterer auch auf Delikte aus dem Bereich der mittleren Kriminalität verweist. **Auch hier bietet sich eine Bezugnahme auf § 138 Abs. 1 StGB an.**

Auch hier ist der Adressatenkreis durch die Bezugnahme auf die §§ 17, 18, 20 des Bundespolizeigesetzes zu weit gefasst. Man muss sich bereits die Frage der Eignung einer Maßnahme stellen, wenn man sie nach § 17 Abs. 2 BPolG nicht nur gegen ein Kind, welches die Gefahr verursacht, sondern auch gegen den Erziehungsberechtigten oder den Betreuer richten kann. Ferner läge in diesen Fällen ein erheblicher Eingriff in das Grundrecht der informationellen Selbstbestimmung der Betreuungsperson vor. Sofern die Möglichkeit be-

[3] Vgl. BVerfG, NJW 2004, 999 (1011).

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

steht, die Maßnahme gegen völlig unbeteiligte Personen zu richten (§ 20 BPolG) ist der Eingriff aufgrund seiner Schwere ebenfalls nicht zu rechtfertigen. **Auch aus systematischen Gründen wäre hier ein Verweis auf § 18 Abs. 1 BKAG sachgerecht.**

- **Zu § 63b BKAG-E**

Die geschilderten Bedenken bestehen auch bezüglich dieser Vorschriften.

- **Zu § 34b BPolG-E**

Die in § 34b Abs. 1 S. 2 BPolG-E aufgeführten Straftatbestände grenzen den Anwendungsbereich der Vorschrift nicht ausreichend ein. Hierbei ist zunächst der Begriff einer „Straftat im Zusammenhang mit lebensgefährdenden Schleusungen“ zu unbestimmt, um einen solchen Eingriff zu rechtfertigen. Bereits aus Gründen der Rechtssicherheit sollten die in Frage kommenden Delikte daher abschließend benannt werden. Zudem sollten auch die Straftaten „die gegen die Sicherheit der Anlagen oder des Betriebes des Luft-, See- oder Bahnverkehrs gerichtet“ sind, abschließend aufgeführt werden. In ihrer derzeitigen Ausgestaltung nennt die Vorschrift hier „insbesondere“ Straftaten nach den §§ 315, 315b, 316b und 316c StGB. Hierbei sind gefährliche Eingriffe in den Straßenverkehr (§ 315b StGB) sowie die Störung öffentlicher Betriebe (§ 316b StGB) lediglich mit einer Höchststrafe von 5 Jahren bedroht und somit dem Bereich der mittleren Kriminalität zuzuordnen. Besser wäre auch hier ein Verweis auf § 138 Abs. 1 StGB, ggf. beschränkt auf dort genannte Straftaten im Aufgabenbereich der Bundespolizei.

Der Adressatenkreis ist zu weit gefasst, siehe oben zu § 39a BKAG-E.

- **Zu § 98d StPO-E**

Auch hier ist der Adressatenkreis zu weit gefasst. Die Maßnahme kann auch gegen nicht beschuldigte Personen, nach denen für die Zwecke des Strafverfahrens gefahndet wird, gerichtet werden. Dies ermöglicht, sofern der Begriff der „Fahndung“ nicht auf Maßnahmen nach den §§ 131 ff. StPO beschränkt wird, einen Eingriff in die Rechte von möglichen Zeugen unabhängig von der Frage, ob ihre Angaben für das Ermittlungsverfahren von besonderer Relevanz wären. Es muss daher bereits vom Wortlaut deutlich werden, dass der Begriff „Fahndung“ hier nicht im umgangssprachlichen Sinne zu verstehen ist. Ferner bedarf es einer Beschränkung auf die Fälle, in denen die Aussage der sonstigen Person für die Fortführung der Ermittlungen unerlässlich ist. Es bestünde in der jetzigen Ausgestaltung der Norm bei einer videografierten Tatbegehung auf einem Volksfest die Möglichkeit, die biometrischen Daten einer Vielzahl möglicher unbeteiligter Besucher des Festes als Zeugen mit im Internet öffentlichen Daten automatisch abzugleichen, nur um diese als Zeugen

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

zu identifizieren, ohne dass dies für die Ermittlungen von ausschlaggebender Bedeutung sein muss. **Neben der erwähnten Ausschärfung des Begriffes der Fahndung bedarf es hier der Einschränkung dahingehend, dass durch die Ermittlung der unbeteiligten Person für das Ermittlungsverfahren voraussichtlich essentielle Erkenntnisse gewonnen werden können.**

Darüber hinaus gelten hier die oben dargestellten Bedenken in Bezug auf den Katalog des § 100a StPO ebenfalls. Die Maßnahme ist zu eingriffsintensiv, um sie für alle dort aufgeführten Delikte freizugeben. **Auch hier bietet sich der Verweis auf § 138 Abs. 1 StGB an.**

§ 98d Abs. 5 StPO-E, der die Löschung nicht mehr benötigter Daten regelt, unterliegt den gleichen Bedenken, wie die vergleichbaren Normen des BKAG-E. **Sachgerecht wäre die sofortige Löschung der abgeglichenen Daten nach Dokumentation des Abgleichergebnisses.**

2. Automatisierte Datenanalyse

- **Zu § 16a BKAG-E**

Die Vorschriften zur automatisierten Datenanalyse in § 16a BKAG-E sind viel zu weit gefasst. Es besteht das Risiko, dass auf Grundlage dieser Norm eine umfassende Datensammlung im Sinne einer Super-Datenbank beim BKA aufgebaut wird. Auch wenn die sprachliche Fassung des § 16a BKAG-E dies auf den ersten Blick nicht nahelegt, ist es ausweislich der Begründung das ausdrückliche Ziel der Regelung.[4]

Möglich werden soll – dauerhaft und unabhängig von einem konkreten Vorgang – die Zusammenführung *aller* Daten aus dem Informationssystem des BKA und dem polizeilichen Informationsverbund *aller* deutschen Polizeibehörden. Dies umfasst eine Vielzahl von Daten Beschuldigter, Opfer, Zeugen oder sogar gänzlich unbeteiligter Personen. Jeder, der einen Wohnungseinbruch anzeigt, kann in dieser Datenbank erfasst werden, wenn ein überregionaler Bezug besteht. Sofern der Einbruch unaufgeklärt bleibt bis zur Verjährung, also für mindestens zehn Jahre. Zudem handelt es sich um Daten sehr unterschiedlicher Sensibilität, von bloßen Adressen über medizinische Gutachten bis hin zu Namen von Vergewaltigungsopfern und Angaben über Details solcher Taten.

[4] Siehe Seite 20 der BT-Drucks., Begründung zu § 16a Abs. 1: „Die Zusammenführung muss aus technischen Gründen vom Einzelfall und weiteren Eingriffsschwellen unabhängig sein. Die Daten können nur dann schnell und effizient analysiert werden, wenn zumindest der Grunddatenbestand bereits zusammengeführt und aktualisiert in einem einheitlichen Datenformat in einer entsprechenden Anwendung vorliegt.“.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Das Bundesverfassungsgericht hat die Bedingungen und Grenzen der automatisierten Datenanalyse durch Sicherheitsbehörden umfassend festgelegt.[5] Nach der Entscheidung ist zunächst zu prüfen, welche Begrenzungen der Gesetzgeber vorsieht, um die Eingriffsintensität abzumildern. Diese betreffen zum einen die einzubeziehenden Daten und Personen. Hier setzt der vorliegende Gesetzentwurf wie dargestellt keinerlei Grenzen. Zum anderen beziehen sie sich auf die eingesetzten Analysemethoden. Auch hier finden sich keine Grenzen, die Regelung ist bewusst technikneutral formuliert und umfasst daher auch die Anwendung künstlicher Intelligenz.[6] **Die Eingriffsintensität der mit dem vorliegenden Entwurf beabsichtigten Praktiken ist also maximal hoch und bedarf dringend der Einschränkung.**

Ferner ist festzustellen, dass das Bundesverfassungsgericht in seiner Entscheidung keine Aussagen über eine dauerhaft zugrundeliegende Datenbank getroffen hat. Es ging anscheinend davon aus, dass jeweils im Zeitpunkt der automatisierten Datenanalyse der dafür verarbeitete Datenbestand zusammengestellt wird. **Die hier beabsichtigte, dauerhaft angelegte Datenbank stellt einen darüber hinaus gehenden, äußerst schwerwiegenden Eingriff dar, welcher nach hiesigem Erachten nicht mit dem Grundgesetz vereinbar ist.**

Sodann ist zu prüfen, welche Eingriffsschwellen der Gesetzgeber festlegen muss. Bei intensiven Eingriffen fordert das Gericht als Schwelle mindestens eine konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut.[7] Dieser Anforderung wird nur die Schwelle in Absatz 1 Satz 1 gerecht. Insoweit sich der Gesetzentwurf in Absatz 1 Satz 2 wiederum von dem klassischen Gefahrenbegriff löst und auf Straftaten abstellt, wird auf die oben zu § 39a BKAG-E dargestellten Bedenken Bezug genommen. Es stellt sich bei Absatz 3 die Frage, ob für die Zentralstellentätigkeit eine derart tiefgreifend in Grundrechte eingreifende Ermächtigung angemessen ist. Die Zentralstellentätigkeit beinhaltet nur koordinierende Aufgaben, aber keine Befugnisse zur Gefahrenabwehr.

Die sprachliche Ausgestaltung des Absatz 4 der Norm ist zu unbestimmt. **Es bedarf bezüglich des Wortlauts „datei- und informationssystemübergreifend“ zumindest einer klaren Beschränkung auf das Informationssystem des BKA**, wie er laut Begründung des Entwurfs angestrebt wird.[8] Absatz 4 zielt offensichtlich darauf ab, neue Erkenntnisse zu gewinnen, indem uneingeschränkt Beziehungen zwischen z. B. Personen und Sachen hergestellt werden. Durch die Formulierung „im Rahmen“ knüpft dieser Absatz zwar an die vorherigen Absätze an. Gleichzeitig spricht er aber im Plural davon, dass „alle eingehenden

[5] BVerfG NJW 2023, 1161.
[6] Siehe Seite 20 der BT-Drucks., Begründung zu § 16a.
[7] BVerfG NJW 2023, 1161 (1206), Rn. 105.
[8] Siehe Seite 20 der BT-Drucks., Begründung zu § 16a.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Erkenntnisse zu bekannten Sachverhalten zugeordnet und die Daten statistisch ausgewertet werden“. Wie oben dargelegt, sollen aber von vornherein alle Daten in einer Super-Datenbank gesammelt werden, **noch bevor eine Gefahrenlage besteht**. Dem Gesetzeswortlaut ist bereits zu entnehmen, dass unbedeutende Informationen und Erkenntnisse ausgeschlossen werden sollen. Dies unterstreicht im Umkehrschluss, dass wie oben dargelegt zunächst in einem großen Umfang Informationen von unbeteiligten Personen Gegenstand der Auswertung sein werden ohne zuvor die Speicherschwellen der §§ 18 und 19 BKAG geprüft zu haben, gegebenenfalls auch Massendaten (aus Telekommunikationsüberwachungen, Funkzellenabfragen u.a.). An besonderen Löschmechanismen bzw. kürzere Aussonderungsprüffristen fehlt es ebenfalls.

- **Zu § 34a BPolG-E**

Auch die Bundespolizei wäre nach dem Gesetzentwurf berechtigt, eine äußerst umfassende dauerhafte Datenbank anzulegen, unabhängig von nachfolgenden Analysen im konkreten Anwendungsfall. **Die Norm ist aus den oben dargestellten Gründen auch hier strikt abzulehnen.**

Die Formulierung „informationssystemübergreifend“ in Abs. 2 ist auch hier klarzustellen.

B. Entwurf eines Gesetzes zur Verbesserung der inneren Sicherheit und des Asylsystems

1. Zu Artikel 1 des Gesetzentwurfs (Änderung des Bundesverfassungsschutzgesetzes)

Mit der Änderung soll den Verfassungsschutzbehörden die Durchführung von Finanzermittlungen (§ 8a Abs. 1 Satz 1 Nr. 2 Bundesverfassungsschutzgesetz -BVerfSchG-) erleichtert werden.

Die verschiedenen besonderen Auskunftsverlangen des § 8a dürfen nach bisheriger Rechtslage im Rahmen der Erforschung von Bestrebungen nach § 3 Abs. 1 Nr. 1 BVerfSchG einschränkend nur dann erfolgen, wenn die Bestrebung einen Gewaltbezug hat, in dem sie z.B. durch verschiedene Aktionen die Bereitschaft zur Gewalt fördert. Bestrebungen nach

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

§ 3 Abs. 1 Nr. 1 sind solche, die sich gegen (u.a.) die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Staates richten.

Durch die Änderung wird laut Begründung auf das zusätzliche Merkmal des Gewaltbezugs bei sog. "legalistischen Bestrebungen mit erheblichem Aktionspotential oder erheblicher gesellschaftlicher Wirkungsbreite" verzichtet (S. 32 des Dokuments), um deren Finanzströme besser erfassen zu können. Unter Legalismus wird verstanden, dass eine Gruppierung von innen heraus an der Abschaffung der freiheitlichen demokratischen Grundordnung arbeitet, also z.B. ohne gewaltsamen Umsturz[9].

Die Möglichkeit, leichter Finanzermittlungen durchzuführen, wird diesseits als solches nicht kritisiert.

Es fällt allerdings auf, dass die konkrete Eingriffsschwelle bzw. die Beobachtungsbedürftigkeit (der Zeitpunkt, ab dem eine legalistische Bestrebung erhebliches Aktionspotential hat) ausschließlich und auch nur ansatzweise aus der Gesetzesbegründung hervorgeht. Seit dem Urteil des Bundesverfassungsgerichts (BVerfG) vom 26.04.2022 (1 BvR 1619/17) müssen auch im BVerfSchG abgestufte Eingriffsschwellen angepasst an die jeweilige Eingriffsintensität der Maßnahme geregelt werden.

In Bezug auf die sog. besonderen Auskunftsverlangen des § 8a BVerfSchG hat das BVerfG ganz aktuell bezüglich der Vorschriften in Hessen deutlich gemacht, dass es sich um Maßnahmen mit "erhöhtem Gewicht" handelt (Beschl. vom 17.09.2024, 1 BvR 2133/22, Rdnr. 159ff[10]). Es gelten daher erhöhte Anforderungen an die Beobachtungsbedürftigkeit einer Bestrebung oder Tätigkeit, sog. modifizierten Verhältnismäßigkeitsanforderungen, die sich im Gesetz wiederfinden müssen. Erforderlich ist eine verfassungsschutzspezifische Eingriffsschwelle (Rdnr. 170).

Besondere Auskunftsverlangen nach § 8a Abs. 1 Satz 1 dürfen eingeholt werden, soweit dies zur Sammlung und Auswertung von Informationen erforderlich ist und Tatsachen die Annahme rechtfertigen, dass schwerwiegende Gefahren für die in § 3 Abs. 1 genannten Schutzgüter vorliegen.

Das dürfte nach der Rechtsprechung des BVerfG nicht ausreichen. Das Gericht fordert z.B., dass hinreichende Anhaltspunkte im Einzelfall dafür vorliegen müssen, dass die ergriffene

[9] Vgl. bspw. https://www.verfassungsschutz.bayern.de/islamismus/definition/erscheinungsformen/legalistischer_islamismus/index.html zum islamistischen Legalismus.
[10] Dort entschieden für Auskunftsersuchen gegenüber Verkehrsunternehmen und Betreibern von Computerreservierungssystemen und Globalen Distributionssystemen für Flüge.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Maßnahme im Einzelfall zur Aufklärung geboten ist, insbesondere wenn sie sich gezielt gegen bestimmte Personen richtet (Rdnr. 172). Das kann bei personengebundenen Bankkonten in Bezug auf Finanzermittlungen durchaus der Fall sein. Außerdem fehlt es u.a. an einer hinreichenden Potentialität der Bestrebung (Rdnr. 177 ff.).

Bei der geplanten Änderung des § 8a BVerfSchG fällt erschwerend ins Gewicht, dass das Gesetz bislang noch keine Abstufung von Bestrebungen an sich vornimmt. Laut Begründung sollen Finanzermittlungen ja offenbar nicht bei jeglicher Art von legalistischer Bestrebung erlaubt sein. Die konkreten Abstufungen, die Eingriffsschwellen, müssen aber im Gesetz selbst geregelt sein. Ohne diese sehe ich – gerade auch im Licht der Entscheidung aus Karlsruhe aus der letzten Woche – keine verfassungskonforme Eingriffsbefugnis.

Die dringend notwendige Reform des Nachrichtendiensterecht, die neben vielen anderen Anliegen auch diese Punkte aus der verfassungsgerichtlichen Rechtsprechung umsetzen muss, lässt leider weiter auf sich warten.

2. Zu Artikel 2 Nr. 3 des Gesetzentwurfs (§ 15b AsylG-E)

- **Automatisierte Anwendung / KI:**

Nach § 15b AsylG-E soll das Bundesamt für Migration und Flüchtlinge (BAMF) die Befugnis erhalten, das im Ausländerzentralregister enthaltene biometrische Lichtbild des Ausländers mit öffentlich zugänglichen personenbezogenen Daten aus dem Internet mittels einer automatisierten Anwendung abzugleichen. § 15b AsylG-E soll dem Zweck der Identitätsfeststellung oder der Feststellung der Staatsangehörigkeit im Asylverfahren dienen.

Der Entwurf geht offenbar davon aus, dass die automatisierte Anwendung im Sinne des § 15b AsylG-E dem Begriff eines Hochrisiko-KI-Systems im Sinne der KI-VO unterfällt. Denn ausweislich der Begründung zum § 15b Abs. 2 AsylG-E soll diese Norm Vorgaben des Art. 14 der KI-VO sowie des Art. 22 DSGVO umsetzen. Der Entwurf nutzt die dem Gesetzgeber zur Verfügung stehende Möglichkeit, die Eingriffsintensität der automatisierten Datenanalyse zu reduzieren, jedoch nicht in vollem Umfang. Dies ist in zweierlei Hinsicht relevant.

Nach der Rechtsprechung des Bundesverfassungsgerichts kann der Gesetzgeber die Eingriffsintensität einer automatisierten Datenanalyse reduzieren, indem er etwa die Methode der Datenanalyse in ihren grundlegenden Zügen im Gesetz selbst regelt (vgl. BVerfGE 165, 363 Rn. 120 ff.). Sollte z.B. der Einsatz selbstlernender Systeme im Rahmen des Abgleichs nach § 15b AsylG-E nicht beabsichtigt sein, bietet es sich an, den Einsatz selbstlernender

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Systeme im Gesetz ausdrücklich auszuschließen (vgl. BVerfGE 165, 363 Rn. 121), um das Risiko einer verfassungsgerichtlichen Verwerfung zu minimieren.

Darüber hinaus müssen Vorschriften, die automatisierte Verarbeitungen personenbezogener Daten rechtfertigen, gemäß Art. 22 Abs. 2 Buchst. b) DSGVO „angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten“. Es wird empfohlen, durch weitere einschränkende Vorgaben im Gesetz z.B. zur Methode der Datenanalyse könnten die im Entwurf bereits vorgesehenen Vorkehrungen und Schutzmechanismen zu komplettieren und damit den Schutz der Grundrechte zu stärken.

§ 15b AsylG-E regelt den Einsatz biometrischer Fernidentifizierungssysteme im Sinne des Anhang III Nr. 1 Buchst. a) KI-VO. Biometrische Fernidentifizierungssysteme sind KI-Systeme, die dem Zweck dienen, natürliche Personen ohne ihre aktive Einbeziehung in der Regel aus der Ferne durch Abgleich der biometrischen Daten einer Person mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren, unabhängig davon, welche Technologie, Verfahren oder Arten biometrischer Daten dazu verwendet werden (EG 17 S. 1 KI-VO). Bei den in Anhang III Nr. 1 Buchst. a genannten Hochrisiko-KI-Systemen müssen die die Aufsichtsmaßnahmen gewährleistenden Vorkehrungen gemäß Art. 14 Abs. 5 KI-VO so gestaltet sein, dass der Betreiber keine Maßnahmen oder Entscheidungen allein aufgrund des vom System hervorgebrachten Identifizierungsergebnisses trifft, solange diese Identifizierung nicht von mindestens zwei natürlichen Personen, die die notwendige Kompetenz, Ausbildung und Befugnis besitzen, getrennt überprüft und bestätigt wurde.

In seiner Begründung fasst der Gesetzentwurf selbst die Vorgaben des Art. 14 der KI-VO dahingehend zusammen, dass der automatisierte Vorgang demnach vor jeglichen weiteren Maßnahmen oder Entscheidungen durch zwei Personen zu überprüfen und zu bestätigen ist (vgl. S. 27 des Entwurfs). Diese Vorgabe findet sich jedoch nicht im Wortlaut des § 15b AsylG-E wieder. In § 15b Abs. 2 S. 1 AsylG-E heißt es lediglich, dass die Treffer des Abgleichs „durch Inaugenscheinnahme zu überprüfen“ sind. Dem Gesetzgeber ist deshalb zu empfehlen, auch im Wortlaut der Norm die Vorgabe zu machen, dass die Überprüfung durch zwei Personen stattzufinden hat.

Ein weiterer Zweck der Erkenntnisse aus dem Abgleich des biometrischen Lichtbilds bei dem BAMF ist im § 15b AsylG-E nicht geregelt. Inwieweit das ein Mehr an innerer Sicherheit bieten soll, ist nicht ersichtlich. Sollen die gewonnenen Erkenntnisse aus der Gesichtserkennung beim BAMF für weitere Zwecke als die Identitätsfeststellung im Asylverfahren Verwendung finden, so ist das gesetzlich zu regeln. Daran fehlt es im Gesetzentwurf bislang.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Zur Geeignetheit der Maßnahme finden sich keine Ausführungen in der Gesetzesbegründung. Das wäre angesichts des Eingriffstiefe in das Recht auf informationelle Selbstbestimmung, als Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz (GG) in jedem Fall angezeigt. Dieses Grundrecht ist ein Menschen-Grundrecht, kein Deutschen-Grundrecht.

- **Im Einzelnen:**

a) Zu §15b Absatz 1 Satz 1 AsylG-E (Abgleich biometrisches Lichtbild, automatisierte Anwendung):

Der biometrische Abgleich mit öffentlich zugänglichen personenbezogenen Daten zum Zweck der Identitätsfeststellung begegnet aus datenschutzrechtlicher Sicht verschiedenen Bedenken.

Die Begrifflichkeit der öffentlich zugänglichen personenbezogenen Daten aus dem Internet sind allesamt unscharfe Tatbestandsmerkmale und ermöglichen erhebliche Eingriffe in die Rechte unbeteiligter Personen (durch den Abgleich wird es zu falschen „Treffern“ mit unbeteiligten Personen kommen). Zwar findet sich in § 15b Absatz 3 AsylG-E eine Löschregelung für erhobene Daten, sobald diese nicht mehr für die Feststellung der Identität oder Staatsangehörigkeit benötigt werden. Wenn sie nicht mehr benötigt werden, sind sie unverzüglich zu löschen. Das setzt jedoch voraus, dass der Zuständige die Entscheidung treffen muss, dass die Daten nicht mehr benötigt werden und unverzüglich heißt auch lediglich ohne schuldhaftes Zögern. Rechtsklare Löschfristen sind das nicht. Aus Gründen der Normenklarheit sollte bei den Tatbestandsmerkmalen mit Legaldefinitionen gearbeitet werden.

Die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person ist nach Art. 9 Abs. 1 DSGVO untersagt und nur unter den Voraussetzungen des Art. 9 Abs. 2 DSGVO ausnahmsweise zulässig.

Die Begründung (S. 27) führt hierzu aus, dass dies im Sinne des Art. 9 Abs. 2 lit g) DSGVO aus Gründen eines erheblichen öffentlichen Interesses erforderlich sei und in angemessenem Verhältnis zu dem verfolgten Ziel stehe, da bei fehlendem Pass oder Passersatz nur die hier geregelte Verarbeitung biometrischer Daten die Identitätsklärung ermöglicht, welche für Zwecke der Prüfung des Asylantrags und für die zügige Durchführung des Asylverfahrens notwendig sei. Zudem ist nach Art. 9 Abs. 2 lit g) DSGVO ist die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses auf der Grundlage von nationalem

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Recht nur zulässig, das in angemessenen Verhältnis zum verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht. Die Begründung bleibt nähere Ausführungen zu diesen Anforderungen bisher schuldig beziehungsweise lässt sogar einen Mangel in der Verhältnismäßigkeit befürchten, da in der Begründung lediglich ausgeführt wird, dass „bei fehlendem Pass oder Passersatz nur die hier geregelte Verarbeitung biometrischer Daten die Identitätsklärung ermöglicht“ (s. S. 23), ohne die Möglichkeit milderer Mittel (entgegen des Normwortlauts) überhaupt zu erwähnen.

Zudem soll laut der Gesetzesbegründung der Begriff der Identität sehr weit zu verstehen sein und auch das Geburtsland, das Land des gewöhnlichen Aufenthalts, der Familienstand, die Volks- und Religionszugehörigkeit sowie die Sprachkenntnisse des Ausländers umfassen. Vor dem Hintergrund der ebenfalls in der Begründung enthaltenen Feststellung, dass zur Identität auch Merkmale zählen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind und zur Ermittlung dieser Daten eine KI eingesetzt werden soll, sollte eine klare Begrenzung der zur Feststellung der Identität des Ausländers zu erhebenden Daten im Gesetzestext selbst erfolgen.

Darüber hinaus muss eine solche automatisierte Anwendung ggf. durch Trainingsdaten angelernt und durch Testdaten getestet werden. Aus dem Gesetzesentwurf geht hierzu nichts hervor. Sollte hier vorgesehen sein, die bereits im Ausländerzentralregister vorhandenen Lichtbilder zu verwenden, ggf. durch Echtdatenabzug und Synthetisierung, so sind hierfür eigene Rechtsgrundlagen erforderlich (Trainingsdaten, Testdaten). Zu dem Themenkomplex Lichtbildsuche im Ausländerzentralregister hat es in den Jahren 2022/2023 bereits eine Beratung meinerseits gegenüber dem Bundesministerium des Innern und für Heimat gegeben mit genau diesem Ergebnis, dass für eine etwaige Verwendung der Echtdaten (Lichtbilder) aus dem Ausländerzentralregister als synthetisierte Testdaten eigene Rechtsgrundlagen erforderlich sind[11].

b) Zu § 15b Absatz 2 Satz 1 AsylG-E (Inaugenscheinnahme):

Treffer des Abgleichs sind laut der Regelung durch Inaugenscheinnahme zu prüfen. Erst in der Gesetzesbegründung wird ausgeführt, dass der automatisierte Vorgang vor jeglichen weiteren Maßnahmen oder Entscheidungen durch zwei Personen zu überprüfen und zu bestätigen ist (Artikel 14 der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz, sog. KI-Verordnung, und Artikel 22 der Datenschutzgrund-Verordnung, DSGVO).

[11] Aktenzeichen BfDI: 16-206/001#1324

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Wesentliche Regelungen zur Ausgestaltungen der Verarbeitung personenbezogener Daten sollten aber im Regelungstext selbst erfolgen. Zur Vermeidung von Inkonsistenzen mit dem bereits bestehenden § 15a Asylgesetz sollte zudem geregelt werden, dass zumindest eine dieser Personen über die Befähigung zum Richteramt verfügen muss. Auch wenn die Aufgabe weitgehend automatisiert durchgeführt wird, sollte hier ausschließlich eine gesonderte Organisationseinheit für den Abgleich zuständig und befugt sein, bei Bedarf entsprechende Auswertungen vorzunehmen, und dann ausschließlich das Ergebnis für die Fallbearbeitung mitteilen. Eine solche organisatorische Trennung würde zum besonderen Schutz beitragen, dessen biometrische Daten bei der Identitätsfeststellung bedürfen. Und auch im Falle eines besonderen Schutzbedarfs der miterfassten Kontexte könnte die organisatorische Trennung zu den nach Art. 9 Abs. 2 lit g) DSGVO vorzusehenden Schutzmaßnahmen gehören. Insofern werden die Vorgaben der Art. 24, 25 und 32 der DSGVO noch nicht hinreichend umgesetzt.

c) Zu § 15b Absatz 4 S. 2 AsylG-E:

Nach Beendigung der Gesichtserkennung soll die Stelle unterrichtet werden, die "für den Datenschutz bei öffentlichen Stellen zuständig ist". Das ist bezüglich des für die Gesichtserkennung zuständigen BAMF nach Artikel 55 Abs. 1 DSGVO in Verbindung mit § 9 Bundesdatenschutzgesetz (BDSG) die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). Dies sollte ausdrücklich in den Gesetzestext geschrieben werden, wie es bereits in vielen anderen Gesetzen erfolgt ist, vgl. statt aller § 22 Absatz 1 Satz 4 Ausländerzentralregistergesetz. Darüber hinaus sollte zumindest in der Begründung klarstellend erläutert werden, welche Erwartungen des Gesetzgebers mit der Übermittlung an die BfDI gestellt werden, da sich hieraus erst die Grundlage für eine Berechnung des noch aufzunehmenden Personalbedarfs ergibt. Denkbar sind hier etwa eine vollständige Prüfung aller Fälle oder eine stichprobenhafte Prüfung von Einzelfällen.

d) Zu § 15b Absatz 1 Satz 1 AsylG-E: sowie zu § 15b Absatz 7 Satz 3 AsylG-E:

Die Nachvollziehbarkeit des verwendeten Verfahrens soll "soweit wie technisch möglich" sichergestellt werden. Diese Einschränkung ist nicht mit Art. 5 Absatz 1 und 2 DSGVO vereinbar.

3. Zur Systematik § 15b AsylG-E (Gesichtserkennung) und § 15a AsylG (Auslesung mobiler Datenträger)

Die Regelung des § 15b AsylG-E ist im systematischen Zusammenhang mit der bereits bestehenden Regelung des § 15a AsylG zu sehen, der die Auslesung mobiler Datenträger er-

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

möglicht. Beide Regelungen sehen vor, dass die Gesichtserkennung bzw. das Auslesen mobiler Datenträger nur erfolgen darf, wenn die Identitätsfeststellung nicht durch mildere Mittel erreicht werden kann. Das ist die Umsetzung des verfassungsrechtlichen Grundsatzes der Verhältnismäßigkeit staatlicher Maßnahmen. In Bezug auf die Auslesung mobiler Datenträger musste jüngst das Bundesverwaltungsgericht die Verwaltung zur Einhaltung dieses verfassungsrechtlichen Grundsatzes anhalten[12].

In welchem Verhältnis nunmehr die Gesichtserkennung und das Auslesen mobiler Datenträger zueinanderstehen sollen, ist im Gesetzestext nicht ausdrücklich geregelt. In der Gesetzesbegründung ist es sogar offen gelassen[13]. Aufgrund der Eingriffsintensität der Maßnahme sollte diese Entscheidung vom Parlament getroffen werden und im Gesetzestext erfolgen. Eine Regelung durch die Vollzugsbehörde reicht meiner Ansicht nach nicht aus (unabhängig von den Anwendungshinweisen, die die Verwaltung für den "Einzelfall" geben wird).

4. Zu Artikel 5 Nr. 2 b) des Gesetzentwurfs (§ 4 Absatz 6 WaffG-E)

In § 4 Abs. 6 WaffG-E wird die Befugnis der Waffenbehörde eingeführt, in öffentlich zugänglichen Quellen zu recherchieren. Diese Art von Befugnis findet sich aktuell auch in immer mehr Sicherheitsgesetzen. Die Formulierung ist datenschutzrechtlich problematisch. Es fehlt eine Legaldefinition der öffentlich zugänglichen Quelle. Es ist unklar, was unter öffentlich zugänglichen Quellen zu verstehen ist, die Gesetzesbegründung bleibt mit dem Hinweis „insbesondere aus dem Internet“ (S. 48) sehr vage.

[12] Bundesverwaltungsgericht, Urteil vom 16. Februar 2023, 1 C 19.21.
[13] „Das Auswerten der mobilen Datenträger nach § 15a AsylG kann im Einzelfall ein milderes Mittel darstellen. § 15b AsylG-E kann im Einzelfall auch ein milderes Mittel zu § 15a AsylG darstellen.“ (s. BT-Drs. 20/12805, S. 23, Begründung B., zu Artikel Artikel 2, zu Nr. 3)

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de