Stellungnahme des Paritätischen Gesamtverbandes zum Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung (KI-Migrationsverwaltungsgesetz - KIMVG) BT-Drucksache 21/8275

Der Paritätische Gesamtverband nimmt Stellung zum Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung (KI-Migrationsverwaltungsgesetz - KIMVG)“ anlässlich der Sachverständigenanhörung des Innenausschusses des Deutschen Bundestages am 23. November 2026.

Die Stellungnahme bewertet zunächst den Entwurf insgesamt, geht dann auf die drei Regelungsbereiche (Entwicklung von KI-Systemen, Verfahrensmonitoring, Internetabgleich) im Einzelnen und auf die Vorschläge des Bundesrates ein und schließt mit Empfehlungen und einer Schlussbemerkung.

I. Gesamtbewertung

Der Paritätische Gesamtverband teilt das Ziel, Asyl-, Aufenthalts- und Visumsverfahren zu beschleunigen und die Qualität von Entscheidungen zu sichern. Die Sicherung der Qualität von Entscheidungen und Verfahren sollte dabei jedoch nicht allein verbesserte und effizientere Verwaltungsverfahren im Blick haben, sondern insbesondere auf die Wahrung der Rechte von Antragstellenden und auf eine Verbesserung der Verfahrens- sowie Entscheidungsqualität aus Sicht der Antragstellenden abzielen. Das gilt vor allem dann, wenn mögliche Risiken und Grundrechtseinschränkungen mit dem Einsatz von künstlicher Intelligenz oder automatisierten Verfahren verbunden sind.

Der vorliegende Gesetzentwurf wird diesem Anspruch jedoch nicht gerecht. Er eröffnet weitreichende Möglichkeiten zur KI-gestützten Verarbeitung sensibler personenbezogener Daten einer besonders schutzbedürftigen Personengruppe, ohne den Schutz der betroffenen Menschen ausreichend sicherzustellen.

Konkret erlaubt der Entwurf den zuständigen Behörden der Migrationsverwaltung, personenbezogene Daten zur Entwicklung, das heißt zum Training, zur Überprüfung und zum Testen von KI-Systemen und anderen automatisierten Anwendungen zu

verarbeiten. Die konkreten Einsatzzwecke und -bedingungen sowie Anwendungsbereiche werden hingegen nicht verbindlich geregelt. Zudem fehlen hinreichend konkrete Vorgaben zur Transparenz, zur Wahrung der Betroffenenrechte und zu wirksamen Grundrechtsschutzgarantien. Die vorgesehenen Schutzvorkehrungen sind vielfach unverbindlich und überlassen es den Behörden, selbst zu bestimmen, was beispielsweise als „angemessen“ gilt.

Der Paritätische hat erhebliche Bedenken, dass der Entwurf in seiner vorliegenden Fassung mit den Vorgaben des Grundgesetzes (Art. 1 Abs. 1, Art. 2 Abs. 1, Art. 3 Abs. 1 GG) und der Grundrechtecharta der Europäischen Union (Art. 7, 8, 20, 21 GRCh) vereinbar ist. Zweifel bestehen zudem an der Vereinbarkeit mit der Verordnung (EU) 2024/1689 über künstliche Intelligenz (KI-VO), auf die sich die Gesetzesbegründung selektiv beruft.

Der Paritätische lehnt den Gesetzentwurf in seiner vorliegenden Fassung ab. Er unterstützt den gemeinsamen Appell „KI in der Migrationsverwaltung braucht klare Grenzen und unabhängige Kontrolle!“[1] mit den folgenden drei Kernforderungen:

- Wirksamen Datenschutz und Grundrechtsschutz im Gesetz definieren
- Verbindliche und unabhängige Evaluation der KI-Systeme verankern
- Nachvollziehbarkeit und Transparenz für Betroffene und Öffentlichkeit herstellen

II. Zu den Regelungen im Einzelnen

Der Gesetzentwurf umfasst im Wesentlichen drei Regelungsbereiche, die jeweils parallel im Asylgesetz und im Aufenthaltsgesetz verankert werden sollen:

- Verarbeitung personenbezogener Daten zur Entwicklung von KI-Systemen (§ 7 Abs. 2a AsylG-E, § 86 Abs. 2 AufenthG-E)
- Automatisiertes Verfahrensmonitoring in Asyl- und aufenthaltsrechtlichen Verfahren (§ 7a AsylG-E, § 90d AufenthG-E)
- Automatisierter Datenabgleich in einzelnen Verfahren (§ 7b AsylG-E, § 90e AufenthG-E)

Im Folgenden nimmt der Paritätische zu den einzelnen Regelungsbereichen und ihren Auswirkungen Stellung:

1. Verarbeitung personenbezogener Daten zur Entwicklung von KI-Systemen (§ 7 Abs. 2a AsylG-E, § 86 Abs. 2 AufenthG-E)

Der Entwurf erlaubt den zuständigen Behörden, personenbezogene Daten, die ursprünglich im Rahmen von Asyl- und Aufenthaltsverfahren erhoben wurden, auch

[1] https://www.der-paritaetische.de/alle-meldungen/ki-in-der-migrationsverwaltung-der-paritaetische-und-36-weitere-organisationen-fordern-mehr-schutz-von-betroffenen/

zur Entwicklung, zum Training, zur Validierung und zum Testen von KI-Systemen und anderen automatisierten Anwendungen zu nutzen (Satz 1).

Zweckänderung ohne ausreichende Begrenzung und Verhältnismäßigkeit

Damit wird eine Verarbeitung der Daten für einen neuen Zweck ermöglicht, der über die ursprüngliche Bearbeitung des jeweiligen Einzelfalls hinausgeht. Besonders kritisch ist, dass die Befugnis sehr weit gefasst ist. Sie legt weder fest, für welche Arten von KI-Systemen und automatisierten Anwendungen die Daten genutzt werden dürfen, noch begrenzt sie die möglichen Einsatzbereiche, Datenkategorien (z.B. Ausschluss biometrischer Daten) oder Verfahrensschritte. Als Voraussetzung genügt, dass die Entwicklung der Erfüllung behördlicher Aufgaben dient (Satz 2). Ob dieser Zweck im Verhältnis zur umfangreichen Verarbeitung besonders schützenswerter personenbezogener Daten steht, wird nicht erwogen.

Vorprägung der Entscheidung

Nach der Gesetzesbegründung sollen die Systeme anhand von Beispieldaten lernen, unter welchen Voraussetzungen über einen Asylantrag zu entscheiden ist, welche Angaben dafür relevant sind und wie Nachweise zu prüfen sind (S. 15). Das geht über eine rein technische Unterstützung hinaus und birgt die Gefahr, dass KI-Systeme die spätere Bewertung und Entscheidung inhaltlich mitprägen. Dies steht im Widerspruch zur Aussage der Gesetzesbegründung, die KI-Systeme sollten Entscheidungen nicht vorwegnehmen (S. 11). Aus Sicht des Verbandes ist daher nicht ausreichend klar geregelt, welche Rolle solche Systeme künftig in Asyl- und Aufenthaltsverfahren übernehmen dürfen und wo die Grenzen ihres Einsatzes liegen.

Unzureichender Schutz sensibler personenbezogener Daten

Die Gesetzesbegründung verweist auf die Anforderungen der KI-VO an Trainingsdaten und leitet daraus ab, es könne sich „auch eine Verpflichtung zur Nutzung von Echtdaten ergeben“ (S. 16). Für das Verfahrensmonitoring verweist sie hingegen auf Art. 6 Abs. 3 KI-VO (S. 17), also auf eine Ausnahme von der Hochrisiko-Einstufung. Dabei gelten KI-Systeme, die Behörden bei der Prüfung von Asyl-, Visums- und Aufenthaltsanträgen unterstützen, nach Anhang III Nr. 7 Buchstabe c KI-VO grundsätzlich als Hochrisiko-Systeme.

Auch die vorgesehenen Schutzvorkehrungen der verwendeten Daten reichen nicht aus. Zwar verpflichtet der Entwurf die Behörden zu technischen und organisatorischen Schutzmaßnahmen und dazu, diskriminierende Algorithmen zu verhindern (Satz 3). Gleichzeitig lässt er offen, welche konkreten Maßnahmen hierfür erforderlich sind, wer deren Einhaltung überprüft und wie sich Betroffene gegen diskriminierende Trainingsinhalte oder -effekte wehren können. Die Gesetzesbegründung hält es zudem ausdrücklich für möglich, auf eine Anonymisierung oder Pseudonymisierung zu verzichten, wenn dies die „Aussagekraft“ der Systeme beeinträchtigen würde (S. 16). Namen und Geburtsdaten gelten nach der Begründung gerade deshalb als „kontextrelevant“, weil sie Rückschlüsse auf soziale Herkunft und Religionszugehörigkeit geben können (S. 16). Daten aus Asyl- und

Aufenthaltsverfahren enthalten zudem häufig Angaben zur persönlichen Lebensgeschichte, zu möglichen Gewalterfahrungen, Gesundheit oder sexueller Orientierung. Auch der Ausschluss von genetischen oder biometrischen Daten wird nicht erwogen. Damit werden gerade besonders geschützte Merkmale zum Trainingsinhalt. Werden diese Daten unmittelbar zum Training von KI-Systemen verwendet, besteht das Risiko, dass sensible Merkmale und Verzerrungen in die Systeme einfließen und spätere Ergebnisse beeinflussen. Der Ausschluss von Sozialdaten findet sich nur in der Begründung (S. 15), nicht im Normtext.

Unklare Risiken beim Einsatz externer Dienstleister

Die Gesetzesbegründung geht davon aus, dass für die Entwicklung der Systeme externe Unternehmen hinzugezogen werden (S. 17). Für das Verfahrensmonitoring legt der Entwurf Mindestanforderungen an solche Dienstleister fest, etwa einen Sitz in der EU und das Verbot, die Daten für eigene Zwecke zu nutzen (§ 7a Abs. 6 AsylG-E, § 90d Abs. 6 AufenthG-E). Für das Training von KI-Systemen hingegen fehlen vergleichbare Vorgaben. Offen bleibt damit insbesondere, wie Zugriffe von Auftragnehmer*innen und Unterauftragnehmer*innen beim Training begrenzt und kontrolliert werden.

2. Automatisiertes Verfahrensmonitoring in Asyl- und aufenthaltsrechtlichen Verfahren (§ 7a AsylG-E, § 90d AufenthG-E)

In einem zweiten Regelungsbereich schafft der Gesetzentwurf eine ausdrückliche gesetzliche Grundlage dafür, dass die zuständigen Behörden abgeschlossene Asyl- und Aufenthaltsverfahren mithilfe automatisierter Verfahren analysieren können. Dabei sollen sie personenbezogene Daten nutzen, um den Ablauf der Verfahren und die bisherige Entscheidungspraxis bei Asylanträgen auszuwerten.

Mittelbare Wirkung auf Einzelverfahren

Das Monitoring soll „ausschließlich“ verallgemeinerungsfähigen Erkenntnissen dienen (Abs. 2 Satz 1). Laut Begründung sollen die Ergebnisse jedoch „in die zukünftige Prüfungsintensität der Einzelfallentscheidungen“ einfließen bzw. wird eingeräumt, dass das Verfahrensmonitoring mittelbar der Einzelfallentscheidung dient (S. 18). Das Verbot der Profilbildung und der Verweis auf Art. 4 Nr. 4 DSGVO (Abs. 2 Satz 3) ist zudem angreifbar: Auch wenn die Auswertung statistisch erfolgt, wird sie zum Profiling, sobald ihre Ergebnisse darüber mitentscheiden, wie intensiv eine bestimmte Person geprüft wird. Wer wegen Herkunft, Geschlecht oder familiärer Bindungen intensiver geprüft wird, wird faktisch nach einem Gruppenprofil behandelt. Das berührt die Pflicht zur individuellen Prüfung und den effektiven Rechtsschutz.

Verfassungsrechtliche Bedenken durch unbegrenzte Datenanalyse

Die Befugnisse in § 7a Abs. 2 Satz 2 AsylG-E und § 90d Abs. 2 Satz 2 AufenthG-E entsprechen nahezu wortgleich § 25a Abs. 2 HSOG, den das Bundesverfassungsgericht am 16. Februar 2023 (1 BvR 1547/19) beanstandet hat. Danach hat eine automatisierte Datenanalyse ein eigenes Eingriffsgewicht. Der Gesetzgeber muss Art und Umfang der Daten sowie die zulässigen Analysemethoden

selbst eng begrenzen. Laut Begründung ist es hingegen „nicht möglich, den Datenkranz [...] auf bestimmte Daten zu beschränken“ (S. 18).

Diskriminierungsrisiko und Verfestigung bisheriger Praxis

Laut Gesetzesbegründung können bestimmte Merkmale (z.B. Geschlecht) und Namen von Betroffenen als Indikator für die „Plausibilität ihrer Angaben“ dienen, weil sie Rückschlüsse auf den „soziokulturellen Kontext“ erlauben (S. 18). An anderer Stelle räumt sie ein, dass Vor- und Nachnamen Auskunft über regionale oder soziale Herkunft und Religionszugehörigkeit geben (S. 16). Damit knüpft das Monitoring mittelbar an ethnische Herkunft, Religion und Geschlecht an, also an Merkmale, die durch Art. 3 Abs. 3 GG und Art. 21 GRCh besonders geschützt sind (zugleich besondere Kategorien nach Art. 9 DSGVO). Benachteiligt werden können insbesondere Menschen, deren Namen für ihr Herkunftsland „untypisch“ erscheinen wie zum Beispiel Minderheiten, Verfolgte, Staatenlose, Binnenvertriebene und Personen mit Namensänderungen oder abweichender Transkription. Das steht im Widerspruch zum Gebot, diskriminierende Algorithmen weder herauszubilden noch zu verwenden (§ 7a Abs. 3 AsylG-E, § 90d Abs. 3 AufenthG-E). Eine Rechtfertigung der Ungleichbehandlung nennt der Entwurf nicht.

Das Verfahrensmonitoring soll Variablen bewerten, die „die Glaubhaftigkeit von Fluchtgründen“ beeinflussen (S. 18). Das lässt sich als Vorstufe einer Glaubhaftigkeitsprognose lesen. Korrelationen der Vergangenheit sind keine Kausalität. Es droht ein Rückkopplungskreislauf: Hohe Ablehnung führt zu intensiverer Prüfung, und die führt wieder zu mehr Ablehnungen.

Verzerrte Datengrundlage

Datengrundlage sind „abgeschlossene“ Verfahren, nicht rechtmäßig entschiedene: Gerichtlich aufgehobene Bescheide und politisch geprägte Ablehnungsmuster würden algorithmisch fortgeschrieben.

Biometrie und Sozialdaten

Das Verbot der Verarbeitung biometrischer Daten (Absatz 1 Satz 3) wird durch die Ausnahme bei „unverhältnismäßig hohem technischen Aufwand“ (Satz 4) im Ergebnis aufgehoben. Technischer Aufwand ist kein Rechtfertigungsgrund nach Art. 9 Abs. 2 DSGVO. Der Ausschluss von Sozialdaten (§ 78 Abs. 1 SGB X) ist nur in der Begründung enthalten (S. 26), die weder Behörden noch Gerichte bindet; er gehört in den Normtext.

3. Automatisierter Abgleich mit öffentlich zugänglichen Daten aus dem Internet (§ 7b AsylG-E, § 90e AufenthG-E)

Ebenso wird unter engen Voraussetzungen der automatisierte Abgleich öffentlich zugänglicher personenbezogener Internetdaten mit entscheidungserheblichen Antragsangaben ermöglicht, um diese zu verifizieren, wenn begründete Zweifel an der Richtigkeit dieser Angaben bestehen.

Niedrige und unbestimmte Eingriffsschwelle

Als “begründete Zweifel” gelten nach Begründung u.a. Dialektabweichungen, Widersprüche zum Reiseweg, im Verfahren geänderte Angaben sowie „Erkenntnisse aus der Beobachtung vergangener Verfahren“ (S. 20). Solche Abweichungen können viele Gründe haben, z.B. als Folge von Traumatisierung, Sprachmittlungsproblemen und Fluchtbedingungen sein, nicht von Unwahrheit.

Eingriff in Daten Betroffener und Dritter

Erfasst sind alle Daten, die „von jedermann eingesehen werden können“, vor allem aus sozialen Medien (S. 20). Sie enthalten häufig Angaben zu Religion, politischer Haltung oder sexueller Orientierung und betreffen zwangsläufig Dritte. Der Kernbereichsschutz greift nur bei „ausschließlich“ kernbereichsrelevanten Erkenntnissen (Abs. 3). Enthalten die Daten daneben auch andere Informationen, greift dieser Schutz möglicherweise nicht. Das ist sogar regelmäßig der Fall, wenn die Fluchtgründe in Verbindung mit dem Geschlecht, der sexuellen Identität oder der politischen Haltung stehen.

Internetdaten, die für den Echtzeit-Abgleich verwendet werden, können mitunter jahrzehntealt und falsch sein. Die Löschung oder Korrektur liegt in der Regel nicht allein in der Hand der Betroffenen. Dies kann zu Abschreckungseffekten mit Blick auf die freie Meinungsäußerung oder die Nutzung des Internets allgemein führen. Zudem kann die Verwaltungspraxis von politischen Gegner*innen ausgenutzt werden, indem gezielt Falschinformationen platziert werden.

Unzureichende Absicherung der menschlichen Prüfung und fehlende Transparenz

Die Ergebnisse des automatisierten Abgleichs müssen zwar „manuell bewertet und gegebenenfalls verifiziert“ werden (Abs. 1 Satz 3). Der Gesetzentwurf legt jedoch nicht fest, nach welchen Kriterien die Prüfung erfolgen soll, welche Qualifikation die prüfenden Personen benötigen und wie ihre Bewertung begründet werden muss. Damit besteht die Gefahr, dass die automatisiert erzeugten Ergebnisse ungeprüft übernommen werden.

Zudem ist nicht vorgesehen, dass die betroffenen Personen über den Datenabgleich und seine Ergebnisse informiert werden oder Gelegenheit erhalten, dazu Stellung zu nehmen. Auch die Dokumentationspflicht (Abs. 4) enthält keine Regelungen zur Information der Betroffenen oder zu ihrer Möglichkeit, die Ergebnisse einzusehen. Dadurch werden ihr Recht auf rechtliches Gehör und die Möglichkeit, gegen fehlerhafte oder diskriminierende Ergebnisse vorzugehen, beeinträchtigt (Art. 19 Abs. 4 GG, Art. 47 GRCh).

III. Zu den Vorschlägen des Bundesrates

Der Paritätische lehnt die Vorschläge des Bundesrates (Anlage 2) ab, weil sie den Schutz der Betroffenen weiter schwächen würden. Die Länderklausel (§ 7a Abs. 7 AsylG-E, § 86 Abs. 3, § 90d Abs. 7 AufenthG-E) würde nach Landesrecht zulässige

Verarbeitungen „unberührt“ lassen, obwohl sie, wie der Bundesrat selbst einräumt, an „weniger eng gefasste Voraussetzungen“ geknüpft sind. Damit wäre der Schutz der Betroffenen vom Bundesland abhängig. Die Erweiterung des Internetabgleichs auf Zwecke der Rückführung (§ 90e Abs. 1a AufenthG-E) würde Erkenntnisse zum „Sachnachweis“ gegenüber der Vertretung des Herkunftslandes machen und kann Betroffene und Angehörige gefährden. Die Zweckänderung für Strafverfolgung, Gefahrenabwehr und aufenthaltsrechtliche Maßnahmen (§ 90e Abs. 4 AufenthG-E) hebt schließlich die Zweckbindung auf, die den Abgleich auf die Prüfung des Einzelfalls beschränkt (S. 21).

IV. Empfehlungen

Sollte der vorliegende Gesetzesentwurf dennoch weiterverfolgt werden, sind zumindest folgende Anpassungen notwendig:

1. Rechtsrahmen und Folgenabschätzung

- Systeme, die Entscheidungen über Asyl, Visa und Aufenthalt vorbereiten oder beeinflussen, sind im Gesetz ausdrücklich als Hochrisiko-Systeme zu behandeln. Die daraus folgenden Pflichten, insbesondere die Grundrechte-Folgenabschätzung (Art. 27 KI-VO) und das Recht Betroffener auf Erläuterung (Art. 86 KI-VO) müssen im Gesetz ausdrücklich festgeschrieben werden und gelten ab Inkrafttreten des Gesetzes, unabhängig von der Selbsteinstufung der Behörde und vom Geltungsbeginn der Hochrisiko-Pflichten der KI-VO.
- Vor jedem Einsatz eines Systems ist eine Grundrechte-Folgenabschätzung durchzuführen, zu veröffentlichen und im Betrieb fortzuführen, einschließlich unabhängiger Bias-Prüfungen und Tests, deren Ergebnisse zu veröffentlichen sind. Zivilgesellschaft (einschließlich Betroffener) und Datenschutzaufsicht von Bund und Ländern sind zu beteiligen.
- Zwecke und Verfahrensschritte sind gesetzlich festzulegen; Ziel ist die Verbesserung der Verfahrens- und Entscheidungsqualität für Antragstellende.

2. Daten, Entwicklung und Training

- Personenbezogene Daten sind grundsätzlich zu anonymisieren; Ausnahmen sind eng zu fassen und zu begründen. Personenbezogene Daten dürfen nur nach erfolgter Einverständniseinholung verarbeitet werden.
- Systeme zur Bewertung der Glaubhaftigkeit oder zur Vorprägung der Asylentscheidung sowie automatisierte Bewertungen von Personen und Sachverhalten sind auszuschließen
- Ganze Asylakten und Datenbestände aus dem Ausländerzentralregister dürfen nicht pauschal und rückwirkend für Training und automatisierte Analysen genutzt werden.
- Es braucht verbindliche Vorgaben zu Datenminimierung, Löschfristen sowie zum Schutz von Sozialdaten im Gesetzestext.

- Für Auswahl und Kontrolle externer KI-Anbieter sind klare gesetzliche Anforderungen vorzusehen, die alle Phasen einschließlich des Trainings erfassen. Die Weitergabe und Nutzung personenbezogener Daten durch privatwirtschaftliche Dritte sind auszuschließen.

3. Verfahrensmonitoring

- Die Rückkopplung des Monitorings in die Prüfungsintensität einzelner Verfahren ist gesetzlich auszuschließen. Die Ergebnisse dürfen zudem nicht zur Ableitung von Risiko-, Plausibilitäts- oder Glaubhaftigkeitsindikatoren genutzt werden.
- Datengrundlage und Analysemethoden sind im Gesetz normenklar und abschließend zu regeln: nur rechtskräftig abgeschlossene Verfahren einschließlich gerichtlicher Entscheidungen, grundsätzlich anonymisiert; Namen, biometrische Daten (ohne Aufwandsausnahme) und Sozialdaten sind auszuschließen; Merkmale nach Art. 3 Abs. 3 GG dürfen keine Steuerungsgrößen sein.

4. Automatisierter Internetabgleich

- Dialekt, Reiseweg oder Änderungen im Vortrag dürfen allein keinen Internetabgleich auslösen.
- Der Abgleich ist auf Daten der antragstellenden Person und das öffentlich zugängliche, indexierte Internet zu beschränken; Höchstpersönliche Daten müssen auch bei gemischten Datensätzen geschützt bleiben.
- Selbstlernende KI ist in der Open Source Intelligence-Recherche (also die systematische Auswertung öffentlich zugänglicher Informationen, beispielsweise aus sozialen Netzwerken) auszuschließen. Die in der Begründung (S. 20 f.) vorgesehene Beschränkung auf einen methodisch einfachen Abgleich und der Ausschluss komplexer Analyseanwendungen sind in den Normtext aufzunehmen.

5. Transparenz, Rechtsschutz und Kontrolle

- Betroffene sind vor jedem Abgleich und jeder Verwertung verständlich zu informieren und anzuhören. Einsatz, Ergebnisse und Quellen sind zu dokumentieren und auf Anfrage herauszugeben. Der Zugang zu unabhängiger Asylverfahrensberatung ist sicherzustellen. Betroffene müssen die Möglichkeit haben, fehlerhafte Ergebnisse überprüfen zu lassen und sich im Rahmen eines wirksamen Rechtsschutzes dagegen zu wehren.
- Alle mit den Systemen befassten Beschäftigten sind vor dem Einsatz und danach regelmäßig verbindlich zu schulen, unter anderem zu Grenzen der Systeme, Automation Bias, Diskriminierung und Betroffenenrechten. Dies gilt insbesondere für Entwicklung und Training, für die der Entwurf bislang keine Schulungspflicht vorsieht. Die Beschäftigten müssen befugt sein, von Systemergebnissen abzuweichen.
- Die Evaluation ist gesetzlich zu verankern und von einer unabhängigen wissenschaftlichen Stelle spätestens zwei Jahre nach Inbetriebnahme und danach regelmäßig durchzuführen, an Grundrechtswirkungen auszurichten, zu

veröffentlichen und dem Bundestag vorzulegen. Bei erheblichen Grundrechtsrisiken ist der Einsatz auszusetzen.
- Alle Systeme sind öffentlich zu registrieren. Die Einhaltung ist durch unabhängige Stellen zu überprüfen.
- Zuständigkeiten und Folgen von Verstößen, einschließlich der Aussetzung des Systems, sind gesetzlich zu regeln.

V. Schlussbemerkung

Der Entwurf begründet den KI-Einsatz damit, dass keine Alternativen bestünden und eine Ausweitung der personellen Kapazitäten aufgrund der Haushaltslage und des Fachkräftemangels ausscheide (S. 12). Dabei handelt es sich um eine politische Prioritätensetzung, nicht um einen Sachzwang. Zudem setzt auch der KI-Einsatz qualifiziertes Personal voraus, insbesondere für eine wirksame menschliche Aufsicht.

Aus Sicht des Paritätischen sind verlässliche Beschleunigung und Entscheidungsqualität vor allem eine Frage ausreichender personeller Ausstattung, qualifizierter Entscheidungspraxis, einheitlicher Qualitätsstandards und unabhängiger Verfahrensberatung. Technische Unterstützung kann dies ergänzen, aber nicht ersetzen. Wenn sie eingesetzt wird, muss sie verhältnismäßig sein und braucht klare gesetzliche Grenzen, insbesondere um die Grundrechte der betroffenen Menschen zu schützen.

Daten sind kein Abbild der Wirklichkeit, sondern stets Produkt von Kategorien, Suchlogiken, Rechtsregeln und menschlichen Entscheidungen. Die Komplexität von Migrations- und Fluchtbiografien bilden sie nur verkürzt ab. Entscheidend ist daher nicht, ob die Systeme funktionieren, sondern wie: mit welchen Daten, unter wessen Kontrolle und mit welchen Rechten für Betroffene. Wo über Schutz und Aufenthalt entschieden wird, braucht es die oben geforderten gesetzlichen Grenzen und wirksame Kontrollen. Der Entwurf sieht diese nicht vor und ist deshalb grundlegend zu überarbeiten.

Berlin, 20. November 2026

Katja Kipping

Geschäftsführerin

Kontakt:
Susann Thiel
Referentin Flüchtlingshilfe/-politik
flucht@paritaet.org
030 24636-456

PARITÄT

Dr. Nannette Swed
Referentin Digitale Innovation
digikom@paritaet.org
030 24636-462