

Zum Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung (KIMVG-E)

KI-Training und -Nutzung in der Migrationsverwaltung Risiken und rechtliche Anforderungen

I. Unzureichender Grundrechtsschutz durch den KIMVG-E

Migrationsbehörden stehen vor erheblichen strukturellen Herausforderungen: komplexer Rechtsrahmen, hoher Verwaltungsaufwand, knappe personelle Ressourcen. Eine Modernisierung der Verfahren ist notwendig. KI kann dabei in bestimmten Bereichen, etwa bei rein unterstützenden, nicht-eingriffsintensiven Verwaltungsaufgaben, durchaus einen Mehrwert bieten. Entscheidend ist jedoch, unter welchen rechtlichen Voraussetzungen und mit welchen Schutzvorkehrungen ein solcher Einsatz erfolgt. Der vorliegende Entwurf zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung verfehlt diesen tatsächlichen Bedarf und ermöglicht stattdessen **tiefgreifende Eingriffe in die Grundrechte der Betroffenen** (Art. 1 Abs. 1, 2 Abs. 1, 3 Abs. 1 GG, Art. 7, 8, 20 f. EU-GR-Charta), die in dieser Form nicht gerechtfertigt sind. Automatisierte Analysetools und KI-Systeme sind diskriminierungs- und fehleranfällig, können rechtsstaatswidrig eingesetzt werden und bedrohen so die Rechte von Migrant*innen.

Der Gesetzentwurf sieht vor, dass für **Training und Einsatz** dieser Systeme große Mengen **hochsensibler Daten** verarbeitet werden dürfen – etwa zu Verfolgungsgeschichte, sexueller Orientierung und geschlechtlicher Identität, Herkunft, Religion, Behinderungen oder biometrischen Daten. Die Datenbanken der Migrationsbehörden enthalten dabei **ungeprüfte und ungefilterte Datensätze**, z.B. nach Auswertung von Mobiltelefonen. Werden solche unübersehbaren Datenmengen zum Training von KI-Systemen eingesetzt, ist **intransparent**, wie sich die Algorithmen entwickeln. **Qualität und Ausgewogenheit** der Daten der Migrationsbehörden ist nicht sichergestellt. Lernen KI-Systeme mit diesen Daten weiter, entstehen **fehlerhafte, diskriminierende Algorithmen**.

Hinzu kommt: Wie die KI-Analysetools zu ihren Ergebnissen kommen, ist nicht nachvollziehbar (**Blackbox**). Diese Ergebnisse werden aber zur Grundlage für staatliche Entscheidungen im Aufenthalts- und Asylrecht. Sachbearbeitende können **Fehler und Diskriminierung** nicht sicher erkennen und ausschließen. Es ist auch zu befürchten, dass Sachbearbeitende fehlerhaften und diskriminierenden Analyseergebnissen ohne ausreichende Überprüfung vertrauen („**automation bias**“). Statt vermeintlicher Effizienzgewinne drohen pauschale, falsche, diskriminierende Ergebnisse. Gleichzeitig können auch Betroffene nicht erkennen und nachweisen, ob die Entscheidung der Migrationsbehörde aufgrund einer fehlerhaften Datenanalyse ergangen ist. Wirksamer Rechtsschutz ist so kaum möglich.

Für den Einsatz von KI bei den Migrationsbehörden braucht es daher **klare, strenge gesetzliche Grenzen**, zum Schutz sowohl der Personen, deren Daten für das Training herangezogen werden, als auch derjenigen, deren Fälle mit den trainierten KI-Systemen bearbeitet werden. Automatisierte Bewertungen und Prüfungen von Personen und Sachverhalten mit KI müssen dabei gesetzlich ausgeschlossen werden.

Zum Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung (KIMVG-E)

II. Einschätzung zum KIMVG-E im Einzelnen

Der vorliegende KIMVG-E wird den dargestellten Risiken und rechtlichen Anforderungen **in keiner Form gerecht**. Der Entwurf ermöglicht den Migrationsbehörden die Verarbeitung personenbezogener Daten zum **Entwickeln und Trainieren von KI-Systemen**, „**Automatisiertes Verfahrensmonitoring**“ durch **Datenanalysen mittels KI** sowie **automatisierte OSINT-Abgleiche**. Diese Maßnahmen stellen **schwerwiegende Grundrechtseingriffe** dar. Der Entwurf ist zu unbestimmt geregelt und ermöglicht die automatisierten Maßnahmen unter zu geringen Voraussetzungen. Er enthält nur völlig unzureichende Schutzvorkehrungen. Hervorzuheben sind insbesondere folgende Gesichtspunkte:

1. Unklare und unzureichende Regelungen zu KI-Training und -Einsatz

Da KI-Training und KI-Einsatz Grundrechtseingriffe darstellen, muss das Gesetz **präzise regeln und begrenzen**, welche Tools unter welchen Voraussetzungen trainiert werden dürfen, was diese können und wie diese eingesetzt werden dürfen. Es muss klar erkennbar sein, welche Tools und Funktionen unzulässig sind. Behörden und Sachbearbeitende müssen sich für zulässigen KI-Einsatz am Gesetz orientieren können. Besonders strenger Vorgaben bedarf es, wenn KI bei der Bearbeitung von Einzelfällen eingesetzt wird, also bei der Prüfung von Anträgen und zur Vorbereitung von Entscheidungen über einzelne Sachverhalte. KI-Analysen im Einzelfall, also die Verarbeitung personenbezogener Daten mit KI, stellen **gravierende eigenständige Grundrechtseingriffe** dar. Deswegen muss der KI-Einsatz in diesen Fällen **besonders detailliert** geregelt und begrenzt werden. **Diesen Anforderungen genügt der vorliegende Entwurf in keiner Weise**. Dieser ist so unbestimmt, dass sich **zulässige Fälle des KI-Einsatzes dem Gesetz kaum entnehmen** lassen.

Der Entwurf enthält zunächst **keinerlei Regelung und Grenzen für die KI-Nutzung bei der Einzelfallbearbeitung**. Es ist nicht klar, **ob und wie** die „verallgemeinerungsfähigen Erkenntnisse“, die durch die Datenanalyse bzw. das Verfahrensmonitoring gewonnen werden (§§ 7a Abs. 2 AsylG-E, 90d Abs. 2 Aufenthaltsg-E) **in die Bearbeitung konkreter Anträge** und in die Vorbereitung und Findung konkreter Entscheidungen **einfließen**. Es bedarf einer **klaren gesetzlichen Regelung und Begrenzung**, die strenge Voraussetzungen und Grenzen für die Datenanalysen und den Einsatz der KI festsetzt. Dazu sind die Maßstäbe des **Bundesverfassungsgerichts** aus seinem **Datenanalyseurteil** zu polizeilichen Datenanalysen (BVerfGE 165, 363) heranzuziehen. Dieses entschied, dass die Anforderungen an die Rechtmäßigkeit von Datenanalysen von deren Eingriffsintensität abhängen. Eingriffserhöhend wirkt sich insbesondere aus, wenn Art und Umfang der einbezogenen Daten und die Analysemethoden nicht streng im Gesetz beschränkt sind. Auch die Nutzung selbstlernender Systeme und komplexer Algorithmen erhöht das Eingriffsgewicht. Auf Basis dieser Grundsätze ist für die im Entwurf ermöglichten KI-Analysen mit sämtlichen auch sensibelsten Daten der Migrationsbehörden **eine hohe Eingriffsschwelle** zu fordern. Für die Polizei

Zum Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung (KIMVG-E)

fordert das Bundesverfassungsgericht in solchen Fällen eine „konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut“. Datenanalysen ohne eigene Eingriffsschwelle sind nur zulässig, „wenn die zugelassenen Analyse- und Auswertungsmöglichkeiten durch Regelungen insbesondere zur **Begrenzung von Art und Umfang der Daten und zur Beschränkung der Datenverarbeitungsmethoden** normenklar und hinreichend **bestimmt in der Sache so eng begrenzt** sind, dass das Eingriffsgewicht der Maßnahmen erheblich gemindert ist“ (BVerfGE 165, 363, Leitsatz 4, Rn. 110). Dies ist schon aufgrund der Offenheit der Ermächtigung zum KI-Einsatz im KIMVG-E ausgeschlossen. Dennoch sieht der Entwurf vorliegend **keine Eingriffsschwelle und keine konkreten Voraussetzungen** für den KI-Einsatz im Einzelfall vor. Die Norm ermächtigt daher zu unverhältnismäßigen Grundrechtseingriffen.

Allein, dass die Datenanalyse nur zum „Verfahrensmonitoring“ (§ 7a Abs. 1 Satz 1 AsylG-E, § 90d Abs. 1 Satz 1 Aufenthaltsg-E) erfolgen soll, schließt die Nutzung von KI zur Einzelfallbearbeitung nicht aus. Der Begriff des „Verfahrensmonitoring“ ist irreführend und entspricht nicht den in der Entwurfsbegründung beschriebenen Anwendungsbeispielen. Die genannten Beispiele (Abgleich von Namen und Herkunftsregion, Verifizierung von Hochschulabschlüssen, Unterstützung der Sachbearbeitung, Anpassung der Prüfungsintensität in Einzelverfahren) stellen **kein abstraktes Verfahrensmonitoring**, sondern gerade **Datenanalysen im Einzelfall** dar.

Es fehlt zudem eine **ausreichend bestimmte Regelung, die bestimmt, welche KI-Systeme** trainiert und eingesetzt werden dürfen. Es sind diverse unterschiedliche Programme und Anwendungen denkbar. Je nach Ausgestaltung des KI-Systems sind unterschiedliche Grundrechtseingriffe zu befürchten und andere Verfahrensvorkehrungen notwendig. Zwei Szenarien sind dabei zu unterscheiden:

- **Eine Art „Wissensdatenbank“ oder „Glossar“:** durch KI-Analysen erstellt, deren Inhalte Sachbearbeitende zur Kontrolle von Daten heranziehen können, z.B. der Echtheit eines Studienabschlusses. Möglich ist ein statisches „Nachschlagewerk“, das händisch durchsucht wird. Technisch möglich und naheliegender wäre aber, dass Sachbearbeitende Daten aus ihrem konkreten Einzelverfahren in das Analysetool eingeben können und dann Ergebnisse zu ihrem Fall erhalten. Letzteres wäre eine individualisierte Datenanalyse im Einzelfall. Unklar ist außerdem, ob Sachbearbeitende auch auf die Daten und Fälle zugreifen können, auf die die KI ihre Ergebnisse stützt. Sucht ein*e Sachbearbeiter*in z.B. nach einer konkreten Hochschule und erfährt durch die KI, dass der Abschluss wahrscheinlich gefälscht ist, ist unklar, ob sie dann auf andere Fälle zugreifen kann, in denen ein Abschluss dieser Hochschule gefälscht war oder ob nur das Ergebnis „hohes Risiko einer Fälschung“ zugänglich ist. Kann sie auf frühere Akten und Fälle zugreifen, ermöglicht die Analyse weitreichende Zugriffe auf sensible Daten anderer Fälle (Zweckänderung). Besteht kein Zugriff auf die Daten, die das Analyseergebnis begründen, bleibt dies für Sachbearbeitende eine Blackbox und nicht nachvollziehbar. Das

Zum Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung (KIMVG-E)

schränkt auch die Möglichkeit wirksamen Rechtsschutzes ein, da auch Gerichte nicht erkennen können, wie und warum ein KI-Analysetool zu seinen Ergebnissen kommt.

- **Direkte Einbindung in die Fallbearbeitung:** Der Entwurf ermöglicht auch, dass die Ergebnisse der Datenanalyse direkt im Rahmen der Bearbeitung von Einzelfällen eingebunden sind, indem das Programm z.B. auf Basis dieser Ergebnisse Auffälligkeiten erkennt oder Hinweise abgibt. Die KI-Programme könnten so direkt mit Computerprogrammen zur Antragsbearbeitung oder Aktenführung verbunden werden. Ähnlich wie bei Steuerprüfungsprogrammen könnte allein bei Eingabe von Daten in Textfeldern schon automatisiert eine Analyse stattfinden, die dann mögliche Falschangaben erkennt und anzeigt (z.B. mit Warnhinweisen oder Fehlermeldungen). Ebenso könnte das Programm automatisiert aufgrund bestimmter Daten eine Prüfungsintensität empfehlen. Dieser Form der Analyse kommt ein sehr hohes Eingriffsgewicht zu, weil sie mit hoher Wahrscheinlichkeit Sachbearbeitende in ihrer Entscheidung beeinflusst. Für solche Datenanalysen muss der Gesetzgeber strenge Voraussetzungen vorsehen (s. oben).

Der Entwurf **lässt** daher **zentrale Fragen des Grundrechts- und Datenschutzes unbeantwortet** und leitet die Behörden nicht ausreichend zu einem grundrechtskonformen KI-Betrieb an.

2. Automatisierte Datenabgleiche mit Internet unverhältnismäßig

Auch die ermöglichten automatisierten Datenabgleiche mit dem Internet stellen unverhältnismäßige Grundrechtseingriffe dar. Die Behörden können unbegrenzt öffentliche Daten einbeziehen, die sie und die Betroffenen selbst nicht überblicken. Ebenso können Daten einfließen, die ohne oder gegen den Willen der Betroffenen im Netz stehen. Laut Gesetzesbegründung sollen auch Daten umfasst sein, die nur entgeltlich oder nach Genehmigung oder Registrierung nutzbar sind. Über soziale Medien und andere Inhalte sind weitreichende Erkenntnisgewinne möglich. Die **Automatisierung** von solchen OSINT-Techniken vertieft den Grundrechtseingriff, da diese beschleunigt und ohne menschliches Betreiben möglich werden. Auch für den Datenabgleich ist nicht ausreichend bestimmt festgelegt, welche automatisierten Anwendungen zum Einsatz kommen dürfen und was diese können.

Die vorgesehenen Voraussetzungen sind für Datenabgleiche mittels automatisierter Anwendung zu gering, da auch für diese bereits „begründete Zweifel“ unbegrenzte Recherchen und Abgleiche zulassen. Es drohen damit Verletzungen der Art. 6, 9 ff., 14 DSGVO, indem Betroffene durch weitreichende automatisierte KI-basierte Abgleiche im Internet zum bloßen Objekt der Datenverarbeitung werden und Kontrolle über ihre personenbezogenen Daten verlieren (hierzu BAG, Urteil vom 5. Juni 2026 – 8 AZR 117/24, Rn. 53, 57). Es ist außerdem zu befürchten, dass sich die „begründeten Zweifel“, also die Anlässe für die OSINT-Recherchen, wiederum aus KI-

Zum Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung (KIMVG-E)

Analyseergebnissen ableiten. Die in der Entwurfsbegründung genannten Beispiele der „widersprüchlichen Sprache, Dialekte oder Reisewege“ bergen erhebliche Diskriminierungsrisiken.

3. Unzureichender Datenschutz

Der Entwurf gewährleistet keinen ausreichenden Datenschutz: In das KI-Training und die Analysen fließen fast alle von der jeweiligen Behörde erhobenen Daten ein (§ 7 Abs. 2a Satz 1, § 7a Abs. 1 Satz 1 AsylG-E, § 86 Abs. 1 Satz 1, § 86 Abs. 1 Satz 1 und Abs. 2 Satz 1, 90d Abs. 1 Satz 1 AufenthG-E). Beim BAMF sind das neben den im Rahmen des individuellen Asylverfahrens erhobenen, teils hochsensiblen Daten auch sämtliche im Ausländerzentralregister gespeicherten Daten, da diese vom BAMF als Registerbehörde erhoben werden. Die Einschränkung in § 7 Abs. 2a Satz 1 AsylG-E, dass nur zum Zwecke der Ausführung des Asylgesetzes erhobene Daten zum KI-Training verwendet werden dürfen, könnte zwar die Daten im Ausländerzentralregister vom KI-Training ausschließen, da diese zum Zweck der Ausführung des Ausländerzentralregisters erhoben wurden. Allerdings findet sich diese Einschränkung in § 7a Abs. 1 Satz 1 nicht mehr, so dass spätestens für das Verfahrensmonitoring sämtliche AZR-Daten einfließen können. Auch andere Behörden, etwa Polizeibehörden, können die von ihnen im Ausländerzentralregister zur Erfüllung ihrer Aufgaben abgerufenen Daten für das KI-Training und die Datenanalyse nutzen.

Diese teils hochsensiblen und zu anderen Zwecken von den jeweiligen Behörden erhobenen Daten dürfen nur in engen Grenzen **zweckändernd** zur KI-Entwicklung und für Datenanalysen zum Verfahrensmonitoring genutzt werden. Auch in die **OSINT-Recherchen** können **sensibelste Daten** einfließen bzw. durch diese gewonnen werden. Das Gesetz muss diskriminierungssensible Daten aus KI-Training und Analyse ausschließen. Zudem besteht das Risiko, dass Daten, auch von unbeteiligten Dritten, selbst nach Löschung dauerhaft in der KI verbleiben und aus dieser sogar wieder extrahiert werden können. Diesen Risiken begegnet der Entwurf nicht.

4. Hochrisiko-KI-Systeme ohne die gebotenen Sicherungen

Der Entwurf ermöglicht mit den Befugnissen zum Verfahrensmonitoring und zu Datenabgleichen mit dem Internet den Einsatz von Hochrisiko-KI-Systemen, ohne die nach der KI-Verordnung erforderlichen Sicherungen zu gewährleisten. Die KI-Verordnung geht bei solchen Systemen von erheblichen grundrechtlichen Risiken aus, da sie Personen betreffen, die sich häufig in einer besonders prekären Lage befinden und vom Ergebnis behördlicher Maßnahmen abhängig sind. Daher unterliegt der Einsatz einem strengen Pflichtenregime. Dem trägt der Entwurf keine Rechnung: Er enthält weder Vorgaben zur Durchführung einer Grundrechte-Folgenabschätzung noch zur wirksamen Protokollierung des Einsatzes, zu einer qualifizierten menschlichen Aufsicht oder zur Information der Betroffenen.

Zum Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung (KIMVG-E)

5. Kein tatsächlicher Schutz vor Fehlern und Diskriminierung durch KI

Der Entwurf enthält keine Schutzvorkehrungen gegen Fehler und Diskriminierungen und schützt nicht vor automation biases: Der Gesetzgeber muss **konkrete Maßnahmen** vorschreiben, wie die Verwaltung Fehler und Diskriminierungen erkennen und beheben kann. Sonst drohen massenhaft falsche und diskriminierende Behördenentscheidungen durch diskriminierende Algorithmen. Im Entwurf fehlen Verpflichtungen zur Kontrolle der KI-Ergebnisse und zu verpflichtenden Tests und Vorgaben an die KI-Trainingsdaten. Bloß abstrakte Programmsätze wie in §§ 7a Abs. 3, AsylG-E, 90d Abs. 3, 90c Abs. 2 AufenthG-E genügen nicht.

Diskriminierungsrisiken drohen auch dadurch, dass die Programme bei längerem Betrieb auch auf Basis ihrer eigenen früheren Entscheidungen weiterlernen. Wie gravierend das sein kann, zeigt die **niederländische Kindergeld-Affäre**: Ein KI-Modell nutzte dort unter anderem die Nationalität von Antragsteller*innen als Analyse-Kriterium und leitete daraus diskriminierende Risikobewertungen ab. Die diskriminierenden Algorithmen verfestigten sich, weil das Programm auch auf Basis der mit ihm früher verarbeiteten Fälle weiterlernte. Nicht-niederländische Staatsangehörigkeiten wurden mit einem höheren Betrugsrisiko verbunden. Die nachfolgende menschliche Kontrolle konnte diese Risiken nicht auffangen, da die Sachbearbeitenden nicht nachvollziehen konnten, warum das System einen Fall als besonders risikobehaftet einstufte. Die Folge waren massenhafte fehlerhafte Verwaltungsentscheidungen mit gravierenden Folgen für das Leben tausender Betroffener: hohe unberechtigte Rückzahlungsforderungen, falsche Verdächtigung wegen Betruges und Mittelerschleichung, Einleitung von Strafverfahren. Gerade im Migrationsrecht ist die Gefahr solcher Entwicklungen gravierend, da den Entscheidungen diskriminierungssensible Daten zugrunde liegen und die Behördenentscheidungen existenzielle Folgen für die Betroffenen mit sich bringen.

6. Intransparenz und unzureichender Rechtsschutz

KI-Training und -nutzung erfolgen ohne Kenntnis der Betroffenen. Der Entwurf sieht weder Informationspflichten für die Betroffenen noch regelmäßige externe Kontrollen vor. Auch regelt das Gesetz keine Pflichten zur umfassenden Protokollierung und Dokumentation der Maßnahmen, sondern schreibt nur abstrakt „erforderliche technische und organisatorische Vorkehrungen“ vor (§§ 7 Abs. 2a Satz 3, 7a Abs. 5 Satz 2 AsylG-E, §§ 86 Abs. 2 Satz 3, 90d Abs. 5 Satz 2 AufenthG-E). Damit Betroffene Entscheidungen nachvollziehen und mögliche Fehler und Diskriminierungen erkennen können, bedarf es einer Pflicht zur Information, wie bei Entscheidungen in ihrem Fall KI zum Einsatz gekommen ist. Ebenso müssen Betroffene detailliert und verständlich informiert werden, wenn ihre Daten in ein KI-Training einbezogen werden. Für die automatisierten Datenabgleiche mit dem Internet bestehen Informationspflichten bereits aus Art. 14 DSGVO. Derartige Pflichten sind jedoch zum Schutz der Betroffenen auch bei KI-Training und Einsatz erforderlich. Die Möglichkeit eines Auskunftsverlangens der Betroffenen nach Art. 15 DSGVO genügt nicht.

Zum Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung (KIMVG-E)

7. Unzureichende Sicherung digitaler Souveränität

Die Vorgaben zur digitalen Souveränität (§§ 7a Abs. 6 AsylG-E, 90d Abs. 6 Aufenthaltsg-E) **genügen nicht**. Aufgrund der hohen Bedeutung für die Grundrechte ist zu fordern, dass der Gesetzgeber Anforderungen an die Anbieter*innen und vor allem ihre angebotenen Analyseprogramme im Gesetz zumindest in Grundzügen vorgibt. Die genutzten Tools müssen transparent sein. Dazu erforderlich ist, dass der Quellcode vor Inbetriebnahme und vor Updates zur umfassenden Prüfung zur Verfügung steht. Nur so kann eine verfassungs- und europarechtskonforme Datenanalysepraxis sichergestellt werden. Zudem muss ausgeschlossen sein, dass Analysetools außereuropäischer Anbieter*innen zum Einsatz kommen, damit nationales und europäisches Recht sicher durchgesetzt werden kann. Als Analysetools kommen in diesem Falle insbesondere öffentliche Softwareprogramme (beispielsweise nach Entwicklung in einem europäischen Verbund) in Betracht.