GESELLSCHAFT FÜR FREIHEITSRECHTE
FREIHEITSRECHTE.ORG

13. November 2026

Stellungnahme

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

BT-Drucksache 21/8275

von Franziska Görlitz, Juristin und Verfahrenskoordinatorin bei der Gesellschaft für Freiheitsrechte e.V.

Die Gesellschaft für Freiheitsrechte setzt sich mit juristischen Mitteln für die Grund- und Menschenrechte ein. Sie hat die Verfassungsbeschwerden initiiert und koordiniert, die zum Datenanalyseurteil des Bundesverfassungsgerichts führten. Sie führt auch Verfahren gegen verfassungswidrige Gesetze und Maßnahmen im Migrationsrecht. Sie hat beispielsweise erfolgreich gegen die anlasslose Auswertung von Mobiltelefonen durch das BAMF geklagt und klagt gegen die Erweiterung des Ausländerzentralregisters.

Der vorliegende Entwurf schafft Befugnisse zum Training von IT-Systemen, zur Nutzung von automatisierten Datenanalysen zum „Verfahrensmonitoring" und zu automatisierten Datenabgleichen mit dem Internet. Dabei dürfen auch Systeme künstlicher Intelligenz (KI) trainiert und eingesetzt werden. Diese Befugnisse werden für alle Behörden geschaffen, die das Asyl- oder Aufenthaltsgesetz anwenden. Ziel ist es, die Effizienz der Arbeit der Migrationsbehörden zu verbessern.

I. Zusammenfassung

Der vorliegende KIMVG-E wird den Risiken und rechtlichen Anforderungen für KI-Einsatz in der Migrationsverwaltung **in keiner Form gerecht**. Er ermöglicht den Migrationsbehörden weitgehend unbegrenzt die Verarbeitung personenbezogener Daten zum Entwickeln und Trainieren von KI-Systemen und zu „automatisiertem Verfahrensmonitoring" durch Datenanalysen mittels KI. Ebenfalls enthalten ist eine Befugnis für automatisierte OSINT-Abgleiche**.** Diese Maßnahmen stellen **schwerwiegende Grundrechtseingriffe** dar. Die geregelten Befugnisse sind **zu unbestimmt** und ermöglichen die automatisierten Maßnahmen **unter zu geringen Voraussetzungen**. Mangels ausreichender Informationspflichten drohen **intransparente Nutzung und Training von KI ohne Gewährleistung effektiven Rechtsschutzes.** Zudem enthält der Entwurf **nur völlig unzureichende Vorkehrungen zum Schutz vor Diskriminierung und Fehlern,** zur Sicherung der **Nachvollziehbarkeit** der Ergebnisse sowie der **digitalen Souveränität**.

II. Einschätzung zum KIMVG-E im Einzelnen

Migrationsbehörden stehen vor erheblichen strukturellen Herausforderungen: komplexer Rechtsrahmen, hoher Verwaltungsaufwand, knappe personelle Ressourcen. Eine **Modernisierung** der Verfahren ist **auch im Sinne der betroffenen Menschen notwendig**. Künstliche Intelligenz 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, 21 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. Gespeichert sind etwa Daten zu Verfolgungsgeschichte, sexueller Orientierung und geschlechtlicher Identität, Herkunft, Religion, Behinderungen und in großem Ausmaß biometrische Daten. Die Datenbanken der Migrationsbehörden enthalten dabei auch **ungeprüfte und ungefilterte Datensätze,** z.B. nach Auswertung von Mobiltelefonen. Werden solche unüberschaubaren Datenmengen zum Training von KI-Systemen eingesetzt, ist **intransparent,** wie sich die Algorithmen entwickeln. **Qualität** und **Ausgewogenheit** der Daten der Migrationsbehörden sind **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 so **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 und 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 und strenge gesetzliche Grenzen**. Zu schützen sind dabei sowohl die Personen, deren Daten für das Training herangezogen werden, als auch die Personen, deren Verfahren mit den trainierten KI-Systemen bearbeitet werden. Automatisierte Bewertungen und Prüfungen von Personen und Sachverhalten mit KI müssen dabei gesetzlich ausgeschlossen werden.

Der Entwurf bedarf vor diesem Hintergrund einer **grundlegenden Überarbeitung.** Die Rechtsgrundlagen für KI-Training und Datenanalysen sind verfassungs- und europarechtswidrig (dazu **1.**). Gleiches gilt auch für die Rechtsgrundlage zum automatisierten Datenabgleich mit dem Internet (dazu **2.**). Transparenz und effektiver Rechtsschutz sind nicht sichergestellt (dazu **3.**). Der Entwurf enthält keine ausreichenden Vorkehrungen zum Schutz vor Diskriminierung und Fehlern (dazu **4.**). Auch die Vorkehrungen zur digitalen Souveränität sind ungenügend (dazu **5.**).

1. Regelungen zu KI-Training und -Einsatz verfassungs- und europarechtswidrig

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

a) Fehlen einer Rechtsgrundlage für KI-Nutzung im Einzelfall

Der Entwurf enthält zunächst **keinerlei Regelung und Grenzen für die KI-Nutzung bei der Einzelfallbearbeitung**. Er enthält nur Rechtsgrundlagen für das Training und die Entwicklung von IT-Produkten (§§ 7 Abs. 2a AsylG-E, 86 Abs. 2 AufenthaltsG-E) und für Datenanalysen zum „Verfahrensmonitoring", mit denen „verallgemeinerungsfähige Erkenntnisse" gewonnen werden sollen (§§ 7a Abs. 1, 2 AsylG-E, 90d Abs. 1, 2 AufenthaltsG-E).

Nicht geregelt sind jedoch die **Nutzung** der IT-Systeme oder der „verallgemeinerungsfähigen Erkenntnisse" **durch Sachbearbeiter*innen** in ausländer- oder asylrechtlichen Einzelverfahren. 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 „Verfahrensmonitorings" ist irreführend und entspricht nicht den in der Entwurfsbegründung beschriebenen Anwendungsbeispielen. Die in der Entwurfsbegründung genannten Beispiele (Abgleich von Namen und Herkunftsregion[1], Verifizierung von

[1] Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung, BT-Drs. 21/8275, S. 16, 18, 24, 26.

Hochschulabschlüssen[2], Unterstützung der Sachbearbeitung und Erhöhung der Entscheidungsqualität,[3] Anpassung der Prüfungsintensität in Einzelverfahren[4]) stellen **kein abstraktes Verfahrensmonitoring,** sondern **Datenanalysen im Einzelfall** dar.

Gerade diese **Nutzung der KI-Systeme und ihrer Analyseergebnisse im Einzelfall** greift jedoch in die Grundrechte ein und bedarf deswegen einer **eigenständigen Rechtsgrundlage.** Auch das Bundesverfassungsgericht sieht komplexe Datenanalysen und -auswertungen als eigenständige Grundrechteingriffe an.[5] Zudem ist die KI-Nutzung im Einzelfall auch eine eigenständige Datenverarbeitung, für die es gemäß Art. 6, 9 DSGVO einer konkreten Rechtsgrundlage bedarf. Es muss daher gesetzlich geregelt werden**, ob und wie** die „verallgemeinerungsfähigen Erkenntnisse", die durch die Datenanalyse bzw. das Verfahrensmonitoring gewonnen werden **in die Bearbeitung konkreter Anträge** und in die Vorbereitung und Findung konkreter Entscheidungen **einfließen**. Ebenso muss geregelt werden, wie die entwickelten KI-Systeme in der Einzelfallbearbeitung zum Einsatz kommen dürfen.
Das Erfordernis einer solchen Rechtsgrundlage wird mit dem Entwurf verkannt. In der Begründung des Referentenentwurfes, der zur Stellungnahme an die Verbände übersandt wurde, wurde vielmehr ausdrücklich angenommen, „der bloße Einsatz von KI-Systemen als solcher" bedürfe „keiner eigenständigen gesetzlichen Ermächtigung"[6].
Diese Einschätzung steht im Widerspruch dazu, dass gerade die KI-Nutzung im Einzelfall Gefahren für die Antragssteller*innen und Betroffenen mit sich bringt. Es bedarf daher **zwingend der Schaffung einer Rechtsgrundlage für die KI-Nutzung im Einzelfall.**

b) Unverhältnismäßigkeit der Befugnisse

Die Ermächtigungen zum KI-Training und zur Datenanalyse sind unverhältnismäßig und verfassungswidrig. Sie ermöglichen schwerwiegende Grundrechtseingriffe unter zu geringen Voraussetzungen.
Die zweckändernde Weiterverarbeitung von Daten ist ein rechtfertigungsbedürftiger Eingriff in **Grundrechte der Betroffenen** aus Art. 1 Abs. 1, 2 Abs. 1, 3 Abs. 1 GG bzw. Art. 7, 8, 20, 21 EU-GR-Charta. Es bedarf daher einer **klaren gesetzlichen Regelung und Begrenzung,** die strenge Voraussetzungen und Grenzen für die Datenanalysen und den Einsatz der KI festsetzt. Dazu können die Maßstäbe des **Bundesverfassungsgerichts** aus seinem **Datenanalyseurteil** zu polizeilichen Datenanalysen herangezogen werden[7].

---

[2] Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung, BT-Drs. 21/8275, S. 26.
[3] Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung, BT-Drs. 21/8275, S. 15, 18, 24, 26.
[4] Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung, BT-Drs. 21/8275, S. 18, 26.
[5] [5] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 54, 66 ff., 71 ff.
[6] Referentenentwurf vom 25. Juni 2026, S. 10.
[7] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, BVerfGE 165, 363.

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.[8] Auch die **Nutzung selbstlernender Systeme** und komplexer Algorithmen erhöht das Eingriffsgewicht.[9]
Diese Maßstäbe hat das Bundesverfassungsgericht zwar außerhalb des Geltungsbereiches der DSGVO und damit in einem lediglich durch die JI-Richtlinie mindestharmonisierten Bereich entschieden. Die Kriterien zur Bestimmung des Eingriffsgewichts können jedoch dem Grunde nach auch auf eine Anwendung der europäischen Grundrechte im Geltungsbereich der DSGVO übertragen werden.
Unter Anwendung dieser Grundsätze ist das **Eingriffsgewicht** der zulässigen Datenanalysen als **schwerwiegend** anzusehen. Es fließen sämtliche gespeicherte Daten, auch individuelle Asyl- und Ausländerakten, in KI-Training und Analyse ein. Die Analysemethode ist gerade mit Blick auf die offene Entwicklung und Nutzung selbstlernender und sonstiger KI-Systeme extrem weitgehend. Es ist bereits **nicht erforderlich**, pauschal alle gespeicherten Daten so weiten Analysemethoden zu unterziehen. Jedenfalls ist das Eingriffsgewicht der ermöglichten KI-Entwicklung und -Analyse gerade aufgrund der Masse der einbezogenen sensiblen Daten extrem hoch.

Auf Basis dieser Grundsätze ist für die im Entwurf ermöglichten KI-Analysen **eine hohe Eingriffsschwelle** zu fordern. Für die Polizei fordert das Bundesverfassungsgericht in solchen Fällen eine „konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut".[10]
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".[11] 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.

Darüber hinaus verletzen die Befugnisse die **Grundsätze der Zweckbindung und Zweckänderung**.
In das KI-Training und die Datenanalysen fließen mit den geplanten Befugnissen 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, Abs. 2 Satz 1, 90d Abs. 1 Satz 1 AufenthaltsG-E). Beim BAMF sind das neben den im Rahmen des

[8] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Leitsatz 3, Rn. 78 ff., 90 ff.
[9] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100 f.
[10] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 104 ff.
[11] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Leitsatz 4, Rn. 110.

individuellen Asylverfahrens erhobenen, teils hochsensiblen Daten auch sämtliche im **Ausländerzentralregister** gespeicherte 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 AsylG-E 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. Auch in ausländerrechtlichen Verfahren werden eine Vielzahl sensibler Daten gespeichert, beispielsweise Gesundheitsdaten im Rahmen der Prüfung von Duldungen oder Daten aus der Auswertung von Mobiltelefonen.

Diese vielfach 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. Mit dem KIMVG-E wären die Zweckänderungen zum KI-Training und zur Datenanalyse aber **faktisch in allen Fällen generell zulässig**. Eine Differenzierung der Daten erfolgt weder nach Sensibilität und Schutzwürdigkeit noch nach ursprünglichem Erhebungszweck. Die **pauschale Nutzung** sämtlicher dieser Daten für jegliches Training und jede Nutzung von KI verletzt die Grundsätze der Zweckbindung und ist **unverhältnismäßig.**

c) Unzureichende Bestimmtheit und Normenklarheit

Es fehlt zudem eine **ausreichend bestimmte Regelung,** die **festlegt, 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. Dies verdeutlichen folgende (nicht abschließende) Beispielskonstellationen:

(1) **Erstellung einer KI-„Wissensdatenbank":**

Vorstellbar ist, dass durch KI-Analysen ein Glossar oder eine Wissensdatenbank erstellt werden, deren Inhalte Sachbearbeitende zur Kontrolle von Daten heranziehen können. So können Sachbearbeitende z.B. die Echtheit eines Studienabschlusses mithilfe der Datenbank überprüfen oder Informationen aus einer „Herkunftsländerdatenbank" erhalten[12]. Möglich ist dabei ein statisches „Nachschlagewerk", das händisch durchsucht wird. Technisch möglich und naheliegender wäre aber, dass Sachbearbeitende Daten aus ihrem konkreten

[12] Zum KI-basierten Umgang mit Herkunftsländerinformationen: https://www.ecoi.net/de/coi-ressourcen/acute-artificial-intelligence-for-country-of-origin-information-understanding-technical-and-ethical-implications/.

Einzelverfahren in das Analysetool[13] eingeben und dann automatisiert Ergebnisse zu ihrem Fall erhalten. Letzteres wäre eine **rechtfertigungsbedürftige 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*er auf frühere Akten und Fälle zugreifen, ermöglicht die Analyse weitreichende Zugriffe auf sensible Daten anderer Personen. Besteht kein Zugriff auf die Daten, die das Analyseergebnis begründen, bleibt dies für Sachbearbeitende eine Blackbox und nicht nachvollziehbar. Das **schränkt** gleichsam die **Möglichkeit wirksamen Rechtsschutzes ein**, da auch Gerichte nicht erkennen können, wie und warum ein KI-Analysetool zu seinen Ergebnissen kommt.

(2) **Direkte Einbindung in die Fallbearbeitung:** Der Entwurf ermöglicht ebenfalls, die Ergebnisse der Datenanalyse **unmittelbar in die Bearbeitung von Einzelfällen einzubeziehen**, indem Programme zur Antragsbearbeitung beispielsweise automatisiert Auffälligkeiten erkennen oder Hinweise geben. 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.[14] 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. soeben b)).

Nochmals deutlich abweichende Fragen und Herausforderungen ergeben sich bei Systemen wie KI-basierter Sprach- oder Dialekterkennung oder bei KI-Systemen, die bei der Antragsstellung unterstützen[15].

Der Gesetzgeber muss in einer Rechtsgrundlage bestimmt und normenklar festlegen, welche IT-Systeme für welchen Zweck trainiert und eingesetzt werden können. Grundrechtlichen Folgefragen und Risiken der zulässigen Anwendungen muss der Gesetzgeber dabei durch klare Vorkehrungen begegnen. **Nach diesen Grenzen müssen sich** die **Behörden** für ihre Softwareanschaffungen **richten.** Eine Befugnis, die pauschal sämtliches KI-Training und sämtliche Datenanalysen zum

[13] Zu einem KI-basierten Recherchetool für den Einsatz bei Verwaltungsgerichte: https://leadershipgarage.de/2024/06/26/ki-und-justiz-ein-einblick-in-das-projekt-emil-am-verwaltungsgericht-hannover/.
[14] Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung, BT-Drs. 21/8275, S. 18, 26.
[15] Beispielsweise: https://www.egovernment.de/ki-einsatz-in-auslaenderbehoerden-a-45da474039f13b7d79e54bb59e082f49/.

Verfahrensmonitoring legalisiert, ist zu unbestimmt und stellt keine verfassungskonforme Rechtsgrundlage dar. Dies kann auch nicht damit gerechtfertigt werden, dass Behörden ggf. schon bestimmte Systeme nutzen oder angeschafft haben. Für derart grundrechtssensible Fragen muss der parlamentarische Gesetzgeber klare Grenzen vorgeben, nach denen sich die Exekutive ausrichtet. Die aktuellen Befugnisse machen eine Vielzahl verschiedener Tools möglich. Es droht daher der **Einsatz verschiedenster technischer Systeme**, die **unterschiedlich sicher** und **nicht miteinander operabel** sind. Eine derart offene Befugnis ist daher auch **nicht zweckmäßig.**

d) Unvereinbarkeit mit Vorgaben der DSGVO und der KI-Verordnung

Die vorgesehenen Rechtsgrundlagen genügen auch nicht den Anforderungen an eine gesetzliche Konkretisierung der zweckändernden Weiterverarbeitung gemäß Art. 6 Abs. 2, 4 DSGVO und verletzen daher auch den europarechtlich verankerten Grundsatz der **Zweckbindung** (Art. 5 Abs. 1 lit. b DSGVO). Die Befugnisse erlauben die Zweckänderung und Nutzung sämtlicher bei den Migrationsbehörden gespeicherter Daten ohne ausreichende Voraussetzungen und verstoßen deshalb gegen den **Grundsatz der Datenminimierung** (Art. 5 Abs. 1 lit. c DSGVO). Davon umfasst sind auch besondere **Kategorien personenbezogener Daten**, die gemäß Art. 9 Abs. 1 DSVGO nur unter besonderen Voraussetzungen verarbeitet werden dürfen. Ein ausreichender Schutz für diese wird nicht vorgesehen.
Zudem verletzen die Ermächtigungen zu KI-Training und -Datenanalyse mit sämtlichen gespeicherten Daten auch den **Grundsatz der Datenrichtigkeit** (Art 5 Abs. 1 lit. d DSGVO), da auch fehlerhafte Daten in das Training und die (selbstlernenden und damit fortlaufend trainierenden) Analysen einfließen werden. Die neuen Befugnisse sollen gerade zum Einsatz kommen, um Daten auf ihre Richtigkeit und Schlüssigkeit zu überprüfen.[16] Gleichzeitig werden die Systeme **genau auf Basis dieser falschen Daten** trainiert und lernen fortlaufend weiter. Der Entwurf sieht auch nicht vor, dass fehlerhafte Inhalte in den Datenbanken und auch in den KI-Systemen **korrigiert** werden müssen, z.B. durch Einbeziehung von aufhebenden oder abändernden Gerichtsentscheidungen.
Die Befugnisse sind aus diesem Grunde **unverhältnismäßig, zu unbestimmt** und deshalb auch **europarechtswidrig**.

Der Entwurf ermöglicht zudem 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. Gemäß Anhang III Nr. 7 KI-VO gelten bestimmte KI-Systeme im Bereich Migration, Asyl und Grenzkontrolle als Hochrisiko-KI-Systeme. Darunter fallen insbesondere KI-Systeme, soweit sie die Prüfung eines Asyl-, Visum- oder Aufenthaltsantrags im Einzelfall unterstützen (Anhang III Nr. 7 lit. c KI-VO). Die KI-Verordnung geht bei solchen Systemen von erheblichen grundrechtlichen Risiken aus, da sie Personen betreffen, die sich

[16] so ausdrücklich §§ 7b Abs. 1 Satz 1 AsylG-E, 90e Abs. 1 Satz 1 AufenthaltsG-E in der Befugnis für den Datenabgleich mit dem Internet; die Datenanalysen zum Verfahrensmonitoring sollen beispielsweise helfen, die Plausibilität von Angaben zu überprüfen und Missbrauch, z.B. durch vorgetäuschte Universitätsabschlüsse zu erkennen, S. 26 f. der Entwurfsbegründung der BT-Drs. 21/875.

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 (hierzu sogleich **3.**).

2. Automatisierte Datenabgleiche mit Internet unverhältnismäßig

Auch die ermöglichten **automatisierten Datenabgleiche mit dem Internet** (§§ 7b AsylG-E, 90e AufenthaltsG-E) 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. 5, 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.[17] Es ist außerdem zu befürchten, dass sich die „begründeten Zweifel", also die Anlässe für die OSINT-Recherchen, wiederum aus KI-Analyseergebnissen ableiten. Die in der Entwurfsbegründung genannten Beispiele der „widersprüchlichen Sprache, Dialekte oder Reisewege" bergen erhebliche **Diskriminierungsrisiken.** Zudem drohen **fehlerhafte Abgleiche**, z.B. durch Verwechslungen mit gleichnamigen Personen.

Auch in die **OSINT-Recherchen** können **sensibelste Daten** einfließen bzw. durch diese gewonnen werden. Über das Internet kann ein Abgleich auch mit falschen oder veralteten Daten erfolgen.

3. Intransparenz und unzureichender Rechtsschutz

KI-Training und -nutzung erfolgen **ohne Kenntnis der Betroffenen**. Der Entwurf sieht dennoch **weder Informationspflichten noch regelmäßige externe Kontrollen** vor. Auch regelt das Gesetz keine Pflichten zur umfassenden **Protokollierung und Dokumentation** der Maßnahmen, sondern

[17] hierzu BAG, Urteil vom 5. Juni 2026 – 8 AZR 117/24, Rn. 53, 57.

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 AufenthaltsG-E).
Damit Betroffene Entscheidungen nachvollziehen und mögliche Fehler und Diskriminierungen erkennen können, müssen sie tatsächlich Einblick bekommen, welche ihrer Daten mit welchem Programm wie analysiert wurden und wie dies in die Entscheidung ihres Falles einfließen wird. Deshalb bedarf es einer **Pflicht zur umfassenden Information**, ob und wie bei der Einzelfallbearbeitung zum Einsatz gekommen ist. Diese Informationen müssen vor der Sachentscheidung erteilt werden. Betroffene müssen sodann die Möglichkeit bekommen, **Stellung zu nehmen** und auf eventuelle Fehler hinzuweisen, **bevor über Sachverhalte entschieden wird**. 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 beschränkte Informationspflichten bereits aus Art. 14 DSGVO. Zur Sicherung effektiven Rechtsschutzes bedarf es jedoch umfassender Informationspflichten zu allen neuen Maßnahmen des KIMVG-E. Die Möglichkeit eines Auskunftsverlangens der Betroffenen nach Art. 15 DSVGO genügt nicht.

Ohne stärkere Transparenzanforderungen besteht das Risiko, dass **von Betroffenen und Behörden unbemerkt** fehlerhafte Entscheidungen ergehen und **auch Gerichte diese Entscheidungen nicht wirksam überprüfen** können. Solche Entscheidungen können, gerade im Asylverfahren, existenzielle und nicht wiedergutzumachende Folgen für Betroffene haben.

4. Kein tatsächlicher Schutz vor Fehlern und Diskriminierung durch KI

Der Entwurf enthält **keine Schutzvorkehrungen** gegen Fehler und Diskriminierungen und schützt nicht vor **automation biases.** Für polizeiliche Datenanalysen hat das Bundesverfassungsgericht entschieden, dass beim Einsatz selbstlernender Systeme oder anderen komplexen Systemen „besondere verfahrensrechtliche Vorkehrungen"[18] notwendig sind. Diese müssen trotz eingeschränkter Nachvollziehbarkeit der Datenanalysen ein hinreichendes Schutzniveau sichern und die Herausbildung und Verwendung diskriminierender Algorithmen verhindern.
Der Gesetzgeber muss also **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 und Verbote** wie in §§ 7 Abs. 2a Satz 3, 7a Abs. 3 AsylG-E, §§ 86 Abs. 2 Satz 3, 90d Abs. 3, 90e Abs. 2 AufenthaltsG-E **genügen nicht.**
Ebenso wenig stellt der Entwurf tatsächlich mit konkreten Vorgaben und Sicherungen sicher, dass KI-Ergebnisse **wirksam menschlich kontrolliert** und so auch **automation biases korrigiert** werden. Gerade bei komplexen KI-Systemen ist für Behördenmitarbeiter*innen nicht nachvollziehbar, wie das

[18] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100 f.

System zu seinen Ergebnissen kommt. Wirksame Vorkehrungen, die eine solche **Nachvollziehbarkeit sichern,** fehlen im Entwurf.

Vorkehrungen zum Schutz vor Diskriminierung, Fehlern oder nicht nachvollziehbaren Ergebnissen sind auch nicht durch Vorgaben der KI-Verordnung sichergestellt. Zwar wären die staatlichen Behörden durch Entwicklung und Betrieb eigener IT-Systeme nicht nur als Betreiber*innen, sondern auch als Anbieter*innen (Art. 16 KI-VO) grundsätzlich an die Vorgaben gebunden. Auch bei Ankauf fremder IT-Produkte ist eine Stellung als „Quasi-Anbieter*innen“[19] wahrscheinlich. Allerdings finden die Bestimmungen zu Hochrisiko-KI-Systemen nach nochmaliger Verschiebung nun **erst frühestens ab dem 2. Dezember 2027** Anwendung.[20] Für Hochrisiko-KI-Systeme, die sich **bereits im Betrieb befinden**, gelten die Anforderungen zudem gemäß Art. 111 Abs. 2 KI-Verordnung **nur bei wesentlichen Änderungen.** Es ist daher zu befürchten, dass zahlreiche Migrationsbehörden im Jahr 2027 nach Inkrafttreten der geplanten Regelungen noch IT-Systeme erwerben und einführen, die dann den Vorgaben der KI-Verordnung nicht unterfallen. Sowohl **vor Inkrafttreten** der Bestimmungen als auch für **zuvor in Betrieb genommene Systeme** bestehen **Schutzlücken**. Diese muss der Gesetzgeber **mit eigenen Vorgaben** schließen.

Besondere 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**[21]: 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.[22] 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 tausendfach fehlerhafte Verwaltungsentscheidungen mit gravierenden Folgen für das Leben tausender Betroffener: hohe unberechtigte Rückzahlungsforderungen, falsche Verdächtigung wegen Betruges, Einleitung von Strafverfahren und Verlust des Sorgerechts für die eigenen Kinder. 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.

---

[19] Zu Art. 25 Abs. 1 lit. a, b DSGVO *Martini/Botta*, DÖV 2025, 1033 (1037 f.) für polizeiliche Datenanalysen.
[20] Rat der Europäischen Union, Pressemitteilung vom 29. Juni 2026, Künstliche Intelligenz: Rat gibt endgültig grünes Licht für Vereinfachung und Straffung der Vorschriften, abrufbar unter: https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/.
[21] Dazu: https://www.amnesty.org/en/latest/news/2021/10/xenophobic-machines-dutch-child-benefit-scandal/ sowie https://netzpolitik.org/2021/kindergeldaffaere-niederlande-zahlen-millionenstrafe-wegen-datendiskriminierung/ und https://www.dw.com/de/niederlande-kindergeldskandal-st%C3%BCrzt-familien-in-not/video-56552757.
[22] Dazu: https://www.amnesty.org/en/latest/news/2021/10/xenophobic-machines-dutch-child-benefit-scandal/.

Der Fall zeigt außerdem deutlich, dass ohne ausreichende Transparenz fehlerhafte und diskriminierende Entscheidungen nur mit größtem Aufwand erkannt und korrigiert werden können und auch eine nachträgliche Aufklärung[23] nur sehr erschwert möglich ist.

5. Unzureichende Sicherung digitaler Souveränität

Die Vorgaben zur digitalen Souveränität (§§ 7a Abs. 6 AsylG-E, 90d Abs. 6 AufenthaltsG-E) **genügen nicht**. Zur Sicherstellung der digitalen Souveränität und des Datenschutzes bedarf es vielmehr Vorgaben **an den Code bzw. an das IT-System selbst**, nicht nur an die Anbieter*innen. Aufgrund der hohen Bedeutung für die Grundrechte ist zu fordern, dass der Gesetzgeber Anforderungen an die **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.

Der vorgesehene Ausschluss, dass Analysetools außereuropäischer Anbieter*innen zum Einsatz kommen, ist grundsätzlich zu begrüßen. Er trägt dazu bei, dass 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. Eine Vorgabe an einen Unternehmenssitz oder einen Ort der Datenverarbeitung allein stellt eine rechtskonforme Datenverarbeitung jedoch keinesfalls ausreichend sicher.

[23] Noch 2026 wurden in zur Kindergeld-Affaire Dokumente gefunden, die dem zuständigen Untersuchungsausschuss bereits 2020 hätten übergeben werden müssen, https://www.trouw.nl/politiek/belastingdienst-ontdekt-miljoenen-documenten-over-toeslagenaffaire~be256232/?referrer=https%3A%2F%2Fwww.google.com%2F.