Deutsches Institut
für Menschenrechte

Das europäische Einreise-/ Ausreisesystem

Die neue EU-Datenbank und ihre grund- und menschenrechtlichen Herausforderungen

Information

Seit zwanzig Jahren treibt die Europäische Union (EU) die Digitalisierung ihrer Außengrenzen voran. In diesem Rahmen soll 2025 das Einreise-/ Ausreisesystem (EES) in Betrieb genommen werden: ein neues europäisches IT-Großsystem, das die Daten aller Drittstaatsangehörigen speichert, die für einen Kurzaufenthalt in die EU einreisen. Das System soll zu automatisierten und damit effizienteren Grenzkontrollen führen. Jedoch bestehen Bedenken, dass grundlegende Rechte wie der Datenschutz, das Recht auf Privatsphäre und das Recht auf einen wirksamen Rechtsbehelf verletzt werden können.[1]

Im Jahr 2005 veröffentlichte die Europäische Kommission erstmals Vorschläge zum Ausbau der Digitalisierung der europäischen Außengrenzen und zu einer verstärkten Vernetzung europäischer Datenbanken.[2] Als Reaktion auf Forderungen des Europäischen Rates, die neue Europäische Sicherheitsstrategie im „Kampf gegen den Terrorismus“ voranzutreiben, zielte die Kommission damit insbesondere auf die Überwachung der Grenzübertritte von Drittstaatsangehörigen ab. Die europäischen Informationssysteme (IT-Systeme) im Bereich Sicherheit, Grenzmanagement und Migrationskontrolle nahmen dabei von Beginn an eine zentrale Rolle ein. Einerseits sollten die beiden bereits bestehenden Datenbanken, das Schengen-Informationssystem (seit 1995) und Eurodac (seit 2003), in ihren Funktionen und Zugriffsberechtigungen erweitert werden. Andererseits sollten neue IT-Großsysteme bestehende Lücken in der Datenverwaltung im Bereich Grenzschutz und Sicherheit schließen. Zentrales Anliegen war es, die Systeme und Datenbanken interoperabel zu machen. Damit wird die Fähigkeit von IT-Systemen bezeichnet, Daten miteinander auszutauschen und gleichzeitige Abfragen verschiedener Datenbanken durch zugriffsberechtigte Behörden zu ermöglichen.

Digitale Grenzkontrollen und zentrale Datenbanken

Im Jahr 2011 konkretisierte die Europäische Kommission diese Pläne mit ihrer „Initiative für intelligente Grenzen”: Durch die Digitalisierung und Automatisierung der Grenzkontrollen sollten einerseits die Grenzübertritte für als vertrauenswürdig eingestufte Reisende erleichtert werden und andererseits eine intensivere Kontrolle ein- und ausreisender Drittstaatsangehöriger erfolgen.[3] Im selben Jahr richtete die Europäische Union die EU-Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) ein, um die Europäische Kommission in der Entwicklung und im Betrieb der IT-Systeme zu entlasten. Durch die Schaffung einer eigenen, zentralen Verwaltungsstruktur für die europäischen IT-Systeme wurde die Interoperabilität maßgeblich vorangetrieben.

Den ersten Vorschlag eines Smart Borders Package (Maßnahmenpaket Intelligente Grenzen) stellte die Europäische Kommission im Jahr 2013 vor. Das Europäische Parlament und der Rat der Europäischen Union sahen die Umsetzbarkeit der

Maßnahmen jedoch aufgrund von technischen, operativen und finanziellen Bedenken kritisch.[4] 2016, vor dem Hintergrund der großen Fluchtbewegung vor dem syrischen Bürgerkrieg und der Terroranschläge in Paris und Brüssel, legte die Kommission ein überarbeitetes Maßnahmenpaket vor. Sie schlug zwei Rechtsakte vor, zum einen zur Einführung des Einreise-/Ausreisesystems (englisch: Entry-Exit-System, EES) (VO (EU) 2017/2226) und zum anderen zur Anpassung der Kontrollen an den Außengrenzen durch eine entsprechende Änderung des Schengener Grenzkodex (VO (EU) 2017/2225). Im November 2017 nahmen Parlament und Rat die beiden Verordnungen an und schufen damit die rechtliche Grundlage für die Einführung des EES.

Im Jahr 2019 verabschiedeten das Europäische Parlament und der Ministerrat zwei EU-Verordnungen zur Interoperabilität (VO (EU) 2019/817 und VO (EU) 2019/818) und ermöglichten damit den Datenaustausch der europäischen IT-Großsysteme.[5] Vier Kernelemente sollen die behördliche Arbeit für Grenzschutz, Polizei, Justiz und Zoll erleichtern: (i) ein europäisches Suchportal, das die gleichzeitige Abfrage der sechs Systeme ermöglicht; (ii) ein Dienst für den Abgleich biometrischer Daten; (iii) ein gemeinsamer Speicher für Identitätsdaten und (iv) ein Detektor für Mehrfachidentitäten. Durch die Verknüpfung der IT-Systeme erhofft sich die Europäische Kommission, Synergien zwischen der Europäischen Sicherheitsagenda und der Europäischen Migrationsagenda zu schaffen.[6]

Die Datenbanken der Interoperabilität

Im Bereich Sicherheit, Grenzkontrolle und Migration der EU existieren drei IT-Großsysteme (Stand Dezember 2024). Drei weitere sollen in den nächsten Jahren hinzukommen. Um Daten miteinander austauschen zu können und die parallele Abfrage aller Datenbanken zu ermöglichen, sollen die folgenden Datenbanken miteinander interoperabel gemacht werden:

Die Fingerabdruckdatenbank **Eurodac** wurde 2003 als Hilfsmittel zur Durchsetzung der Dublin-Verordnung eingeführt, um asylsuchende Personen und Personen mit irregulärem Aufenthaltsstatus durch den Abgleich ihrer Fingerabdrücke dem Staat ihrer Erstankunft in der EU zuzuordnen. In den nächsten Jahren sollen neben Fingerabdrücken auch Gesichtsbilder und andere personenbezogene Daten gespeichert werden.

Das **Schengener Informationssystem (SIS)** ermöglicht seit 1995 die Personen- und Sachfahndung im Schengen-Raum, indem gesuchte Personen, Fahrzeuge, Identitätsdokumente und andere Sachen vermerkt und eingesehen werden können. Nach einer ersten Erneuerung 2013 (SIS II), die unter anderem die Erfassung biometrischer Daten in dem System ermöglichte, wurde das SIS 2023 weiter ausgebaut: Unter anderem erlaubt es nun präventive Fahndungen und erfasst neben Gesichtsbildern und Fingerabdrücken auch DNA-Daten vermisster Personen und Handflächenabdrücke.

Im **Visa-Informationssystem (VIS)** können die Schengen-Staaten seit 2011 alle Daten zu Personen speichern, die Anträge auf Kurzzeitvisa für die EU stellen. Dies soll die Bearbeitung von Visaanträgen erleichtern, Grenzkontrollen beschleunigen und Identitätsbetrug verhindern.

Das **Einreise-/Ausreisesystem (EES)** soll der Registrierung und Kontrolle von Drittstaatsangehörigen dienen, die für einen Kurzaufenthalt in die EU einreisen. Ursprünglich war die Inbetriebnahme für 2022 geplant. Im Oktober 2024 gab die damalige EU-Innenkommissarin Ylva Johansson eine erneute Verzögerung bekannt, sodass der Zeitpunkt der Einführung derzeit unklar ist. Medienberichten zufolge ist ein Start vor Frühjahr 2025 unwahrscheinlich.[7]

Das **Europäische Reiseinformations- und -genehmigungssystem (ETIAS)** soll der Sicherheitsüberprüfung visumbefreiter Drittstaatsangehöriger dienen, die in den Schengen-Raum einreisen wollen. Die Inbetriebnahme ist derzeit für 2025 geplant.

Das **Europäische Strafregisterinformationssystem (ECRIS)** ermöglicht seit 2012 den Austausch von Daten zu strafrechtlichen Verurteilungen von EU-Bürger*innen. Durch die Einführung von **ECRIS-TCN** soll das System um eine weitere Datenbank mit entsprechenden Informationen zu Drittstaatsangehörigen ergänzt werden. Ein

genaues Datum für die Inbetriebnahme des neuen Systems ist bisher nicht bekannt.

Das EES im Detail

Das Einreise-/Ausreisesystem stellt ein zentrales Element in den Bestrebungen der Europäischen Union nach „intelligenten Grenzen“ dar. Als europäische Datenbank erfasst und speichert es die Daten aller Drittstaatsangehörigen, die für einen Kurzaufenthalt (max. 90 Tage innerhalb von 180 Tagen) in eines der teilnehmenden europäischen Länder einreisen.[8] Dabei wird jeder Übertritt der Außengrenze eines Mitgliedsstaates sowie jede Einreiseverweigerung von Drittstaatsangehörigen elektronisch erfasst. Während sowohl visumpflichtige als auch visumbefreite Drittstaatsangehörige von der Datenerhebung betroffen sind, sollen die Daten von EU-Bürger*innen und Personen mit einer anderen Aufenthaltserlaubnis, wie beispielsweise einem nationalen Langzeitvisum oder einem Aufenthaltstitel als anerkannte*r Schutzsuchende*r, nicht im EES gespeichert werden (Artikel 2 EES-Verordnung).

Zweck, Ziele und Funktionen: Gemäß Absatz 15 EES-Verordnung soll das EES vorrangig der effizienteren Grenzkontrolle dienen und das „Außengrenzmanagement“ verbessern. Um die Bearbeitung der steigenden Anzahl an Grenzkontrollen bei begrenztem Personal zu gewährleisten sowie den Reisenden zügige Grenzübertritte zu ermöglichen, sollen die Verfahren an den Grenzen durch das EES (partiell) automatisiert und damit effizienter gestaltet werden. Darüber hinaus sollen Grenzkontrollen verschärft und sogenannte Aufenthaltsüberzieher*innen (englisch: overstayers) identifiziert werden. Neben dem Ziel, Migrationsbewegungen zu erfassen und zu steuern, dient das EES auch Strafverfolgungs- und Gefahrenabwehrzwecken. Durch die Zugriffsberechtigung für Behörden der Polizei, des Zolls, der Staatsanwaltschaften und nationalen Geheimdiensten soll es dazu beitragen, terroristische oder sonstige schwere Straftaten zu verhüten, aufzudecken und zu untersuchen.

Datenspeicherung im EES: Im EES werden zunächst alle im Reisepass enthaltenen Daten gespeichert, sowohl die Daten zur Person (Name, Geburtsdatum, Geschlecht, Staatsangehörigkeit) als auch zum Reisedokument (Art des Dokuments, Nummer, Gültigkeitsdauer). Darüber hinaus werden Datum, Uhrzeit und Ort des Grenzübertritts sowie die Grenzübergangsstelle erfasst. Bei visumpflichtigen Einreisenden werden außerdem Informationen zum Visum, zur ausstellenden Behörde und zu früheren Aufenthalten gespeichert; bei visumbefreiten Personen wird ihr Status (zum Beispiel Familienangehörige von Unionsbürger*innen) vermerkt. Neben alphanumerischen Daten werden im EES auch biometrische Daten in Form eines Gesichtsbildes und Fingerabdrücken verarbeitet. Ausgenommen von der Pflicht, Fingerabdrücke abzugeben, sind lediglich Kinder unter zwölf Jahren sowie Personen, bei denen die Abnahme aufgrund körperlicher Merkmale nicht möglich ist. Während der Grenzkontrolle werden das Gesichtsbild und die Fingerabdrücke mit den im Pass hinterlegten Daten abgeglichen, um festzustellen, ob die Person rechtmäßige Inhaberin des Passes ist.

Für jede Person werden die entsprechenden Daten in einem persönlichen Dossier regulär drei Jahre gespeichert. Bei Aufenthaltsüberzieher*innen beträgt die Speicherfrist bis zu fünf Jahre. Falls sich der Aufenthaltsstatus ändert (etwa weil die Person in einem EU-Mitgliedsstaat eingebürgert wird oder Asyl beantragt), müssen die Daten entsprechend vorzeitig gelöscht werden. Erfolgt keine Ausreise innerhalb der gültigen Aufenthaltsdauer, wird die Person innerhalb des EES automatisch gekennzeichnet und in die „Liste der Aufenthaltsüberzieher“ aufgenommen. Diese Liste soll nationalen Behörden wie der Bundespolizei automatisch zur Verfügung gestellt werden, damit diese „geeignete Maßnahmen” zum Umgang mit den betroffenen Personen treffen können (Artikel 12, 16 EES-Verordnung). Besagte Maßnahmen bleiben bisher unspezifiziert.

Personenbezogene, alphanumerische und biometrische Daten

Artikel 4 (1) der Datenschutz-Grundverordnung (DSGVO) definiert personenbezogene Daten als jegliche Informationen, die sich auf eine natürliche Person beziehen und so potenziell zu ihrer Identifizierung beitragen können. Dies können alphanumerische Daten sein wie zum Beispiel der Name, eine Ausweisnummer oder eine

IP-Adresse, oder biometrische Daten, also körperbezogene Daten wie der Fingerabdruck, ein Gesichtsbild, das Muster der Iris oder die Stimme.

Der Schutz personenbezogener Daten wird rechtlich in Artikel 7 und 8 der EU-Grundrechtecharta (GRCh) festgelegt. Aufgrund ihrer Universalität, Dauerhaftigkeit und Eindeutigkeit kommt biometrischen Daten dabei eine besondere Rolle zu. Da sie die eindeutige Identifizierung einer Person ermöglichen, gehören sie gemäß Artikel 9 der DSGVO zu den besonderen Kategorien personenbezogener Daten; ihre Verarbeitung ist demnach nur in bestimmten Fällen und unter besonderen Auflagen erlaubt. Auch der Europäische Gerichtshof für Menschenrechte hat wiederholt die besondere Schutzwürdigkeit von biometrischen Daten im Sinne von Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) betont.

Zugriff, Nutzung und Monitoring: Gemäß Artikel 9 der EES-Verordnung sollen Grenz-, Visum-/Einwanderungsbehörden sowie Gefahrenabwehr- und Strafverfolgungsbehörden Zugriff auf die erhobenen Daten erhalten.[9] Behörden, die EES-Daten zu Zwecken der Strafverfolgung oder Gefahrenabwehr nutzen, müssen zunächst einen Antrag auf Dateneinsicht stellen, der von einer nationalen zentralen Zugangsstelle geprüft wird; die zentrale Zugangsstelle und die Strafverfolgungsbehörde dürfen dabei Teil der gleichen Organisation sein (Artikel 19). Artikel 46 wiederum verpflichtet die Europäische Agentur für IT-Großsysteme (eu-LISA) dazu, Protokolle zu allen Datenverarbeitungsvorgängen im EES zu führen. Die Verarbeitung personenbezogener Daten durch eu-LISA muss mindestens alle drei Jahre durch den Europäischen Datenschutzbeauftragten überprüft werden. Die Datenverarbeitung durch die Mitgliedsstaaten soll durch die nationalen Aufsichtsbehörden nach DSGVO überwacht werden. Dies umfasst die Anzahl an Anträgen auf Vervollständigung, Berichtigung und Löschung der Daten sowie die Folgen der Anträge (Artikel 55 (2), 56).

Das EES in Deutschland

Die Implementierung des EES in Deutschland wird durch das Gesetz zur Durchführung des Einreise-/Ausreisesystems (EESDG) vom 20. April 2023 geregelt. Das EESDG ist Teil eines umfangreichen Gesetzespakets, das auch die Durchführung der ETIAS-Verordnung umfasst und Anpassungen am Aufenthaltsgesetz, am Freizügigkeitsgesetz und dem Rechtsrahmen des Ausländerzentralregisters vornimmt. Primär legt das EESDG nationale Zuständigkeiten fest und spezifiziert die Bedingungen für die Nutzung der EES-Daten zu Strafverfolgungs- und Gefahrenabwehrzwecken.

Demnach leitet das Bundesverwaltungsamt (BVA) die Implementierung und Anwendung des EES. Es ist damit für die Datenverarbeitung sowie die Bereitstellung nötiger Infrastruktur verantwortlich und soll gewährleisten, dass befugte nationale Behörden auf das EES und alle damit verbundenen Anwendungen zugreifen können. Gemeinsam mit der Bundespolizei, dem Bundesamt für Sicherheit in der Informationstechnik, dem Bundeskriminalamt und dem Informationstechnikzentrum setzt das BVA die EU-Verordnung um. Die Arbeit erfolgt in Kooperation mit Vertreter*innen der Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI). Die BfDI sowie die Datenschutzbeauftragten der Länder sind in Deutschland für die Überwachung der rechtskonformen Datenverarbeitung zuständig (Artikel 1 EESDG; Artikel 55 EES-Verordnung).[10]

Zum Zweck der Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten sollen die Bundespolizei, sonstige mit grenzpolizeilichen Aufgaben betraute Behörden, Zollkriminalamt und -fahndungsdienst sowie die Kriminalämter und Staatsanwaltschaften von Bund und Ländern auf das EES zugreifen können. Mit den Verfassungsschutzbehörden, dem Bundesnachrichtendienst und dem Militärischen Abschirmdienst sind außerdem die Geheimdienste zugriffsberechtigt (Artikel 2 EESDG).

Grund- und menschenrechtliche Relevanz des EES

Die Inbetriebnahme des EES ist für 2025 geplant. Die Auswirkungen von Technologien und IT-Systemen bei Grenzkontrollen auf die Grund- und Menschenrechte beschäftigen Menschenrechtsakteure jedoch schon viel länger. So begleiten unter anderem das Europäische Netzwerk nationaler Menschenrechtsorganisationen (ENNHRI), die EU-Agentur für Grundrechteagentur (FRA), Menschenrechtsorganisationen, nationale Datenschutzbehörden sowie Wissenschaftler*innen aus der Sicherheits- und Migrationsforschung das Projekt der Interoperabilität und die Einführung des EES seit Jahren mit kritischer Aufmerksamkeit. Bedenken bestehen insbesondere in Bezug auf Datenschutzrechte sowie eine mögliche Stigmatisierung und Verunsicherung von Migrant*innen.

Risiken für den Datenschutz: Aufgrund der umfassenden Datenverarbeitung berührt das EES den Schutzbereich des Grund- und Menschenrechts auf Privatsphäre und Datenschutz. Dies betrifft insbesondere Artikel 7 (Recht auf Privatleben) und Artikel 8 (Recht auf Datenschutz) der Europäischen Grundrechtecharta (GRCh), Artikel 8 (Recht auf Achtung des Privat- und Familienlebens) der EMRK sowie Artikel 17 (Schutz des Privatlebens) des UN-Zivilpaktes (ICCPR). Zusätzlich gelten seit 2018 die Vorschriften der Datenschutzgrundverordnung (DSGVO) und der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (JI-Richtlinie).

Datenschutzrechtliche Bedenken betreffen zunächst die Frage, ob die Umsetzung des EES mit Grundsätzen des Datenschutzes vereinbar ist. Laut der EU-Grundrechteagentur (FRA) wird das Zweckbindungsprinzip, nach dem personenbezogene Daten nur zu einem festgelegten Zweck verarbeitet werden dürfen (zum Beispiel Artikel 8 (2) GRCh), durch die Interoperabilität des EES mit anderen großen IT-Systemen herausgefordert.[11] Wissenschaftler*innen bezeichnen die Implementierung der Interoperabilität daher als Paradigmenwechsel: Durch die Vernetzung der sechs EU-Datenbanken werde die Limitierung der Datenabfrage zu den vorgesehenen Zwecken der Datenerhebung aufgehoben und Datenbanken operierten stattdessen wie Puzzleteile innerhalb der europäischen IT-Landschaft mit dem vorrangigen Zweck, einreisende Drittstaatsangehörige zu überwachen. Durch die steigende Anzahl der miteinander vernetzten IT-Systeme, der Zunahme der gespeicherten Daten sowie einer Ausweitung der Zugriffsberechtigungen komme es zu einer schleichenden Ausdehnung der Funktionen und Verwendungszwecke der Daten (function creep).[12]

Eine weitere Kritik richtet sich gegen Umfang und Ausmaß der Datenverarbeitung. Laut EU-Grundrechteagentur und Wissenschaftler*innen sei fraglich, ob diese vereinbar sind mit den Grundsätzen von Rechtmäßigkeit und Datensparsamkeit, nach dem nur so viele Daten gesammelt werden, wie für den jeweiligen Zweck notwendig sind (zum Beispiel Artikel 8 (2), 51 (1) GRCh). Demnach führe die Inklusion des EES sowie der anderen europäischen Datenbanken in den Interoperabilitätsrahmen dazu, dass die personenbezogenen Daten unzähliger Personen jahrelang gespeichert und abgefragt werden können, ohne dass sie in einem Zusammenhang mit Identitätsbetrug, Terrorismus oder sonstigen schweren Straftaten stehen.[13] Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder sieht darin eine anlasslose, nicht vertretbare Vorratsdatenspeicherung.[14] Herausgefordert werde der Rechtmäßigkeitsgrundsatz auch durch den Zugriff auf die Daten für Zwecke der Gefahrenabwehr und Strafverfolgung: So hat die FRA in einer Analyse zu Interoperabilität und Grundrechten festgestellt, dass die Nützlichkeit des Datenzugriffs allein noch nichts über die Notwendigkeit oder Verhältnismäßigkeit aussagt.[15] Wissenschaftler*innen warnen, dass die Entwicklung und Vernetzung von Instrumenten, die terroristische Straftaten verhindern sollen, leicht als Werkzeug zur Massenüberwachung aller EU-Bürger*innen und Drittstaatsangehörigen ausgestaltet werden können.[16] Der ehemalige Bundesbeauftragte für Datenschutz und Informationsfreiheit äußerte im Jahr 2023 zudem Bedenken hinsichtlich des Zugriffs durch deutsche Geheimdienste: Es sei fraglich, ob diese nach deutschem Recht Aufgaben von Gefahrenabwehr- und Strafverfolgungsbehörden im Sinne der EES-Verordnung wahrnehmen.[17]

Der Umgang mit biometrischen Daten

Die Verarbeitung großer Mengen biometrischer Daten stellt einen Kernaspekt des EES und des Interoperabilitätsvorhabens dar. ENNHRI sowie Wissenschaftler*innen bezeichnen die gesetzlichen Vorschriften zum Schutz biometrischer Daten, insbesondere in Bezug auf die Nutzung für Zwecke der Gefahrenabwehr und Strafverfolgung, als unzureichend: Demnach bedürfe es strengeren Zugriffsvoraussetzungen für Strafverfolgungsbehörden und effektiven und umfassenden Verfahren bei Rechtsverstößen.[18]

Der Abgleich von Gesichtsbildern oder Fingerabdrücken in verschiedenen Datenbanken soll zur Feststellung von Identitätsbetrug und Dokumentenfälschung beitragen. Die große Menge der im EES erfassten Daten erhöht jedoch Risiken, die sich durch mangelhafte Datenqualität, verursacht beispielsweise durch Rechtschreibfehler, Übersetzungsschwierigkeiten oder veraltete biometrische Gesichtsbilder, für Betroffene ergeben. Laut Kritiker*innen seien die Auswirkungen fehlerhafter Daten in Anbetracht der großen Anzahl an betroffenen Personen sowie der Interoperabilität, durch welche fehlerhafte Datensätzen in anderen Datenbanken reproduziert werden können, besonders problematisch.[19] Bei Grenzkontrollen oder Visaentscheidungen können Daten von geringer Qualität zu fälschlichen Ablehnungsbescheiden führen; bei der Nutzung zu Strafverfolgungszwecken kann es sogar zu ungerechtfertigten Verfahren gegen Unbeteiligte kommen. Selbst eine Fehlerquote der Abgleichverfahren von weniger als einem Prozent bedeutet eine hohe absolute Zahl bei Massendatenbanken.

ENNHRI und Wissenschaftler*innen vermerken außerdem, dass Verfahren des biometrischen Abgleichs höhere Fehlerquoten beim Umgang mit Gesichtsbildern von Schwarzen Personen, nonbinären Personen sowie Frauen und Kindern aufweisen.[20] Die Folge können Diskriminierungseffekte von ohnehin marginalisierten Personengruppen sein. In diesem Zusammenhang weist die FRA darauf hin, dass die Interoperabilität allein durch die Nutzung von Algorithmen zu einer ungleichen Behandlung aus Gründen des Geschlechts, der Hautfarbe, einer Behinderung oder aus rassistischen Gründen führen kann, die einen Verstoß gegen Artikel 21 GRCh darstellen würde.[21]

Intransparenz der Datenverarbeitung: Allgemein gelten die Datenverarbeitung und die zugrundeliegenden Gesetze der Interoperabilitäts-Datenbanken, inklusive des EES, als undurchsichtig. Jede EU-Datenbank wurde durch eine oder mehrere eigene Verordnungen eingerichtet, die spezifische Regelungen zur Datenverarbeitung beinhalten. Diese umfassen eine Vielzahl an Querverweisen auf andere Rechtsakte und benötigen die Regelung von Details durch nationales Recht. Darüber hinaus wird die Interoperabilität durch zwei separate Verordnungen geregelt. Nicht nur für Rechtsanwender*innen, sondern auch für Betroffene erschwert diese Komplexität die Möglichkeit, die Datenverarbeitung nachzuvollziehen und gegebenenfalls Rechtsverletzungen geltend zu machen.[22] Zwar sieht die EES-Verordnung in Kapitel VII spezifische Datenschutzrechte vor, die zum Beispiel bei fehlerhaften oder rechtswidrig verarbeiteten Daten greifen sollen. Allerdings ist fraglich, ob diese Rechte in der Praxis den Betroffenen einen wirksamen Zugang zum Recht gewährleisten können. Dies gilt insbesondere für Drittstaatsangehörige, die sich nicht (mehr) in der EU befinden. Durch eine intransparente Datenverarbeitung und Gesetzeslage kann das Recht auf einen wirksamen Rechtsbehelf nach Artikel 47 GRCh und Artikel 13 EMRK daher erheblich eingeschränkt werden. Das Ziel, durch die Interoperabilität die Abfrage von Datenbanken für Polizeibeamt*innen zu erleichtern,[23] scheint somit zu Lasten der Transparenz und Durchsetzung datenschutzrechtlicher Grundsätze zu gehen.

Weitere Auswirkungen auf Migrant*innen

Während die EU-Kommission die engere Verbindung zwischen der EU-Migrationsagenda und der EU-Sicherheitsstrategie explizit als Anreiz und wünschenswertes Resultat des Interoperabilitätsprojektes anführt, bemerken ENNHRI, Menschenrechtsorganisationen und Wissenschaftler*innen, dass dadurch Grenzen von Strafverfolgungs- und Migrationsfragen verwischt und Migrant*innen stigmatisiert würden. Demnach fördere die Einführung und Ausweitung von Datenbanken im Bereich Innere Sicherheit und Gefahrenabwehr, in denen vorrangig Drittstaatsangehörige erfasst werden, die Darstellung von Migrant*innen als universelles Sicherheitsrisiko. Dies könnte eine pauschalisierende Krimina-

lisierung und Diskriminierung von Ausländer*innen zur Folge haben.[24] In einem Bericht zu den grundrechtlichen Auswirkungen biometrischer Datenerfassung durch europäische IT-Systeme verweist die FRA auf die Gefahr, dass Drittstaatsangehörige bei Systemfehlern in den biometrischen Abgleichverfahren schnell unrechtmäßig des Identitätsbetrugs bezichtigt werden. In diesem Zusammenhang verzeichnet die FRA eine Tendenz staatlicher Behörden, Asylsuchenden Identitätsbetrug zu unterstellen, bei gleichzeitiger schwacher (rechtlicher) Position der betroffenen Individuen.[25]

Darüber hinaus verweist ENNHRI darauf, dass Interoperabilität per se zwar keine Menschenrechtsverletzung darstelle, bislang jedoch die nötigen Sicherheitsvorkehrungen in der Umsetzung der Systeme fehle, um Menschenrechtsverletzungen vorzubeugen. Dabei würden sich Schwächen der EU-Datenbanken hinsichtlich des Grund- und Menschenrechtsschutzes insbesondere auf vulnerable Personengruppen und Menschen mit irregulärem Aufenthaltsstatus auswirken. Einer Studie der FRA zufolge kann zum Beispiel die Erfassung von Daten bei Menschen mit irregulärem Aufenthaltsstatus im Inland zu Ängsten und Verunsicherung hinsichtlich der Nutzung führen und diese dadurch davon abhalten, Grundleistungen wie medizinische Versorgung, Schulbildung oder Rechtsschutz in Anspruch zu nehmen.[26] Darüber hinaus kann das Teilen von Daten mit Drittstaaten im Falle von Abschiebungen ernsthafte Risiken für das Leben und die Freiheit der betroffenen Personen zur Folge haben.[27] Dies würde eine Gefahr für das Recht auf Leben und Unversehrtheit nach Artikel 2 und 3 GRCh und Artikel 3 EMRK bedeuten.

Fazit

Seit nunmehr zwanzig Jahren baut die Europäische Union die digitalen Grenzkontrollstrukturen des Schengenraumes aus. Dienten die ersten IT-Großsysteme noch der direkten Umsetzung von spezifischen Gesetzesänderungen im Rahmen des Schengen Abkommens, hat sich das Projekt “intelligente Grenzen” mittlerweile zu einer systematisierten und weitreichenden Struktur zur Überwachung von Drittstaatsangehörigen entwickelt, die der lückenlosen Erfassung aller Einreisenden dienen soll. Als Datenbank für alle Drittstaatsangehörigen, die für einen Kurzaufenthalt die Außengrenzen des Schengenraumes übertreten, stellt das EES einen zentralen Baustein in dieser Entwicklung dar.

Bei der Umsetzung der Systeme bestehen schwerwiegende grund- und menschenrechtliche Bedenken: Interoperable Datenbanken allgemein und das EES im Speziellen bergen die Gefahr, dass etwa das Recht auf Privatsphäre und Datenschutz, das Recht auf Achtung des Privat- und Familienlebens sowie das Recht auf einen wirksamen Rechtsbehelf verletzt werden. Infrage steht auch, inwieweit das Ausmaß der Verarbeitung personenbezogener Daten beziehungsweise der umfassende Zugriff nationaler Behörden auf diese Daten verhältnismäßig und den Zwecken angemessen ist. Zusätzlich können algorithmische Abgleichverfahren eine Diskriminierung bestimmter Personengruppen begünstigen. Darüber hinaus warnen Menschenrechtsinstitutionen und Wissenschaftler*innen vor den Folgen für Migrant*innen: Die Verwischung der Datenerhebung für Migrations- und Sicherheitszwecke kann zur Kriminalisierung und Stigmatisierung von Ausländer*innen führen und Betroffene davon abhalten, Grundleistungen in Anspruch zu nehmen. Diese Risiken für die Grund- und Menschenrechte machen deutlich: Der zukünftige Betrieb des EES und anderer europäischer IT-Großsysteme braucht in den nächsten Jahren dauerhafte und wirksame Kontrollmechanismen (über die Datenschutzaufsicht hinaus) sowie eine kritische, öffentliche Aufmerksamkeit – zum Beispiel von Nationalen Menschenrechtsinstitutionen und der Zivilgesellschaft. Die EU-Mitgliedsstaaten und nationalen Parlamente sind aufgerufen, bei der Umsetzung des EES auf die Einhaltung der Grund- und Menschenrechte zu dringen.

1 Die Autorin bedankt sich bei Nele Allenberg, Claudia Engelmann und Eric Töpfer für die fachliche Unterstützung und die wertvolle Kommentierung des Textes.
2 KOM (2005) 597 endgültig.
3 KOM(2011) 680 endgültig, S. 4.
4 Jeandesboz, Julien u.a. (2013): The Commission‘s Legislative Proposals on Smart Borders: Their feasibility and costs. Brüssel: Europäisches Parlament, PE 493.026, S. 8-10.
5 Die VO (EU) 2019/817 regelt die Interoperabilität im Bereich Grenzmanagement und Visa und die VO (EU) 2019/818 im Bereich Polizei, Justiz, Asyl und Migration.
6 COM(2016) 205 final, S. 2.
7 Netzpolitik (01.11.2024): Geplantes EU-Biometriesystem wird zum Desaster. https://netzpolitik.org/2024/ein-ausreisesystem-geplantes-eu-biometriesystem-wird-zum-desaster/ (abgerufen am 14.11.2024); euronews (11.10.2024). ‘Politically courageous’: EU postpones Entry/Exit System once again – but what’s behind it? https://www.euronews.com/travel/2024/10/11/politically-courageous-eu-postpones-entryexit-system-once-again-but-whats-behind-it (abgerufen am 14.11.2024).
8 Das EES soll in allen Ländern der EU mit Ausnahme von Irland und Zypern verwendet werden. Darüber hinaus wird es auch in Norwegen, Liechtenstein, Island und der Schweiz eingeführt.
9 Die konkreten Behörden können sich in den Mitgliedsstaaten unterscheiden und werden von diesen Mitgliedsstaaten benannt.
10 Bundesverwaltungsamt (19.05.2024): Entry Exit System (EES). https://www.bva.bund.de/DE/Das-BVA/Aufgaben/S/Smart_Borders/_documents/EES-FAQ.html (abgerufen am 14.11.2024).
11 FRA - European Union Agency for Fundamental Rights (2017): Fundamental rights and the interoperability of EU information systems: borders and security, S. 21-23, Luxemburg.
12 Aden, Hartmut (2020): Interoperability Between EU Policing and Migration Databases: Risk for Privacy, In: European Public Law 26, Nr. 1, S. 95; Arden, Anna / Züllig, Leon (2023): Intelligente Grenzen? Potenziale und Risiken von Smart Borders. In: Zeitschrift für Ausländerrecht und Ausländerpolitik, 11-12, S. 410; Bunyan, Tony (2018): The “Point of no return.” Interoperability morphs into the creation of a Big Brother centralised EU state database including all existing and future Justice and Home Affairs databases. Statewatch Analysis 332, S. 14, London: Statewatch; Vavoula, Niovi (2022): Interoperability of EU Information Systems in a ’Panopticon’ Union: A Leap towards Maximised Use of Third-Country Nationals’ Data or a Step Backwards in the Protection of Fundamental Rights? In: Mitsilega, Valsamis / Vavoula, Niovi (Hg.): Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives; Quintel, Teresa (2018): The impact of Interoperability on the processing of (Biometric) Data of Third Country Nationals by Europol. In: Kritische Vierteljahreszeitschrift für Gesetzgebung und Rechtswissenschaft, S. 347.
13 Aden, Hartmut / Töpfer, Eric (2020): Problematische Interoperabilität von EU-Polizei- und Migrationsdatenbanken. In: Armbruster, Leoni u.a. (Hg.): Grundrechte-Report 2020. Zur Lage der Bürger- und Menschenrechte in Deutschland. Frankfurt/Main: Fischer, S. 42; FRA - European Union Agency for Fundamental Rights (2017): Fundamental rights and the interoperability of EU information systems: borders and security, S. 19-24; Vavoula, Niovi (2022): Interoperability of EU Information Systems in a ’Panopticon’ Union: A Leap towards Maximised Use of Third-Country Nationals’ Data or a Step Backwards in the Protection of Fundamental Rights? In: Mitsilega, Valsamis / Vavoula, Niovi (Hg.): Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives.
14 Datenschutzkonferenz (2017): Keine anlasslose Vorratsspeicherung von Reisedaten, Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, 09.11.2017.
15 FRA - European Union Agency for Fundamental Rights (2018): Interoperability and fundamental rights implications. Opinion of the European Union Agency for Fundamental Rights, FRA Opinion – 1/2018, S. 29-30, Vienna.
16 Vavoula, Niovi (2022): Interoperability of EU Information Systems in a ’Panopticon’ Union: A Leap towards Maximised Use of Third-Country Nationals’ Data or a Step Backwards in the Protection of Fundamental Rights? In: Mitsilega, Valsamis / Vavoula, Niovi (Hg.): Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives.
17 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2023): Tätigkeitsbericht BfDI 2022. 21. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit, S. 54, Bonn.
18 European Network of National Human Rights Institutions (2024): Technologies, migration, and human rights: the role of European NHRIs, ENNHRI scoping paper, S. 13; Vavoula, Niovi (2022): Interoperability of EU Information Systems in a ’Panopticon’ Union: A Leap towards Maximised Use of Third-Country Nationals’ Data or a Step Backwards in the Protection of Fundamental Rights? In: Mitsilega, Valsamis / Vavoula, Niovi (Hg.): Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives; Quintel, Teresa (2018): The impact of Interoperability on the processing of (Biometric) Data of Third Country Nationals by Europol. In: Kritische Vierteljahreszeitschrift für Gesetzgebung und Rechtswissenschaft, S. 347.
19 Arden, Anna / Züllig, Leon (2023): Intelligente Grenzen? Potenziale und Risiken von Smart Borders. In: Zeitschrift für Ausländerrecht und Ausländerpolitik, 11-12, S. 409; European Network of National Human Rights Institutions (2024): Technologies, migration, and human rights: the role of European NHRIs, ENNHRI scoping paper, S. 13.
20 Arden, Anna / Züllig, Leon (2023): Intelligente Grenzen? Potenziale und Risiken von Smart Borders. In: Zeitschrift für Ausländerrecht und Ausländerpolitik, 11-12, S. 409; European Network of National Human Rights Institutions (2024): Technologies, migration, and human rights: the role of European NHRIs, ENNHRI scoping paper, S. 15; Ozkul, Derya (2023): Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe, S. 5. Oxford: Refugee Studies Centre, University of Oxford.
21 FRA - European Union Agency for Fundamental Rights (2018): Interoperability and fundamental rights implications. Opinion of the European Union Agency for Fundamental Rights, FRA Opinion – 1/2018, S. 13, Vienna.
22 Aden, Hartmut (2020): Interoperability Between EU Policing and Migration Databases: Risk for Privacy, In: European Public Law 26, Nr. 1, S. 108; Töpfer, Eric (2022): (Ver)Wachsende Datenbanken. Digitale Grenzen als Integrationsprojekt. In: Bürgerrechte und Polizei/CILIP 128, S. 37-39.
23 Europäische Kommission (06.04.2016): Mitteilung der Kommission an das Europäische Parlament und den Rat. Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit. COM(2016) 205 final, S. 3.
24 Aden, Hartmut / Töpfer, Eric (2020): Problematische Interoperabilität von EU-Polizei- und Migrationsdatenbanken. In: Armbruster, Leoni u.a. (Hg.): Grundrechte-Report 2020. Zur Lage der Bürger- und Menschenrechte in Deutschland. Frankfurt/Main: Fischer, S. 41; European Network of National Human Rights Institutions (2024): Technologies, migration, and human rights: the role of European NHRIs, ENNHRI scoping paper, S. 14; Jones, Chris (2019): Data Protection, Immigration Enforcement and Fundamental Rights: What the EU‘s Regulations on Interoperability Mean for People with Irregular Status, Brüssel: PICUM and Statewatch.
25 FRA - European Union Agency for Fundamental Rights (2018): Under watchful eyes: biometrics, EU IT systems and fundamental rights, S. 20. Luxemburg.

26 FRA - European Union Agency for Fundamental Rights (2017): Fundamental rights and the interoperability of EU information systems: borders and security, S. 41, Luxemburg; siehe auch McGregor, Lorna / Molnar, Petra (2023): Digital Border Governance: A Human Rights Based Approach, S. 14. Geneva: University of Essex, OHCHR.

27 McGregor, Lorna / Molnar, Petra (2023): Digital Border Governance: A Human Rights Based Approach, S. 15. Geneva: University of Essex, OHCHR.

Impressum

Information Nr. 52 | Dezember 2024 | ISSN 2509-9493 (PDF)

HERAUSGEBER: Deutsches Institut für Menschenrechte
Zimmerstraße 26/27 | 10969 Berlin
Tel.: 030 259 359–0 | Fax: 030 259 359–59
info@institut-fuer-menschenrechte.de
www.institut-fuer-menschenrechte.de

AUTORIN: Karla Marek

Das Institut

Das Deutsche Institut für Menschenrechte ist die unabhängige Nationale Menschenrechtsinstitution Deutschlands (§ 1 DIMR-Gesetz). Es ist gemäß den Pariser Prinzipien der Vereinten Nationen akkreditiert (A-Status). Zu den Aufgaben des Instituts gehören Politikberatung, Menschenrechtsbildung, Information und Dokumentation, anwendungsorientierte Forschung zu menschenrechtlichen Themen sowie die Zusammenarbeit mit internationalen Organisationen. Es wird vom Deutschen Bundestag finanziert. Das Institut ist zudem mit dem Monitoring der Umsetzung von UN-Behindertenrechtskonvention und UN-Kinderrechtskonvention sowie der Berichterstattung zu den Konventionen des Europarats zu Menschenhandel und zu Gewalt gegen Frauen und häuslicher Gewalt betraut worden. Hierfür hat es entsprechende Monitoring- und Berichterstattungsstellen eingerichtet.