17. September 2025 POL 30/0290/2025

Advocacy-Briefing zur Verteidigung der Rechte von Geflüchteten, Asylsuchenden und Migrant:innen im digitalen Zeitalter

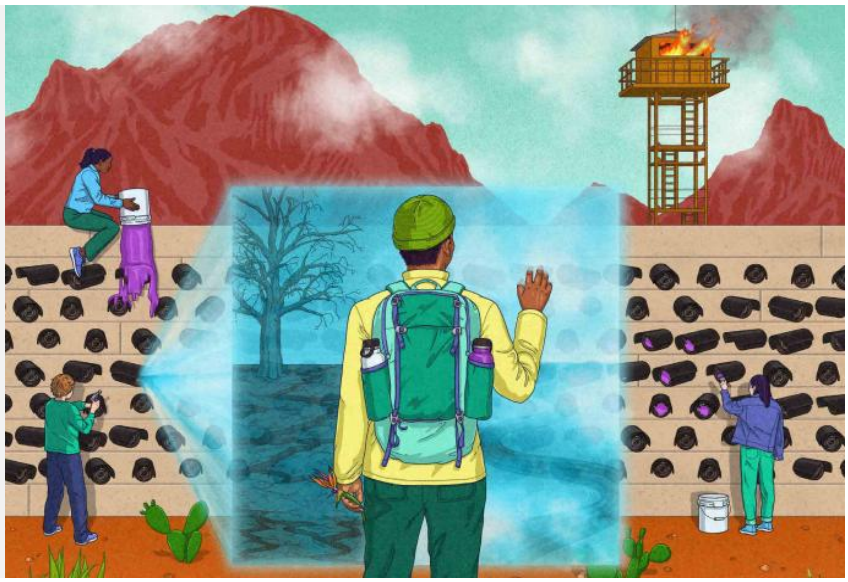

Illustration von Eliana Rodgers: „A Dream Deterred". Ein Migrant wird an einem Grenzübergang mit massiver Überwachung konfrontiert und an seine ungewisse Zukunft erinnert. Aktivist:innen setzen sich gegen diese Überwachungssysteme und Mauern ein.

Titelbild für die Broschüre „Defending the Rights of Refugees and Migrants in the Digital Age" von Amnesty International, 2024, Index: POL 40/7654/2024.

Inhalt

Einleitung

Amnesty International ist eine weltweite Bewegung von mehr als 10 Millionen Menschen, die sich für eine Zukunft einsetzen, in der alle Menschen ihre Menschenrechte wahrnehmen können. Unsere Vision ist eine Welt, in der Machthaber:innen ihre Versprechen einhalten, das Völkerrecht achten und zur Rechenschaft gezogen werden. Wir sind unabhängig von Regierungen, politischen Ideologien, wirtschaftlichen Interessen und Religionen und finanzieren uns hauptsächlich durch unsere Mitgliederbeiträge und private Spenden. Wir glauben, dass weltweite Solidarität und Mitgefühl mit Menschen unsere Gesellschaften zum Besseren verändern können.

AlgorithmWatch ist eine gemeinnützige Nichtregierungsorganisation in Berlin und Zürich. Wir setzen uns dafür ein, dass Algorithmen und Künstliche Intelligenz Gerechtigkeit, Demokratie, Menschenrechte und Nachhaltigkeit stärken, statt sie zu schwächen. Unsere Vision ist eine Welt, in der Technologie im Allgemeinen und algorithmische Systeme im Besonderen den Menschen zugutekommen. Die Systeme sollen Gesellschaften gerechter, demokratischer, inklusiver und nachhaltiger machen – sei es hinsichtlich zugeschriebener Herkunft und Gender, Rassifizierung, sexueller Orientierung, Alter, Klasse und Wohlstand oder Ressourcenverbrauch.

Die #ProtectNotSurveil Koalition ist in Europa ansässig und besteht aus Aktivist:innen, Organisationen, Forscher:innen und anderen, die sich dafür einsetzen, dass die Digital- und Migrationspolitik Menschen auf der Flucht vor Schäden durch KI-Systeme schützt. Unsere Mission ist es, den Einsatz digitaler Technologien auf verschiedenen Ebenen der EU-Politik zu hinterfragen und uns dafür einzusetzen, dass Menschen sich frei bewegen und Sicherheit suchen können, ohne Schaden, Überwachung oder Diskriminierung zu riskieren. Unser Engagement zielt darauf ab, die EU, ihre Mitgliedstaaten und private Unternehmen, die von Menschenrechtsverletzungen an und innerhalb der EU-Grenzen profitieren, zur Verantwortung zu ziehen. Dazu verbinden wir Organisationen für digitale Rechte, Migrationsrecht und Antirassismus, um technokratische Lösungsansätze in der Migrationspolitik in Frage zu stellen.

Über dieses Dokument

Dieses Dokument ist als Advocacy-Ressource für Aktivist:innen, Fürsprecher:innen, Akteur:innen der Zivilgesellschaft und Communities, die von digitalen Technologien und Überwachung im Asyl- und Migrationskontext betroffen sind, gedacht. Es bietet einen Menschenrechtsrahmen und Grundsätze, anhand derer die Auswirkungen neuer und bestehender Technologien auf Geflüchtete, Asylsuchende und Migrant:innen analysiert werden können. Das schließt auch die Berücksichtigung diskriminierender und intersektionaler Folgen der Systeme mit ein. Zudem enthält das Dokument Empfehlungen für Staaten, Unternehmen, internationale Organisationen und Dienstleister:innen, die digitale Technologien und Überwachungssysteme entwickeln und/oder einsetzen.

Dieses Dokument wurde von Amnesty International mit Unterstützung von AlgorithmWatch, Border Violence Monitoring Network (BVMN), EuroMed Rights und Privacy International verfasst. Die Grundlage bieten die rechtlichen und politischen Empfehlungen der Koalition #ProtectNotSurveil zu Migration, Asyl und Grenzüberwachungstechnologien, einschließlich der Entwicklung und Nutzung Künstlicher Intelligenz (KI). Es ist als „lebendiges" Dokument konzipiert, das regelmäßig

aktualisiert wird.[1] Die Übersetzung aus dem Englischen ins Deutsche hat AlgorithmWatch übernommen. Es ist zu beachten, dass die aufgeführten Empfehlungen keineswegs erschöpfend sind, sondern vielmehr als Ausgangspunkt für nationale und internationale Advocacy-Arbeit dienen sollen. Der Abschnitt „Quellen" enthält eine Liste von Publikationen, in denen diese Empfehlungen ursprünglich formuliert wurden.

Einsatz digitaler Technologien im Asyl- und Migrationskontext

Digitale Technologien sind zu allgegenwärtigen, risikoreichen und oft experimentellen Instrumenten in der Gestaltung und Umsetzung der Migrations- und Asylpolitik von Staaten und regionalen Organisationen geworden. Von Satellitenbildern, Drohnen und anderen Sensordaten bis hin zu Gesichtserkennung, Iris-Scans und sog. „Lügendetektoren": Im Grenz- und Migrationskontext wird auf diverse fragwürdige Technologien vertraut.

Sowohl direkt als auch indirekt haben digitale Technologien das Potenzial, schwerwiegende Menschenrechtsverletzungen zu verursachen oder zu verstärken. Wenn Staaten aktiv eine Agenda vorantreiben, die im Widerspruch zu ihren Menschenrechtsverpflichtungen gegenüber Geflüchteten und Migrant:innen steht, besteht die Gefahr, dass diese Technologien Menschenrechtsverletzungen und Leiden verschärfen. Grenz- und Migrationstechnologien können auch an sich problematisch sein, da ihre Systeme anfällig für Verzerrungen (sog. „Bias") und Fehler sind. Oft beruhen sie auf einer übermäßigen Erhebung, Speicherung und Nutzung von Informationen, die das Recht auf Privatsphäre, Nichtdiskriminierung und andere Menschenrechte gefährden.
Digitale Technologien verstärken repressive Grenzregime, die aufgrund von Rassifizierung, ethnischer Zugehörigkeit, nationaler Herkunft und Staatsangehörigkeit diskriminieren. Inhärenter Rassismus und Diskriminierung sind tief in den Migrationsmanagement- und Asylsystemen verwurzelt. Digitale Technologien bergen die Gefahr, dass rassistische Vorurteile und Diskriminierung, die in historischen und kolonialen Praktiken der rassistischen Ausgrenzung begründet sind, unter dem Deckmantel der technologischen Neutralität und Objektivität fortbestehen und verschleiert werden. Ihr Einsatz kann zu negativen Folgen für rassifizierte Gruppen führen und verschiedene Formen der Diskriminierung schaffen, wodurch systemischer Rassismus, Unterdrückung und Gewalt fortbestehen.

In den letzten Jahren ist die Tendenz zu beobachtet, dass Technologien, die für Migrations- und Grenzmanagementzwecke eingesetzt werden, von bestimmten Vorschriften ausgenommen werden. Darunter befinden sich u.a. Ausnahmen von Datenschutz- und Datensicherheitsvorschriften, Anforderungen an die öffentliche Rechenschaftspflicht und Transparenz.[2] Dies geschieht im

[1] Das Dokument wird alle 12 Monate überprüft und wenn wir wichtige ad-hoc-Rückmeldungen erhalten, um die Empfehlungen zu aktualisieren. Rückmeldungen können an charlotte.phillips@amnesty.org gesendet werden.

[2] Siehe bspw. #ProtectNotSurveil (2024). Joint statement – A dangerous precedent: How the EU AI Act fails migrants and people on the move. https://www.accessnow.org/press-release/joint-statement-ai-act-fails-migrants-and-people-on-the-move/.

Rahmen einer allgemeinen Verlagerung hin zur Kriminalisierung von Migration[3] und der Vermischung von Migrations-, Polizei- und nationaler Sicherheitspolitik.[4]

Durch diese Trends wird der Bedarf immer größer und dringlicher, Staaten, Unternehmen und andere Interessengruppen dazu aufzufordern, sicherzustellen, dass jede Entwicklung und Nutzung von neuen Technologien die Menschenrechte aller, einschließlich von Geflüchteten, Asylsuchenden und Migrant:innen, achtet und schützt. Transparenz ist eine Form der Absicherung und ein wichtiger erster Schritt zur Verwirklichung von Rechten, Gerechtigkeit und Rechenschaftspflicht. Isoliert kann Transparenz aber keine Rechte schützen, sondern muss von anderen Schutzmaßnahmen begleitet werden. Es ist ganz klar: Wenn Schäden nicht verhindert oder gemildert werden können und Technologien schon im Design mit internationalen Menschenrechtsnormen unvereinbar sind, müssen diese Technologien verboten werden.

Leitprinzipien und Rahmenbedingungen

Staaten haben gemäß dem internationalen Recht der Menschenrechte verbindliche Verpflichtungen und Pflichten. Das bedeutet, dass sie die Menschenrechte aller Menschen achten, schützen und verwirklichen müssen. Internationale Organisationen, Unternehmen und andere nichtstaatliche Akteur:innen müssen die Menschenrechte ebenfalls achten.

Um einen menschenrechtsbasierten Ansatz zu folgen, ist es hilfreich, einige übergeordnete Grundsätze und Rahmenbedingungen zu beachten, die auf jede potenzielle Technologie im Bereich Asyl und Migration (und ganz allgemein) angewendet werden sollten. Dazu gehören:

Technologie ist nicht neutral. Finanzielle und andere Anreize, strukturelle Macht- und Unterdrückungssysteme, institutioneller Rassismus, verschiedene Diskriminierungsformen, Ungleichheit und politische Rahmenbedingungen fließen in die Technologie ein und werden durch deren Einsatz reproduziert. In vielen Fällen ist Technologie ein Instrument, das in der Absicht oder Praxis rassistisch und diskriminierend sein kann.

Kritische Haltung gegenüber dem „Tech-Solutionismus"– der Vorstellung, dass komplexe soziale, wirtschaftliche und politische Probleme durch Technologie überwunden werden können. Anstatt davon auszugehen, dass die Entwicklung und der Einsatz von Technologien notwendig oder unvermeidlich ist, sollte frühzeitig und kontinuierlich hinterfragt werden, ob bestimmte Technologien tatsächlich notwendig oder nützlich sind, um das jeweilige Problem zu lösen. Statt Problemlösung können neue Technologien nämlich auch Probleme verschärfen oder (unbeabsichtigt) verursachen.

[3] Equinox Initiative for Racial Justice (2025): Towards a safer migration system: Ending the criminalisation of migration & solidarity. Equinox's position on the EU Facilitator's Package. https://www.equinox-eu.com/wp-content/uploads/2025/07/Ending-the-criminalisation-of-migration-solidarity.pdf.

[4] Siehe bspw. The New York Times (2025). Trump fordert 20.000 zusätzliche Beamte zur Unterstützung der Abschiebungsbemühungen. https://www.nytimes.com/2025/05/10/us/politics/dhs-deportation-extra-officers.html

Neue Technologien müssen die Menschenrechte (sowohl direkt als auch indirekt) achten, schützen und fördern, einschließlich Nichtdiskriminierung, Privatsphäre, Recht auf Leben, Recht auf Asyl, Recht auf Freiheit und das Prinzip der Nichtzurückweisung. Dies gilt auch für den Export von Technologien in andere Rechtsordnungen.

Intersektionalität ist entscheidend. Staaten und Unternehmen sollten die direkten und indirekten Auswirkungen und Risiken der Technologie-Designs und ihrer Nutzung abschätzen. Dies muss frühzeitig, vor der Einführung und kontinuierlich erfolgen und sollte unter Berücksichtigung einer intersektionalen Perspektive geschehen. Das bedeutet, dass Staaten, Unternehmen und andere Akteur:innen untersuchen müssen, wie sich durch die Interaktion mit den Technologien verschiedene Formen der Diskriminierung überschneiden und verstärken.

Verbindliche Umsetzung. Maßnahmen zur Regulierung von Technologien sollten verbindlich und durchsetzbar sein**.** Dies ist besonders wichtig, da es bereits viele *softe*, unverbindliche Ethikkodizes, Verhaltenskodizes und Richtlinien gibt, die oft keinen angemessenen Schutz gewährleisten.

Transparenz, Rechenschaftspflicht und Zugänglichkeit. Informationsfreiheit ist ein wesentlicher Bestandteil des Rechts auf freie Meinungsäußerung.[5] Staaten, Unternehmen und andere Akteur:innen müssen Transparenz, Rechenschaftspflicht und den Zugang zu relevanten Informationen sicherstellen. Dies ist entscheidend, um eine öffentliche Kontrolle sowie die Beteiligung verschiedener Interessengruppen, insbesondere der Betroffenen, an politischen Entscheidungsprozessen zu ermöglichen. Transparenz muss sich auch auf die Rollen und Verantwortlichkeiten aller Beteiligten in Entwicklung, Beschaffung und Umsetzung erstrecken. Dabei gilt: Transparenz ist ein wichtiger erster Schritt, reicht jedoch allein nicht aus.

Betroffene Communities einbinden. Staaten, Unternehmen und andere Akteur:innen müssen eine sinnvolle Beteiligung der betroffenen Communities sicherstellen. Policy-Diskussionen sollten sich an den Bedürfnissen und Prioritäten dieser Communities orientieren. Dafür ist es notwendig, ausreichende Ressourcen bereitzustellen, um eine gleichberechtigte Beteiligung von repräsentativen Interessenvertreter:innen und Organisationen zu ermöglichen. Zudem müssen faire Rahmenbedingungen für alle Interessengruppen und Rechteinhaber:innen geschaffen und Erfahrungswissen als wertvolle Expertise anerkannt werden. Besonderes Gewicht sollte dabei den

[5] Menschenrechtsausschuss der Vereinten Nationen (12. September 2011). Allgemeine Bemerkung 34, Internationaler Pakt über bürgerliche und politische Rechte. CCPR/C/GC/34, Abs. 18-19. https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

Stimmen und Perspektiven der betroffenen Communities sowie den zivilgesellschaftlichen Akteur:innen der Globalen Mehrheit zukommen.

Empfehlungen

Empfehlungen an Staaten

Vollständige Verbote

Unter keinen Umständen sollten Staaten die Entwicklung, Herstellung, den Verkauf, die Verwendung, den Export und Import von Technologien zulassen, die aufgrund ihrer Beschaffenheit Menschenrechte verletzen, irreparable, irreversible Schäden verursachen und/oder inakzeptable Risiken darstellen. In diesen Fällen sollten Staaten vollständige Verbote erlassen. Zu diesen Technologien gehören:

- Automatisierte Risikobewertungs-, Scoring- und Profilsysteme im Zusammenhang mit Migrationsmanagement, Asyl und Grenzkontrolle (einschließlich Betrugserkennungssystemen): Solche Systeme sollen bewerten, ob Migrant:innen oder Geflüchtete ein „Risiko" für rechtswidrige Handlungen oder Sicherheitsbedrohungen darstellen. Dabei sind diese Systeme von Natur aus diskriminierend, da sie Menschen aufgrund von Faktoren außerhalb ihrer Kontrolle oder auf Grundlage diskriminierender Rückschlüsse aus persönlichen Merkmalen vorverurteilen. Solche Systeme verletzen grundlegende Rechte, darunter das Recht auf Gleichheit und Nichtdiskriminierung, Privatsphäre und Datenschutz sowie die Unschuldsvermutung. Sie können außerdem zu ungerechtfertigten Eingriffen in weitere Rechte führen, etwa das Recht auf Arbeit, Freiheit (etwa durch unrechtmäßige Inhaftierung), ein faires Verfahren, soziale Absicherung oder Gesundheit. Angesichts des besonders hohen Diskriminierungsrisikos in diesem Kontext sollte die automatisierte Profilerstellung von Personen verboten werden.

- Technologien zur individuelle Risikobewertung durch die Verarbeitung oder Ableitung sensibler persönlicher Merkmale oder Ersatzmerkmale wie Rassifizierung, politische Zugehörigkeit, Weltanschauung, genetische, gesundheitliche und biometrische Daten: Dazu gehört die Verwendung von Daten über Staatsangehörigkeit, „Migrationsgeschichte" und Nationalität. Weitere Beispiele hierfür sind die Verwendung von Daten über die Postleitzahl einer Person, um Rückschlüsse auf ihren sozioökonomischen Status zu ziehen. Auch die Verwendung von Daten über Ernährungsgewohnheiten als Ersatz für religiöse Überzeugungen oder den Gesundheitszustand sollten verboten werden.

- Vorausschauende Technologien, die Vorhersagen darüber treffen, wo das Risiko einer „irregulären Migration" besteht: Diese Systeme können verwendet werden, um präventive Maßnahmen zu erleichtern, die darauf abzielen, Bewegungen zu verbieten oder zu stoppen. Häufig werden diese Maßnahmen von EU-Drittländern durchgeführt, die als „Torwächter Europas" fungieren. Vorausschauende Technologien bergen die Gefahr, zu strafenden und missbräuchlichen Grenzkontrollmaßnahmen beizutragen, wenn sie sich auf rassistische Vorurteile und Stereotypen stützen. So hindern sie Menschen daran, Asyl zu beantragen, setzen sie dem Risiko der Zurückweisung aus und beschneiden das Recht auf Leben, Freiheit und Sicherheit.

- KI-basierte Anwendungen zur Emotionserkennung, wie KI-„Lügendetektoren“ und Verhaltensanalysen: Systeme wie KI-„Lügendetektoren“ sind pseudowissenschaftliche Technologien, die behaupten, Emotionen anhand biometrischer Daten ableiten zu können. Verhaltensanalysen dienen dazu, „verdächtige“ Personen anhand ihres Aussehens oder anderer nicht relevanter persönlicher Merkmale zu erkennen. Ihr Einsatz verstärkt rassistische Vorurteile gegenüber Migrant:innen und Asylsuchenden und kann diskriminierende Annahmen aufgrund rassistischer und religiöser Vorurteile automatisieren. Dadurch wird das Recht auf Nichtdiskriminierung, Privatsphäre, Freiheit und ein faires Verfahren bedroht.[6] Die angebliche Nützlichkeit dieser Technologien wird auch durch ableistische Vorstellungen von körperlicher, kognitiver und verhaltensbezogener „Normalität“ untermauert, mit dem Ziel, Behinderungen und Neurodiversität zu „korrigieren“, zu „heilen“ und zu beseitigen.

- Nachträgliche biometrische Fernidentifizierung (Remote Biometric Identification) zusätzlich zu Echtzeit-Massenüberwachung, wie beispielsweise die Verwendung von Gesichtserkennung: Diese Technologien erleichtern die massenhafte und diskriminierende Überwachung in allen Kontexten, einschließlich der Migrations- und Grenzverwaltung. Sie können zur Überwachung von Grenzgebieten als Abschreckungsmaßnahme und als Teil eines umfassenderen Sanktionsregimes eingesetzt werden. Flüchtende werden so daran gehindert, Asyl zu beantragen und Staaten untergraben ihre internationalen Schutzverpflichtungen, insbesondere die Verpflichtung zur Nichtzurückweisung (Non-Refoulement).

- Praxis der massenhaften Erhebung, Verarbeitung, Zusammenführung und Nutzung personenbezogener Daten, einschließlich des Austauschs der erhobenen Daten zwischen Migrations-, Sozial-, Polizei- und nationalen Sicherheitsbehörden. Diese Praxis untergräbt etablierte Datenschutzgrundsätze sowie das Recht auf Privatsphäre. Der Austausch personenbezogener Daten mit Drittländern über supranationale Strafverfolgungsbehörden unter dem Deckmantel der nationalen Sicherheit sollte ebenfalls verboten werden, wenn er weder notwendig noch verhältnismäßig ist oder wenn die Gefahr von Menschenrechtsverletzungen besteht.

Vor dem Einsatz

Zusätzlich zu klaren Verboten von solchen Technologien, die mit den Menschenrechten unvereinbar sind**,** sollten Staaten **vor dem Einsatz eines Technologiesystems Folgendes tun:**

- Verzichten Sie auf die Verabschiedung von Gesetzen, die digitale (und nicht-digitale) Diskriminierung begünstigen und bestehende Systeme der Unterdrückung und Marginalisierung verstärken.

- Beurteilen und weisen Sie die Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit jeder neuen digitalen Technologie sowie deren Wert und Auswirkungen nach. Jede eingesetzte Technologie muss im Einklang sein mit

[6] Erklärung der Zivilgesellschaft (2022). Das KI-Gesetz muss alle Menschen schützen, unabhängig von ihrem Migrationsstatus. https://edri.org/wp-content/uploads/2022/12/Joint-Statement_The-EU-AI-Act-must-protect-people-on-the-move_December-2022.docx.pdf

- dem internationalen Menschenrechtsrahmen und Prinzipien, einschließlich des Diskriminierungsverbots

- Datenschutzstandards, einschließlich der Grundsätze der Rechtmäßigkeit, Fairness und Transparenz, Zweckbindung, Datenminimierung, Genauigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit (Sicherheit) sowie Rechenschaftspflicht.[7]

- Schaffen Sie für verbindliche und durchsetzbare Governance-Rahmen, die die Entwicklung und den Einsatz digitaler Technologien regulieren und dabei die Rechte aller Menschen, einschließlich Migrant:innen, Geflüchteter und Asylsuchender, schützen und fördern. Diese rechtlichen Rahmenwerke müssen ausdrücklich frei von pauschalen Ausnahmeregelungen für Zwecke der nationalen Sicherheit oder vergleichbare Begründungen sein. Solche Ausnahmen sind weder notwendig noch verhältnismäßig und führen häufig zu diskriminierenden Auswirkungen.

- Verabschieden passen Sie bestehende Normen, Richtlinien und Gesetze an, um sicherzustellen, dass der Einsatz automatisierter Entscheidungssysteme im Bereich Asyl, Migration und ähnlichen Bereichen keine Diskriminierung aufgrund von Einkommen, ethnischer Zugehörigkeit, Religion, Migrationsstatus oder anderen persönlichen Merkmalen verstärkt oder beibehält. Diese Normen und Gesetze stellen sicher, dass die Systeme vollständig im Einklang mit den einschlägigen internationalen Menschenrechtsstandards stehen.

- Erlegen Sie allen öffentlichen Einrichtungen, einschließlich Sicherheits-, Strafverfolgungs-, Migrations- und Grenzbehörden, strenge Rechenschafts- und Transparenzpflichten beim Einsatz digitaler Technologien auf. Diese Verpflichtungen umfassen:

    - Einrichtung einer öffentlich zugänglichen Datenbank, die Informationen über die produktiven Systeme offenlegt, wo und wie die Technologie eingesetzt wird und ggf. über die Zusammenarbeit mit privaten Technologieentwickler:innen.

    - Auf Grundlage der Verpflichtung zur Gleichberechtigung und Verhinderung rassistischer Diskriminierung müssen offizielle, nach relevanten Merkmalen zerlegte Daten zu möglichen diskriminierenden Auswirkungen erhoben und offengelegt werden.

    - Einführung eines verbindlichen Prozesses zur Menschenrechtsverträglichkeitsprüfung. Neben der menschenrechtlichen Folgenabschätzung hilft eine Datenschutz-Folgenabschätzung die potenziellen Risiken, insbesondere diskriminierende Auswirkungen, frühzeitig zu identifizieren und minimieren. Die Durchführung dieser Bewertungen sollte mit ausreichenden personellen und finanziellen Ressourcen sowie menschenrechtlicher Expertise erfolgen. Sie sollten aufgeschlüsselte Daten (z. B. zu Herkunft, Geschlecht, Behinderung) enthalten und unter Einbeziehung relevanter Stakeholder stattfinden,

[7] Irischer Datenschutz Beafutragte. Principles of Data Protection. https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection

insbesondere jener, die von den Technologien betroffen sind. Die Ergebnisse und Analysen sollten öffentlich zugänglich gemacht werden, um Transparenz zu gewährleisten. Ihre Ergebnisse und die Umsetzung der Empfehlungen sollten durch eine unabhängige, öffentlich legitimierte Stelle kontrolliert werden, die über ein Mandat zur Durchsetzung digitaler Governance-Vorgaben verfügt. Die Bewertungen sollten kontinuierlich, vor Einführung und während des gesamten Lebenszyklus der Technologien, durchgeführt werden. Jedes identifizierte menschenrechtliche Risiko muss vor der Erlaubnis zum Einsatz abgemildert und verhindert werden. Besondere Aufmerksamkeit gilt dabei intersektionalen Diskriminierungen gegenüber Geflüchteten, Migrant:innen, rassifizierten Gruppen, Menschen in Armut, älteren Menschen, Menschen mit Behinderungen sowie Kindern und Jugendlichen. Können Risiken nicht wirksam abgewendet werden können, sollte der Einsatz der betreffenden Technologie unterbunden werden.

- Bewerten und bekämpfen Sie die Umweltauswirkungen in der Entwicklung und während des Einsatzes. Technologien sind in hohem Maße auf fossile Brennstoffe angewiesen, üben erheblichen Druck auf natürliche Ressourcen wie Land und Wasser aus und verschärfen den Klimawandel und die Umweltzerstörung.[8]

- Verabschieden Sie verbindliche Sorgfaltspflichten, die Unternehmen, die an der Entwicklung und Bereitstellung von Technologien im Zusammenhang mit Asyl, Migration und Grenzkontrollen beteiligt sind, einschließlich Big Data, KI und biometrischen Systemen. Dies hilft dabei, die Einhaltung der Menschenrechte gemäß internationalen Standards wie den UN-Leitprinzipien für Wirtschaft und Menschenrechte und den OECD-Leitfaden für die Erfüllung der Sorgfaltspflicht für verantwortungsvolles unternehmerisches Handeln zu erfüllen.

- Wählen Sie, wo immer möglich, Alternativen, die die Grundrechte am wenigsten einschränken. Das Recht auf Privatsphäre, Gleichbehandlung, Schutz vor Überwachung und andere menschenrechtliche Standards sollten vor Eingriffen der Technologie geschützt werden.

- Beteiligen Sie betroffene Communities, zivilgesellschaftliche Organisationen und Menschenrechtsexpert:innen aktiv in Entwicklung, Einsatz und Kontrolle von KI-Systemen. Das bedeutet auch, dass sie an der Umsetzung, Beobachtung und Evaluierung von KI-Vorschriften eingebunden werden.

- Schaffen Sie zur Stärkung öffentlicher Rechenschaftspflicht von KI-Entwickler:innen und -Anwender:innen wirksame Schutzmechanismen für Whistleblower.

[8] Eine Erklärung der Zivilgesellschaft (2025). Innerhalb der Grenzen: Begrenzung der Umweltauswirkungen von KI. https://greenscreen.network/en/blog/within-bounds-limiting-ai-environmental-impact/#:~:text=KI-Technologien%20dürfen%20nicht%20als%20Energiequelle%20für%20neue%20Rechenzentren%20genutzt%20werden.

Während der Einführung

Während des Lebenszyklus von Technologien sollten Staaten:

- Einzelpersonen die Möglichkeit geben, über die Erhebung, Verarbeitung und Nutzung ihrer personenbezogenen Daten informiert zu werden, der Nutzung freiwillig zuzustimmen oder diese Zustimmung zu widerrufen. Dies umfasst auch das Recht, Maßnahmen zur Datenerhebung anzufechten. Dies sollte durch den Zugang zu Informationen in einer für sie verständlichen Sprache erfolgen. Außerdem ist es transparent darzulegen, wer die Daten erhebt, welche Daten betroffen sind und zu welchem Zweck sie verwendet werden. Die Einwilligung sollte frei von Zwang, Manipulation oder Einschüchterung erfolgen. Der Widerruf der Zustimmung sowie die Löschung der Daten sollte unkompliziert und ohne Angst vor Nachteilen möglich sein. Dies gilt auch für unbeabsichtigte Datenerhebungen, etwa durch Drohnenaufnahmen, die personenbezogene Informationen erfassen.

- Betreiber:innen von KI-Systemen verpflichten, betroffene Personen darüber zu informieren, wenn Entscheidungen über sie ganz oder teilweise durch KI-Systeme, insbesondere algorithmische Entscheidungsprozesse, unterstützt wurden. Dies sollte mindestens zugängliche und aussagekräftige Informationen darüber umfassen, wie eine KI-Bewertung zustande gekommen ist; wie ihre Daten verarbeitet wurden; inwieweit sie die endgültige Entscheidung eines menschlichen Entscheidungsträgers beeinflusst haben; sowie Hinweise zu ihrem Recht auf Widerspruch, Beschwerde und Wiedergutmachung.

- Bei Verstößen die Entwickler:innen und Betreiber:innen für die von ihnen (mit)verursachten Menschenrechtsverletzungen sowie für die Nichtdurchführung angemessener Sorgfaltspflichten im Bereich Menschenrechte und Datenschutz verantwortlich machen, wobei ggf. Wiedergutmachung gewährleistet werden sollte.

- Sicherstellen, dass Personen, die aufgrund des Missbrauchs von digitalen Technologien Menschenrechtsverletzungen erlitten haben, Zugang zu wirksamen gerichtlichen und außergerichtlichen Rechtsbehelfen haben, ohne befürchten zu müssen, dass dies ihre laufenden Asylanträge oder ihr bestehendes Aufenthalts- oder Einreiserecht gefährdet. Organisationen von öffentlichem Interesse müssen in die Lage versetzt werden, betroffene Personen bei der Einreichung von Klagen zu unterstützen und von sich aus Klagen einzureichen, unter anderem durch den Zugang zu Rechtshilfe.

- Jede diskriminierende Auswirkung oder Folge beseitigen, die sich aus der Nutzung digitaler Technologien ergibt, und Maßnahmen ergreifen, um jede Form von Diskriminierung basierend auf den internationalen Menschenrechten zu verhindern.

Empfehlungen an Unternehmen

Unternehmen, die zu einem beliebigen Zeitpunkt am Lebenszyklus von Technologien beteiligt sind, einschließlich Unternehmen, die Technologien für Asyl, Migration und Grenzkontrolle entwickeln und bereitstellen, sollten:

- Die Menschenrechte überall auf der Welt und in allen Geschäftsbereichen – unter Einhaltung der weltweit anerkannten Leitprinzipien der Vereinten Nationen für Wirtschaft

und Menschenrechte (UNGP) und der OECD-Leitsätze für multinationale Unternehmen zu verantwortungsvollem unternehmerischem Handeln, achten.[9]

- Sorgfaltsprüfungen im Bereich der Menschenrechte, systematische Durchführung von menschenrechtlichen Folgenabschätzung und Datenschutz-Folgenabschätzungen in Übereinstimmung mit internationalen Standards wie dem UNGP und dem OECD-Leitfaden für die Erfüllung der Sorgfaltspflicht für verantwortungsvolles unternehmerisches Handeln durchführen.[10] Diese Bewertungen sollten frühzeitig und kontinuierlich von denjenigen durchgeführt werden, die die Technologien einsetzen, und über ausreichende personelle und finanzielle Ressourcen sowie Fachkenntnisse im Bereich der Menschenrechte verfügen. Sie sollten aufgeschlüsselte Daten zu Rassifizierung, ethnischer Zugehörigkeit, Geschlecht, Alter und anderen Diskriminierungsgründen enthalten und in Absprache mit den relevanten Interessengruppen, einschließlich derjenigen, die von den Technologien betroffen sind, durchgeführt werden. Die Ergebnisse und Analysen dieser Bewertungen sollten aus Gründen der Transparenz veröffentlicht und öffentlich zugänglich gemacht werden. Ihre Ergebnisse und die Umsetzung der Empfehlungen sollten von einer unabhängigen öffentlichen Stelle überwacht werden, die mit der Durchsetzung des geltenden Rahmens für die digitale Governance beauftragt ist. Diese Bewertungen sollten auch während des gesamten Lebenszyklus der Technologien kontinuierlich durchgeführt werden. Jedes festgestellte menschenrechtliche Risiko, einschließlich potenzieller diskriminierender Auswirkungen, müssen gemindert oder verhindert werden, bevor der Einsatz der Technologie genehmigt oder fortgesetzt wird. Besondere Aufmerksamkeit sollte intersektionalen Schäden oder diskriminierenden Auswirkungen auf rassifizierte Gruppen, in Armut lebende Menschen, ältere Menschen, Menschen mit Behinderungen und andere marginalisierte Bevölkerungsgruppen sowie Kinder und Jugendliche gewidmet werden. Wenn festgestellt wird, dass Risiken für die Menschenrechte nicht gemindert werden können, sollte der Einsatz dieser Technologien eingestellt werden.

- Alternative, nicht-invasiven Wege aufdecken und priorisieren, mit denen die ermittelten Bedürfnisse erfüllt werden können, ohne das Recht auf Privatsphäre, Gleichheit und Nichtdiskriminierung, Freiheit von Überwachung und andere Menschenrechte unangemessen zu beeinträchtigen.

- Den Schutz von persönlichen Daten gewährleisten, die andernfalls für rechtsverletzende Zwecke verwendet werden, einschließlich der Grundsätze der Datenminimierung, der Sicherheit aller erhobenen personenbezogenen Daten und aller Geräte, Anwendungen, Netzwerke oder Dienste, die an der Erhebung, Übertragung, Verarbeitung und Speicherung beteiligt sind. Einzelpersonen die Möglichkeit geben, sich über Maßnahmen zur Erhebung,

[9] Büro des Hohen Kommissars der Vereinten Nationen für Menschenrechte (2011). Leitprinzipien für Wirtschaft und Menschenrechte: Umsetzung des Rahmenwerks „Schützen, achten, wiedergutmachen“ der Vereinten Nationen, UN Doc. HR/PUB/11/04. https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf; Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (2023). OECD-Leitsätze für verantwortungsvolles unternehmerisches Handeln. https://doi.org/10.1787/81f92357-en

[10] Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (2018). OECD-Leitsätze für die Sorgfaltspflicht bei verantwortungsvollem unternehmerischem Handeln. https://doi.org/10.1787/15f5f4b3-en

Aggregation, Speicherung und Verwendung ihrer personenbezogenen Daten zu informieren, ihre Zustimmung frei zu erteilen oder zu widerrufen und diese Maßnahmen anzufechten. Dies sollte durch Zugang zu Informationen in einer für sie verständlichen Sprache und durch eine klare Erklärung darüber erfolgen, wer die Daten erhebt, welche Daten erhoben werden und wie sie verwendet werden. Einzelpersonen sollten eine echte Wahlmöglichkeit haben, ohne jegliche Art von Zwang, Einschüchterung oder Manipulation. Es sollte einfach sein, die Einwilligung zu widerrufen und Daten löschen zu lassen, ohne Repressalien befürchten zu müssen. Dies gilt auch für Fälle, in denen Daten unbeabsichtigt erhoben werden, beispielsweise bei Drohnenaufnahmen, die unbeabsichtigt personenbezogene Daten erfassen.

- Geschäftsaktivitäten die Menschenrechtsverletzungen verursachen oder dazu beizutragen, vermeiden und sich mit den Auswirkungen befassen, an denen sie beteiligt sind, einschließlich der Beseitigung tatsächlicher Verstöße. Dabei sollten die Lieferkette und der Lebenszyklus des Produkts oder der Unternehmensaktivität, einschließlich Exporte, berücksichtigt werden. Dies sollte auch Fälle unbeabsichtigter diskriminierender Auswirkungen umfassen, die sich aus der praktischen Nutzung digitaler Technologien ergeben.

- Die negativen Auswirkungen auf die Menschenrechte, die mit ihren Tätigkeiten, Produkten oder Dienstleistungen durch ihre Geschäftsbeziehungen verbunden sind, verhindern oder mindestens vermindern, auch wenn sie nicht zu diesen Auswirkungen beigetragen haben. Nutzen Sie Ihren Einfluss auf diese Geschäftsbeziehungen, um diese Risiken und Auswirkungen zu mindern und zu verhindern.

- Transparenz- und Rechenschaftsmechanismen einführen und Informationen über ihre KI-Technologien offenlegen, einschließlich darüber, wo und wie die Technologie eingesetzt wird/werden soll.

- Davon absehen, Lobbyarbeit bei Regierungen für Zugeständnisse oder Vorteile einzusetzen, wie Änderungen von Gesetzen oder Richtlinien, die negative Auswirkungen auf die Menschenrechte anderer haben können.

- Bei der Entwicklung von Technologien proaktiv mit Community-Organisationen, insbesondere solchen, die marginalisierte Communities und Akteur:innen der Zivilgesellschaft vertreten, zusammenarbeiten und diese sinnvoll konsultieren.

Empfehlungen an internationale Organisationen (einschließlich Organisationen der UN)

- Bewerten und belegen Sie die Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit der Entwicklung oder des Einsatzes neuer Technologien. Jede eingesetzte Technologie muss im Einklang sein mit

    - dem internationalen Menschenrechtsrahmen und -grundsätzen, einschließlich des Diskriminierungsverbots,

- Datenschutzstandards, einschließlich der Grundsätze der Rechtmäßigkeit, Fairness und Transparenz, Zweckbindung, Datenminimierung, Sorgfalt, Speicherbegrenzung, Integrität, Vertraulichkeit (Sicherheit) und Rechenschaftspflicht.[11]

- Adressieren Sie die Risiken der Diskriminierung und anderer Menschenrechtsverletzungen durch digitale Technologien, indem ein Prozess zur Bewertung von Menschenrechtsrisiken eingerichtet und eine menschenrechtliche Folgenabschätzung und Datenschutz-Folgenabschätzungen durchgeführt wird.

    - Diese Bewertungen sollten mit ausreichenden personellen und finanziellen Ressourcen sowie Fachwissen im Bereich Menschenrechte durchgeführt werden und aufgeschlüsselte Daten zu Rassifizierung, ethnischer Zugehörigkeit, Geschlecht und anderen Diskriminierungsgründen enthalten, in Absprache mit den relevanten Interessengruppen, einschließlich derjenigen, die von den Technologien betroffen sind.

    - Die Ergebnisse und Analysen dieser Bewertungen sollten aus Gründen der Transparenz veröffentlicht und öffentlich zugänglich gemacht werden.

    - Ihre Ergebnisse und die Umsetzung der Empfehlungen sollten von einer unabhängigen öffentlichen Stelle überwacht werden, die mit der Durchsetzung des geltenden Rahmens für die digitale Governance beauftragt ist.

    - Diese Bewertungen sollten sowohl vor dem Einsatz als auch kontinuierlich während des gesamten Lebenszyklus der Technologien durchgeführt werden.

    - Alle identifizierten Risiken für die Menschenrechte müssen gemindert und verhindert werden, bevor der Einsatz der Technologie genehmigt wird. Wenn festgestellt wird, dass Risiken für die Menschenrechte nicht gemindert werden können, sollte der Einsatz dieser Technologien eingestellt werden.

    - Besondere Aufmerksamkeit sollten intersektionale Schäden oder diskriminierenden Auswirkungen auf rassifizierte Menschen und Communities, Geflüchtete und Migrant:innen, Menschen, die in Armut leben, ältere Menschen, Menschen mit Behinderungen und andere marginalisierte Bevölkerungsgruppen sowie Kinder und Jugendliche gewidmet werden.

- Prüfen und priorisieren Sie alternative, nicht-invasive Wege, mit denen die ermittelten Bedürfnisse erfüllt werden können, ohne das Recht auf Privatsphäre, Gleichheit und Nichtdiskriminierung, Freiheit von Überwachung und andere Menschenrechte unangemessen zu beeinträchtigen.

- Schützen Sie die Daten von Personen davor, für rechtsverletzende Zwecke verwendet zu werden, einschließlich der Gewährleistung der Grundsätze der Datenminimierung, der Sicherheit aller erhobenen personenbezogenen Daten und aller Geräte, Anwendungen,

[11] Die Datenschutzkommission. Grundsätze des Datenschutzes. https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection

Netzwerke oder Dienste, die an der Erhebung, Übertragung, Verarbeitung und Speicherung beteiligt sind.

- Geben Sie Einzelpersonen die Möglichkeit, sich über Maßnahmen zur Erhebung, Aggregation, Speicherung und Verwendung ihrer personenbezogenen Daten, einschließlich biometrischer Daten, zu informieren, ihre Zustimmung frei zu erteilen oder zu widerrufen und diese Maßnahmen anzufechten. Dies sollte durch Zugang zu Informationen in einer für sie verständlichen Sprache und durch eine klare Erklärung darüber erfolgen, wer die Daten erhebt, welche Daten erhoben werden und wie sie verwendet werden. Einzelpersonen sollte eine echte Wahlmöglichkeit gegeben werden, ohne jegliche Art von Zwang, Manipulation oder Einschüchterung. Es sollte einfach sein, die Einwilligung zu widerrufen und Daten löschen zu lassen, ohne Angst vor Repressalien wie der Verweigerung von Rechten oder Dienstleistungen haben zu müssen. Dies gilt auch, wenn Daten unbeabsichtigt erhoben werden.

- Informieren Sie Personen, wenn Entscheidungen, die sie betreffen, durch KI-Systeme getroffen werden, einschließlich algorithmischer Entscheidungsfindung. Dazu sollten mindestens aussagekräftige und zugängliche Informationen darüber gehören, wie eine KI-Bewertung zustande gekommen ist, wie ihre Daten verarbeitet wurden, inwieweit sie die endgültige Entscheidung eine:r menschlichen Entscheidungsträger:in beeinflusst haben, sowie Informationen über ihr Recht auf Einspruch, Wiedergutmachung und Rechtsbehelf und über bestehende Mechanismen zur Durchsetzung dieser Rechte.

- Stellen Sie sicher, dass Personen, die aufgrund des Missbrauchs von Technologien Menschenrechtsverletzungen erlitten haben, Zugang zu wirksamen Rechtsbehelfen haben.

- Integrieren Sie explizite und spezifische Schutzmaßnahmen gegen den Missbrauch von Technologien, einschließlich des Datenaustauschs mit nationalen Sicherheitsbehörden oder Herkunftsländern, der zu Menschenrechtsverletzungen führen könnte.

- Stellen Sie sicher, dass betroffene Gemeinschaften sich sinnvoll an der Entwicklung und dem Einsatz von KI-Technologien sowie an deren Umsetzung, Überwachung und Bewertung beteiligen können.

- Handeln Sie im Einklang mit den einschlägigen Menschenrechtsverpflichtungen und stellen Sie sicher, dass jegliche Unterstützung, einschließlich Finanzierungs- und technischer Hilfsprogramme, nicht zur Verbreitung von Technologien führt, die die Rechte von Migrant:innen, Geflüchteten und Asylbewerber:innen verletzen.

Empfehlungen für andere Dienstleister

An Dienstleister, die digitale Technologien in den Bereichen Asyl, Migration, Grenzsicherung und humanitäre Hilfe einsetzen, einschließlich Nichtregierungsorganisationen (NGOs) und humanitären gemeinnützigen Dienstleistern:

- Achten Sie die Menschenrechte überall auf der Welt und bei allen ihren Tätigkeiten, einschließlich der Einhaltung der weltweit anerkannten Leitprinzipien der UNGP, der

OECD-Leitsätze für multinationale Unternehmen zu verantwortungsvollem unternehmerischem Handeln[12] und der Sphere-Standards.[13]

- Gehen Sie die Risiken durch digitale Technologien an, die Diskriminierung und andere Menschenrechtsverletzungen gegen Personen begünstigen, u.a. durch die Durchführung von Menschenrechtsverträglichkeitsprüfungen mit besonderem Augenmerk auf die intersektionalen Auswirkungen auf rassifizierte Menschen und Communities, Geflüchtete und Migrant:innen, Menschen, die in Armut leben, ältere Menschen, Menschen mit Behinderungen und andere marginalisierte Bevölkerungsgruppen sowie Kinder und Jugendliche.

- Prüfen und priorisieren Sie alternative, nicht-invasive Wege, die den ermittelten Bedürfnissen gerecht werden, ohne das Recht auf Privatsphäre, Gleichheit und Nichtdiskriminierung, Freiheit von Überwachung und andere Menschenrechtsverletzungen unangemessen zu beeinträchtigen.

- Schützen Sie die Daten von Personen davor, für rechtsverletzende Zwecke verwendet zu werden, einschließlich der Gewährleistung der Grundsätze der Datenminimierung, der Sicherheit aller erhobenen personenbezogenen Daten und aller Geräte, Anwendungen, Netzwerke oder Dienste, die an der Erhebung, Übertragung, Verarbeitung und Speicherung beteiligt sind. Geben Sie Einzelpersonen die Möglichkeit, sich über Maßnahmen zur Erhebung, Aggregation, Speicherung und Verwendung ihrer personenbezogenen Daten, einschließlich biometrischer Daten, zu informieren, ihre Zustimmung frei zu erteilen oder zu widerrufen und diese Maßnahmen anzufechten. Dies sollte durch Zugang zu Informationen in einer für sie verständlichen Sprache und durch eine klare Erklärung darüber erfolgen, wer die Daten erhebt, welche Daten erhoben werden und wie sie verwendet werden. Einzelpersonen sollten eine echte Wahlmöglichkeit haben, ohne jegliche Art von Zwang, Manipulation oder Einschüchterung. Es sollte einfach sein, die Einwilligung zu widerrufen und Daten löschen zu lassen, ohne Repressalien wie die Verweigerung des Zugangs zu Rechten oder Dienstleistungen befürchten zu müssen.

- Integrieren Sie explizite und spezifische Schutzmaßnahmen gegen den Missbrauch von Technologien, einschließlich der Weitergabe von Daten an nationale Sicherheitsbehörden oder Herkunftsländer, die zu Menschenrechtsverletzungen führen könnte.

[12] Büro des Hohen Kommissars der Vereinten Nationen für Menschenrechte (2011). Leitprinzipien für Wirtschaft und Menschenrechte: Umsetzung des Rahmenwerks „Schützen, achten, wiedergutmachen“ der Vereinten Nationen, UN Doc. HR/PUB/11/04. https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf; Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (2023). OECD-Leitsätze für verantwortungsvolles unternehmerisches Handeln. https://doi.org/10.1787/81f92357-en

[13] Sphere. Humanitäre Standards. https://www.spherestandards.org/humanitarian-standards/

Glossar A-Z

Algorithmische Entscheidungsfindung (ADM)	Ein algorithmisches System, das in verschiedenen Schritten (zur Unterstützung) von Entscheidungsprozessen eingesetzt wird.
Automatisierte Entscheidungsfindung	Ein algorithmisches Entscheidungsfindungssystem *ohne* menschliche Beteiligung. Die Entscheidung wird ausschließlich durch das System getroffen.
Betreiber:innen	Diejenigen, die ein KI-System unter ihrer Aufsicht verwenden. Dabei kann es sich um privatwirtschaftliche und öffentliche Akteur:innen handeln. Ein einzelnes Unternehmen oder eine Behörde kann dabei gleichzeitig Entwickler:in und Betreiber:in sein, wenn sie über interne Kapazitäten verfügt, um KI-Tools selbst zu entwickeln.
Biometrische Fernidentifizierung (RBI)	Wird verwendet, um Personen aus der Ferne zu identifizieren, indem ihre individuellen biometrischen Merkmale mit einer Datenbank abgeglichen werden. RBI kann in Echtzeit erfolgen, dabei werden die gesammelten Informationen sofort oder nahezu sofort verarbeitet, oder rückwirkend, wobei die Analyse der aufgenommenen Bilder zu einem späteren Zeitpunkt erfolgt. Die Gesichtserkennungstechnologie ist das bekannteste Beispiel für RBI-Technologie, s. „Gesichtserkennungstechnologie“, und wird manchmal synonym mit RBI verwendet.
Biometrische (Überwachungs-)Technologien	Werden zur Identifizierung menschlicher Körpermerkmale von Personen anhand biologischer individueller Merkmale wie Fingerabdrücke, Netzhaut und Iris, Stimmmuster, Gangart, Gesichtsmerkmale und Handmaße eingesetzt. Dazu gehören bspw. Technologien, die Personen anhand biometrischer Merkmale kategorisieren, Gesichtserkennungstechnologien zur Identifizierung von Personen und sogenannte Emotionserkennungstechnologien.
Entwickler:innen	Vorwiegend Unternehmen und internationale Organisationen, die Ressourcen in die

	Entwicklung von KI-Tools investieren, um diese Tools anderen zur Nutzung zur Verfügung zu stellen oder selbst einzusetzen.
Gesichtserkennungstechnologie (FRT)	Oberbegriff, der verwendet wird, um eine Reihe von Anwendungen zu beschreiben, die eine bestimmte Aufgabe unter Verwendung eines menschlichen Gesichts zur Überprüfung oder Identifizierung einer Person ausführen. FRT ist eine von zahlreichen biometrischen Technologien, die von Staaten und kommerziellen Einrichtungen in einer Vielzahl von Anwendungsfällen eingesetzt werden.
Globale Mehrheit	Begriff, der sich auf Menschen bezieht, die aufgrund ihrer ethnischen Zugehörigkeit diskriminiert werden, wie indigene Gruppen, Menschen afrikanischer, asiatischer oder südamerikanischer Herkunft, die zusammen den größten Teil der Weltbevölkerung ausmachen. Der Begriff wird verwendet, um Begriffe wie „Minderheiten" in Frage zu stellen, die oft als marginalisierend angesehen werden. Auch soll durch den Begriff die kollektive Handlungsfähigkeit und Solidarität zwischen Menschen bekräftigt werden, die institutionellem Rassismus und historischen rassistischen Ungerechtigkeiten ausgesetzt sind.[14]
Intersektionalität	Kategorie zur Untersuchung, wie sich verschiedene Diskriminierungsformen überschneiden und einander verstärken. Erklärt, wie erfahrene Diskriminierung einer Person aufgrund ihrer Zugehörigkeit zu einer bestimmten sozialen Gruppe, Geschlecht, sexuellen Orientierung, Rassifizierung, Klasse, Kaste, Behinderung, Migrationsstatus, Religion, ethnischen Zugehörigkeit, indigenen Identität, Alters oder aus anderen Gründen mit einer weiteren Diskriminierungsform zusammenwirken. Dadurch geht es über die Anerkennung hinaus, dass verschiedene Formen der Unterdrückung

[14] Siehe Campbell-Stephens, R.M. (2020). Globale Mehrheit: Wir müssen über Bezeichnungen wie „BAME" sprechen. https://www.linkedin.com/pulse/global-majority-we-need-talk-labels-bame-campbell-stephens-mbe/; Campbell-Stephens, R.M. (2021). Einleitung: Globale Mehrheit – Dekolonisierung von Narrativen. In: Bildungsführung und die globale Mehrheit. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-88282-2_1

	existieren, und untersucht stattdessen, wie sie zusammen ein bestimmtes Muster der Diskriminierung schaffen. Wenn bspw. ein Schwarzer oder muslimischer Asylsuchender mit höherer Wahrscheinlichkeit inhaftiert wird, weil er migriert ist, sind die Diskriminierung und die Verletzung seiner Menschenrechte auf eine Kombination aus Rassifizierung, nationalen Herkunft, Migrationsgeschichte und Staatsbürgerschaft zurückzuführen.
Künstliche Intelligenz (KI)	Jede Technik oder jedes System, das es Computern ermöglicht, menschliches Verhalten nachzuahmen. Die Definition von KI ist umstritten, kann aber allgemein als „ein maschinelles System, das für explizite oder implizite Ziele aus den erhaltenen Eingaben ableitet, wie es Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen generieren kann, die physische oder virtuelle Umgebungen beeinflussen können [verstanden werden]. Verschiedene KI-Systeme unterscheiden sich in ihrem Grad an Autonomie und Anpassungsfähigkeit nach ihrer Einführung.“[15]
Menschenrechtsverträglichkeitsprüfung	Ein Verfahren zur Bewertung der Auswirkungen auf die Menschenrechte, einschließlich der Identifizierung von Risiken während des gesamten Lebenszyklus einer KI. Sollte eine Bewertung der Angemessenheit des KI-basierten Systems in einem bestimmten Szenario beinhalten. Dazu gehört die Herausarbeitung der betroffenen Gruppen, der zu erwartenden Folgen, Konsultation der betroffenen Communities und einer Einschätzung, wie Schäden gemindert werden können.
Non-Refoulement-Verpflichtung	Rechtliche Verpflichtung von Staaten, niemanden an einen Ort oder in eine Gerichtsbarkeit zurückzuschicken oder zu überstellen, wo er/sie* einem realen Risiko der Verfolgung oder anderer schwerwiegender Menschenrechtsverletzungen oder -verstöße ausgesetzt wäre.

[15] Siehe Übersicht über die KI-Grundsätze der OECD. https://oecd.ai/en/ai-principles

Profiling	Die automatisierte Verarbeitung personenbezogener Daten zur Bewertung persönlicher Aspekte einer Person, wie z. B. ihrer Arbeitsleistung, ihrer wirtschaftlichen Situation, ihrer Gesundheit, ihrer persönlichen Vorlieben oder Interessen, ihres Verhaltens, ihres Aufenthaltsorts oder ihrer Bewegungen.[16]
Rassistische Diskriminierung	Das Internationale Übereinkommen zur Beseitigung jeder Form von Rassismus (ICERD) definiert Rassismus als „jede Unterscheidung, Ausgrenzung, Beschränkung oder Bevorzugung aufgrund der Rassifizierung, der Hautfarbe, der Abstammung oder der nationalen oder ethnischen Herkunft, die zum Ziel oder zur Folge hat, dass die Anerkennung, Inanspruchnahme oder Ausübung der Menschenrechte und Grundfreiheiten im politischen, wirtschaftlichen, sozialen, kulturellen oder jedem anderen Bereich des öffentlichen Lebens auf der Grundlage der Gleichberechtigung vereitelt oder beeinträchtigt wird“.[17]
Risikobewertungsinstrumente	Die halb- oder vollautomatische Verarbeitung von Daten für statistische Bewertungen und/oder Vorhersagemodelle, um das Risiko zu ermitteln, dass ein unerwünschtes Ergebnis eintritt, entweder auf individueller oder gemeinschaftlicher Ebene oder spezifisch für ein Ereignis.
Social Scoring	Die Verwendung von KI und anderer Formen der algorithmischen Entscheidungsfindung zur Bewertung und Klassifizierung von Personen, um bestimmte Einschätzungen oder Entscheidungen über sie zu treffen. Dieses Bewertungs- und Klassifizierungssystem ist in der Regel prädiktiv – es kann beispielsweise so programmiert sein, dass es die Wahrscheinlichkeit ableitet, mit der ein:e Arbeitssuchende:r eine Stelle findet, oder

[16] Siehe Artikel 4.4, Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[17] Artikel 1, Vereinte Nationen (1965). Internationales Übereinkommen zur Beseitigung jeder Form von Rassendiskriminierung. [online] OHCHR. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial

	wie wahrscheinlich es ist, dass ein:e Kund:in einen Kredit zurückzahlt. Social Scoring stützt sich auf vielfältige Informationen wie die Identität der Person (z. B. Alter, Geschlecht, Rassifizierung und ethnische Zugehörigkeit), ihr bisheriges Verhalten (z. B. beruflichen Werdegang oder Vorstrafen) oder ihre sozioökonomische Situation (z. B. Einkommen und Bildungsniveau).[18]
Struktureller Rassismus	Der beratende Ausschuss des Menschenrechtsrats der UN weist darauf hin, dass Rassismus eine systemische Diskriminierungsform ist, die „durch ein miteinander verbundenes oder eng koordiniertes Netzwerk von Gesetzen, Richtlinien, Praktiken, Einstellungen, Stereotypen und Vorurteilen wirkt. Es wird von einer Vielzahl von Akteur:innen aufrechterhalten, darunter staatliche Institutionen, der Privatsektor und gesellschaftliche Strukturen im weiteren Sinne. Rassismus führt nicht nur zu ausdrücklicher, direkter, *de jure* oder absichtlicher Diskriminierung, sondern auch zu verdeckter, indirekter, *de facto* oder unbeabsichtigter Diskriminierung, Unterscheidung, Ausgrenzung, Einschränkung oder Bevorzugung aufgrund von race, Hautfarbe, Abstammung, nationaler oder ethnischer Herkunft. Rassismus hat seine historischen Wurzeln in der Versklavung, des Handels mit versklavten Afrikaner:innen und generell im Kolonialismus. Außerdem neigt Rassismus dazu, Lebensrealitäten über Generationen hinweg zu steuern.“[19]

Kontakt

Bei Fragen, Anliegen und Rückmeldungen, auch zur Barrierefreiheit des Dokuments oder Übersetzungen, wenden Sie sich gerne an charlotte.phillips@amnesty.org oder mher.hakobyan@amnesty.org.

[18] Adaptiert aus Human Rights Watch, Q&A: Wie die mangelhafte Regulierung der künstlichen Intelligenz durch die EU das soziale Sicherheitsnetz gefährdet. https://www.hrw.org/sites/default/files/media_2021/11/202111hrw_eu_ai_regulation_qa_0.pdf

[19] Beratender Ausschuss des Menschenrechtsrats (8. August 2023). Förderung von Rassengerechtigkeit und Gleichheit durch die Beseitigung von systemischem Rassismus, UN Doc. A/HRC/54/70, Abs. 7. https://documents.un.org/doc/undoc/gen/g23/140/55/pdf/g2314055.pdf?OpenElement

Quellen

- Amnesty International, Primer on Defending the Rights of Refugees and Migrants in the Digital Age, Februar 2024, AI Index: POL 40/7654/2024.https://www.amnesty.org/en/documents/pol40/7654/2024/en/
- Amnesty International, Brief: Die EU muss die Menschenrechte von Migranten im KI-Gesetz achten, April 2023, Die EU muss die Menschenrechte von Migranten im KI-Gesetz achten – Büro für europäische Institutionen. https://www.amnesty.eu/news/the-eu-must-respect-human-rights-of-migrants-in-the-ai-act/
- Amnesty International, Verwirklichung des Rechts auf soziale Sicherheit: Vorlage beim Büro des Hohen Kommissars der Vereinten Nationen für Menschenrechte, 2024, AI-Index: IOR 40/7558/2024. https://www.amnesty.org/en/documents/ior40/7558/2024/en/
- Amnesty International, Dänemark: Codierte Ungerechtigkeit: Überwachung und Diskriminierung im automatisierten Sozialstaat Dänemarks, 2004, AI-Index: EUR 18/8709/2024. https://www.amnesty.org/en/latest/news/2024/11/denmark-ai-powered-welfare-system-fuels-mass-surveillance-and-risks-discriminating-against-marginalized-groups-report/#:~:text=The%20Danish%20welfare%20authority%2C%20Udbetaling%20Danmark%20%28UDK%29%2C%20risks,Amnesty%20International%20said%20today%20in%20a%20new%20report.
- Amnesty International, Die digitale Grenze: Migration, Technologie und Ungleichheit, 21. Mai 2024, Indexnummer: POL 40/7772/2024. https://www.amnesty.org/en/documents/pol40/7772/2024/en/
- Amnesty International, USA/Global: Von Palantir und Babel Street entwickelte Technologien stellen eine Überwachungsgefahr für pro-palästinensische studentische Demonstranten und Migranten dar, August 2025. https://www.amnesty.org/en/latest/news/2025/08/usa-global-tech-made-by-palantir-and-babel-street-pose-surveillance-threats-to-pro-palestine-student-protestors-migrants/
- Dänemark: Leicht lesbare Fassung: Codierte Ungerechtigkeit: Überwachung und Diskriminierung im automatisierten Sozialstaat Dänemarks, 21. Mai 2025, Indexnummer: EUR 18/9419/2025. https://www.amnesty.org/en/documents/eur18/9419/2025/en/
- Koalition #Protect Not Surveil, der Amnesty angehört, siehe Website: EU AI | Protect Not Surveil. https://protectnotsurveil.eu/
- Koalition #ProtectNotSuveil, Gemeinsame Erklärung, Ein gefährlicher Präzedenzfall: Wie das EU-KI-Gesetz Migranten und Menschen auf der Flucht im Stich lässt, 13. März 2024. https://www.accessnow.org/press-release/joint-statement-ai-act-fails-migrants-and-people-on-the-move/
- #ProtectNotSuveil, Gemeinsame Erklärung, Der EU-Migrationspakt: ein gefährliches System der Überwachung von Migranten, 10. April 2024. https://www.accessnow.org/press-release/joint-statement-eu-migration-pact-a-dangerous-regime-of-migrant-surveillance/