



# Künstliche Intelligenz und Menschenhandel: Chancen und Risiken

## Einleitung

Die rasante Verbreitung Künstlicher Intelligenz (KI) verändert, wie Menschen denken, arbeiten, kommunizieren und sich informieren.

Bereits in einer 2022 erschienenen [Studie](#) zum Einfluss von Informations- und Kommunikationstechnologien (IKT) auf den Menschenhandel in Deutschland stellte der KOK fest, dass technologischer Fortschritt und Digitalisierung auch von Menschenhändler\*innen genutzt werden. Sie ermöglichen eine größere Reichweite, ortsunabhängiges Handeln und ein geringeres Entdeckungsrisiko. IKT kommen dabei in allen Phasen des Ausbeutungsprozesses zum Einsatz, insbesondere bei der Anwerbung potenzieller Betroffener über soziale Netzwerke sowie zur Kontrolle und Druckausübung während und nach der Ausbeutung. KI verschärft diese Dynamiken zusätzlich. Gleichzeitig kann KI Ermittlungen unterstützen, Täter\*innen zu identifizieren und kriminelle Netzwerke aufzudecken. Sie kann zur Prävention und zum Schutz von Betroffenen eingesetzt werden und den Zugang zu Hilfsangeboten erleichtern.





## Glossar<sup>1</sup>

### ● KÜNSTLICHE INTELLIGENZ (KI)

Ein Teilgebiet der Informatik, das Systeme entwickelt, die Aufgaben übernehmen, für die normalerweise menschliche Intelligenz und Interaktion nötig sind.

### ● GENERATIVE KI

Ein Teilbereich der KI, die Texte, Bilder, Videos und andere Inhalte generieren kann. Generative KI lernt anhand von Milliarden bis Billionen Textbausteinen typische Muster und erstellt darauf aufbauend neue Inhalte.

### ● LARGE LANGUAGE MODELS (GROSSE SPRACHMODELLE, LLMS)

Generative KI, die sich auf die Erstellung von Text konzentriert. LLMs werden mit sehr großen Textmengen trainiert. „Groß“ bezieht sich auf die Komplexität und die Leistungsfähigkeit des KI-Modells.

### ● CHATBOT

Ein textbasiertes Dialogsystem, das Kommunikation mit technischen Systemen ermöglicht. Nutzer\*innen können in natürlicher Sprache Informationen abrufen oder Transaktionen durchführen.<sup>2</sup>

### ● DEEPPFAKE

Ein mit KI erzeugtes oder manipuliertes Bild, Video oder eine Tonaufnahme. Deepfakes können eine reale oder erfundene Person zeigen. Sie werden häufig eingesetzt, um Täuschungen zu erzeugen, die kaum als solche erkennbar sind. Dies birgt Risiken für die Manipulation der öffentlichen Meinung, die Verletzung von Persönlichkeitsrechten (zum Beispiel durch bildbasierte sexualisierte Gewalt) sowie für gezielte Desinformationskampagnen.<sup>3</sup>

<sup>1</sup> Die folgenden Definitionen stammen, sofern nicht anders angegeben, von der Organisation für Sicherheit und Zusammenarbeit in Europa: Organisation für Sicherheit und Zusammenarbeit in Europa (2024): New frontiers: The use of generative artificial intelligence to facilitate trafficking in persons, <https://www.osce.org/cthb/579715>, abgerufen am 14.04.2026.

<sup>2</sup> Bundesamt für Sicherheit in der Informationstechnik: Exkurs: Social Bots und Chatbots, <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Soziale-Netzwerke/Sichere-Verwendung/Exkurs-bots/social-bots.html>, abgerufen am 14.04.2026.

<sup>3</sup> Bundesamt für Sicherheit in der Informationstechnik: Deepfakes – Gefahren und Gegenmaßnahmen, [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html), abgerufen am 14.04.2026.



## KI als Katalysator: Wie KI-Technologien bestehende Mechanismen des Menschenhandels verstärken

Menschenhandel ist eine schwere Menschenrechtsverletzung. Betroffene werden durch Täuschung, Zwang oder Gewalt in Ausbeutungssituationen gebracht. Oft befinden sie sich in wirtschaftlicher Not oder sie werden mit falschen Versprechungen angeworben.

Digitalisierung und KI verstärken diese Dynamiken. Menschenhändler\*innen nutzen digitale Möglichkeiten, wie günstige, leicht verfügbare und leistungsfähige KI-Werkzeuge, um ihr Vorgehen zu professionalisieren und neue Zielgruppen zu erreichen. Die zunehmende Nutzung von IKT durch Täter\*innen zur Kontaktabnähung mit den Betroffenen wird bereits seit Jahren im Bundeslagebild Menschenhandel des Bundeskriminalamtes beschrieben.

KI-gestützte Übersetzungen und Chatbots ermöglichen Kommunikation in Echtzeit über Sprach- und Kulturgrenzen hinweg. Täter\*innen können so mit wenig Aufwand sehr viele Menschen ansprechen. Nach Einschätzung der Organisation für Sicherheit und Zusammenarbeit in Europa ermöglichen KI-Technologien, sehr große Zahlen potenzieller Betroffener gleichzeitig anzusprechen, zum Beispiel durch automatisiert erstellte personalisierte Nachrichten oder täuschende Online-Profile.<sup>4</sup> So können Täter\*innen etwa über Dating-Apps Personen in anderen Weltregionen kontaktieren, ohne die jeweilige Sprache zu beherrschen. KI-gestützte Sprachtools übernehmen die Kommunikation und lassen den Austausch glaubwürdig erscheinen. Viele dieser Anwendungen sind leicht zugänglich und günstig, sodass auch Personen ohne technische Vorkenntnisse sie nutzen können.

Deepfake-Technologien ermöglichen zudem die Erstellung täuschend echter Texte, Bilder oder Stimmen. So entstehen gefälschte Identitäten, mit denen Täter\*innen über soziale Netzwerke, Jobbörsen oder Dating-Plattformen Kontakt zu potenziellen Betroffenen aufnehmen. Auch die Erstellung nicht einvernehmlicher sexueller Darstellungen zum Zwecke der Nötigung und Kontrolle ist technisch möglich.



**KI ermöglicht Täter\*innen, mit wenig Aufwand große Gruppen von Menschen über Sprach- und Kulturgrenzen hinweg anzusprechen – etwa über Dating-Apps, Jobbörsen oder soziale Netzwerke – und diese mit täuschend echten Identitäten und Inhaltsboten zu manipulieren.**

Ein internationales Beispiel für den Einsatz von KI-Technologien im Kontext von Menschenhandel und Ausbeutung sind sogenannte Cyber-Scam-Zentren in Südostasien.<sup>5</sup> In diesen Zentren werden Personen gezwungen, über Social-Media Betrugsdelikte zu begehen.

KI-Anwendungen werden hier genutzt, um Identitäten zu verschleiern, mehrsprachig zu kommunizieren und Menschen weltweit zu erreichen.

<sup>4</sup> Organisation für Sicherheit und Zusammenarbeit in Europa (2024): New frontiers: The use of generative artificial intelligence to facilitate trafficking in persons, <https://www.osce.org/cthb/579715>, abgerufen am 15.04.2026.

<sup>5</sup> United Nations Office on Drugs and Crime (2023): Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia, [https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP\\_for\\_FC\\_Policy\\_Report.pdf](https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf), abgerufen am 15.04.2026.



## Prävention und Strafverfolgung: Aktuelle KI-Initiativen und Methoden auf nationaler und internationaler Ebene sowie deren Erfolgspotenziale

Die Strafverfolgung steht vor großen Herausforderungen: Online-Aktivitäten von Menschenhändler\*innen nehmen stetig zu und die genutzten Technologien entwickeln sich schnell weiter. Gleichzeitig ist die Überwachung und Nachverfolgung dieser Aktivitäten sehr ressourcenintensiv und unterliegt rechtlichen Grenzen.

Die Täter\*innen in die Verantwortung zu nehmen ist im Zuge der fortschreitenden Digitalisierung deutlich schwieriger geworden. Sie nutzen Pseudonyme, anonymisierende Software wie Virtual Private Network (VPN)-Verbindungen oder verschlüsselte Kommunikationskanäle und passen ihr Verhalten im digitalen Raum schnell an. Die Entwicklung von KI-Tools verstärkt diese Dynamik. Die Tools automatisieren die Erstellung und Anpassung digitaler Identitäten und Kommunikationsmuster und professionalisieren sie so stark, dass echte und synthetische Profile kaum voneinander zu unterscheiden sind.

Gleichzeitig bieten die Technologien auch Chancen: KI-Software kann Chat-Daten nach verdächtigen Mustern durchsuchen<sup>6</sup> und die forensische Auswertung von Smartphones, Computern, Tablets oder Speichergeräten kann wichtige Beweise liefern.<sup>7</sup> Auf diesen Geräten können sich entscheidende Hinweise auf Täter\*innen und Tatabläufe befinden.

In der Praxis gestaltet sich diese Auswertung jedoch oft sehr aufwendig. Die Entschlüsselung von Sicherheitssystemen und Passwörtern kann mehrere Monate dauern.<sup>8</sup> Die Ermittlungsbehörden dürfen nur auf solche privaten Daten zugreifen und sie auswerten, die durch eine gesetzliche Eingriffsbefugnis gedeckt sind und für den konkreten Ermittlungszweck erforderlich sind. Dabei gelten die Vorgaben aus der Datenschutz-Grundverordnung, dem Bundesdatenschutzgesetz und der Strafprozessordnung – insbesondere Zweckbindung, Verhältnismäßigkeit und Datenminimierung.

Häufig fehlen spezialisierte technische Ressourcen und Fachwissen, um KI-basierte Strategien der Täter\*innen zu erkennen und zu verfolgen. Behörden benötigen daher ein tiefes Verständnis KI-basierter Methoden und der eingesetzten Technologien, um effektiv gegen Menschenhandel vorzugehen.<sup>9</sup>

<sup>6</sup> Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2021): Künstliche Intelligenz in der Strafverfolgung, <https://www.bfdi.bund.de/DE/BfDI/Inhalte/Konsultationsverfahren/KI-Strafverfolgung/KI-Strafverfolgung-Bericht.html?>, abgerufen am 15.04.2026.

<sup>7</sup> United Nations Office on Drugs and Crime (2019): Trafficking in Persons & Smuggling of Migrants, <https://www.unodc.org/e4j/en/tip-and-som/module-14/key-issues/use-of-technology-to-facilitate-tip-and-som.html>, abgerufen am 15.04.2026.

<sup>8</sup> Europol (2023): Internet Organised Crime Threat, <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023>, abgerufen am 15.04.2026.

<sup>9</sup> Europol (2023): ChatGPT – The impact of Large Language Models on Law Enforcement, <https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement>, abgerufen am 15.04.2026.



## Nationaler Aktionsplan gegen Menschenhandel setzt auf Digitalisierung und Datenanalyse – Künstliche Intelligenz muss künftig systematisch einbezogen werden

### Was ist der Nationale Aktionsplan gegen Menschenhandel?

Mit dem [Nationalen Aktionsplan zur Prävention und Bekämpfung des Menschenhandels und zum Schutz der Betroffenen](#) (NAP MH) reagiert die Bundesregierung auf die komplexen Herausforderungen des Menschenhandels.

Der NAP MH bündelt Maßnahmen zur Prävention, Bekämpfung und zum Schutz Betroffener. Ziel ist es, Menschenhandel einzudämmen, Unterstützung zu verbessern und die Zusammenarbeit auf Länder- und EU-Ebene zu stärken.

#### DIE THEMENSCHWERPUNKTE DES NAP MH SIND:

1. Prävention
2. Schutz, Unterstützung und Entschädigung für Betroffene
3. Strafverfolgung
4. Kooperation auf nationaler, europäischer und internationaler Ebene

Das dritte Kapitel des NAP MH befasst sich mit dem Thema Digitalisierung. Es enthält einen umfassenden Maßnahmenkatalog, der darauf abzielt, digital gestützte Formen der Ausbeutung – etwa die „Loveboy“-Methode oder Online-Streaming-Ausbeutung – wirksam zu bekämpfen. Vorgesehen sind unter anderem Sensibilisierungskampagnen, eine verstärkte bilaterale Zusammenarbeit mit Drittstaaten sowie der Ausbau digitaler Kompetenzen von Ermittlungsbehörden, um solchen Straftaten präventiv zu begegnen. Auch die Fachberatung soll im Zuge des digitalen Wandels weiterentwickelt werden, um Beratungsangebote auszubauen und Zugänge zu erleichtern.



## Risiken für vulnerable Gruppen durch den Einsatz von KI-Tools am Beispiel von Grenzkontrollen

Der zunehmende Einsatz von KI durch staatliche und private Akteure birgt erhebliche Risiken für Privatsphäre und Menschenrechte. Besonders deutlich wird das an den EU-Außengrenzen, wo Technologien zur Migrationssteuerung immer stärker zum Einsatz kommen. Menschenrechtsorganisationen warnen, dass die rechtlichen Schutzmechanismen hier nicht Schritt halten: Der EU AI Act, das zentrale Regulierungsgesetz der Europäischen Union, schafft nach Ansicht der Organisation European Digital Rights ein Zwei-Klassen-System.<sup>10</sup> Während EU-Bürger\*innen vor biometrischer Überwachung weitgehend geschützt sind, entsteht an den EU-Außengrenzen ein Regulierungsvakuum, das den Einsatz nahezu jeder Technologie erlaubt und dadurch Migrant\*innen nicht ausreichend vor Menschenrechtsverletzungen schützt.<sup>11</sup>

Zwar ordnet der EU AI Act KI-Systeme im Kontext von Migration, Asyl und Grenzschutz grundsätzlich als Hochrisiko-Anwendungen ein und knüpft ihre Nutzung an strenge Anforderungen. Doch gleichzeitig nimmt das Gesetz alle KI-Systeme aus, die für nationale Sicherheitszwecke eingesetzt werden. Da alle Mitgliedstaaten selbst definieren, was unter diesen Begriff fällt, können sie Teile ihres Grenzschutzes auslagern und so der Regulierung entgehen.

Selbst dort, wo der EU AI Act formell greift, bleibt die Kontrolle begrenzt: Hochrisiko-KI-Systeme müssen nicht öffentlich registriert werden, sondern werden in einer internen Datenbank erfasst. Eine unabhängige oder öffentliche Kontrolle ist damit kaum möglich.<sup>12</sup> Darüber hinaus wird davor gewarnt, dass Erstaufnahmeeinrichtungen zu Testfeldern für wissenschaftlich umstrittene Technologien werden. KI-basierte Lügendetektoren oder automatisierte Dialektanalysen werden dort weitgehend unkontrolliert eingesetzt und getestet.<sup>13</sup>

Die Folgen für Schutzsuchende können gravierend sein: Automatisierte Bewertungen verletzen nicht nur das Recht auf Privatsphäre und Datenschutz, sondern gefährden auch das Recht auf ein faires Asylverfahren und Gleichbehandlung.<sup>14</sup>

Hinzu kommt der psychische Druck ständiger Überwachung in den Aufnahmeeinrichtungen. Datengrundlagen und Algorithmen müssen daher transparent, menschenrechtskonform und diskriminierungssensibel entwickelt und kontrolliert werden. Nur so lässt sich verhindern, dass technologische Innovation zulasten der Rechte besonders schutzbedürftiger Gruppen geht.



Was bedeutet das für potenziell Betroffene von Menschenhandel?

Da KI-Systeme oft mit Wahrscheinlichkeiten statt mit individuellen Fakten arbeiten, bestehen für vulnerable Personen hohe Risiken. Eine asylsuchende Person kann aufgrund einer KI-basierten Bewertung oder Empfehlung zu wichtigen Aspekten ihres Asylantrags als „Sicherheitsrisiko“ eingestuft werden. Dadurch steigt das Risiko systematischer Fehlbeurteilungen von Asylgesuchen deutlich an.<sup>15</sup>

Gleichzeitig greifen Schutz- und Unterstützungsangebote unter diesen Bedingungen möglicherweise nicht ausreichend.<sup>16</sup>

<sup>10</sup> European Digital Rights (2023): EU Parliament calls for ban of public facial recognition, but leaves human rights gaps in final position on AI Act, <https://edri.org/our-work/eu-parliament-plenary-ban-of-public-facial-recognition-human-rights-gaps-ai-act/>, abgerufen am 15.04.2026.

<sup>11</sup> Amnesty International (2023): The EU must respect human rights of migrants in the AI Act, <https://www.amnesty.eu/news/the-eu-must-respect-human-rights-of-migrants-in-the-ai-act/>, abgerufen am 15.04.2026.

<sup>12</sup> Picum (2024): A dangerous precedent: how the EU AI Act fails migrants and people on the move, <https://picum.org/blog/a-dangerous-precedent-how-the-eu-ai-act-fails-migrants-and-people-on-the-move/>, abgerufen am 15.04.2026.

<sup>13</sup> European Digital Rights (2020): Technological Testing Grounds – Migration Management Experiments and Reflections from Ground up, <https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf>, abgerufen am 15.04.2026.

<sup>14</sup> European Parliamentary Research Service (2025): Artificial intelligence in asylum procedures in the EU - Briefing PE 775.861, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775861/EPRS\\_BRI\(2025\)775861\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775861/EPRS_BRI(2025)775861_EN.pdf), abgerufen am 15.04.2026.

<sup>15</sup> Ebd.

<sup>16</sup> Ebd.



## KI in der Beratung: Aktuelle Entwicklungen und Einsatzmöglichkeiten in den spezialisierten Fachberatungsstellen für Betroffene von Menschenhandel

Spezialisierte Fachberatungsstellen für Betroffene von Menschenhandel können von KI-Systemen profitieren. Vor allem administrative Aufgaben wie Dienstplanung, Organisation oder Informationsvermittlung lassen sich damit effizienter gestalten. Übersetzungstools können helfen, Sprachbarrieren in der Beratung zu überwinden. Darüber hinaus können KI-gestützte Chatbots eingesetzt werden, um allgemeine Informationen wie Öffnungszeiten oder Leistungsangebote zu vermitteln.

Das Potenzial von Chatbots scheint auf den ersten Blick hoch: Chatbots bieten niedrigschwelligen Zugang zu Unterstützung. Sie ermöglichen anonyme Beratung und helfen bei Sprachbarrieren, etwa durch automatische Übersetzungen, Untertitel oder vereinfachte Sprache. Ratsuchende können unabhängig von Öffnungs- und Beratungszeiten oder Standort Kontakt aufnehmen. Allerdings gibt es bisher nur wenige wissenschaftliche oder praxisnahe Erkenntnisse über den Einsatz von KI in der Beratung, insbesondere für Betroffene von Menschenhandel oder Ausbeutung. Große Sprachmodelle wie ChatGPT können zwar Informationen vermitteln und einfühlsame Antworten simulieren, komplexe Fallbewertungen und persönliche Hilfe erfordern jedoch weiterhin menschliche Fachkräfte.<sup>17</sup>

Chatbots haben sich jedoch als sinnvolle Ergänzung in der Aus- und Weiterbildung von Berater\*innen bewährt.<sup>18</sup> Besonders sensibel ist in diesem Zusammenhang der Datenschutz: Die erfassten Daten betreffen oft hoch vulnerable Personen, deren Identität und Aufenthaltsort geschützt werden müssen. Viele KI-Systeme stammen von privatwirtschaftlichen Anbietern, deren Datenverarbeitung nicht immer transparent ist.

Expert\*innen bewerten hybride Modelle als verantwortungsvolle Lösung: KI kann bei administrativen und operativen Prozessen unterstützen, Informationen vorsortieren oder zur Schulung von Fachkräften beitragen, während die persönliche Betreuung weiterhin durch erfahrene Fachkräfte erfolgt.<sup>19</sup>

Das Projekt Chayn unterstützt weltweit Betroffene geschlechtsspezifischer Gewalt.

2017 entwickelte es den Chatbot „Little Window“. Er wurde 2020 wieder abgeschaltet, weil er in Krisensituationen nicht zuverlässig funktionierte und zu wenig auf den Kontext der Anfragen einging. Heute setzt Chayn auf geschulte, menschliche Beratung.



← mehr dazu

<sup>17</sup> Beranek, Angelika (2025): Der Einsatz digitaler Tools und Künstlicher Intelligenz in der Sozialen Arbeit, In: Prof. Dr. Buttner, Peter (Hrsg.): Digitalisierung und KI in der Sozialen Arbeit. Archiv für Wissenschaft und Praxis der Sozialen Arbeit, Nr. 3/2025, S. 4–14.

<sup>18</sup> Ebd., S. 11.

<sup>19</sup> Gravelmann, Reinhold (2025): Auswirkungen Künstlicher Intelligenz auf die Soziale Arbeit: Chancen und Risikofaktoren, In: Prof. Dr. Buttner, Peter (Hrsg.): Digitalisierung und KI in der Sozialen Arbeit. Archiv für Wissenschaft und Praxis der Sozialen Arbeit, Nr. 3/2025, S. 20.



## Fazit

KI verändert den Kontext von Menschenhandel grundlegend. Täter\*innen nutzen KI, Deepfakes und automatisierte Kommunikation, um Betroffene zu kontaktieren, anzuwerben und zu kontrollieren. Gleichzeitig eröffnet KI Behörden und Beratungsstellen neue Möglichkeiten bei der Strafverfolgung und in der psychosozialen Beratung. Maßnahmen zur Prävention von Menschenhandel und zur Unterstützung Betroffener müssen dabei an Demokratie und Rechtstaatlichkeit, Menschenrechten sowie an die Vorgaben der Europaratskonvention zu KI und den EU AI Act gebunden sein. Diese Rahmenwerke fordern Transparenz, Verhältnismäßigkeit, wirksame Aufsicht und den Schutz der Grundrechte. Es ist unerlässlich, dass diese Prinzipien bei der Entwicklung und dem Einsatz von KI-Systemen zur Bekämpfung von Menschenhandel konsequent beachtet werden, damit Betroffene weder zusätzlich gefährdet noch diskriminiert werden.

