Model **United Nations**
Schleswig-Holstein

Gremientext - MRR

Recht auf Privatsphäre in Zeiten digitaler Überwachung

Dieser Gremientext behandelt unter anderem das Thema Verletzung von Privatsphäre. Bei manchen Personen löst dieses Thema starke Emotionen aus. Falls Sie zu den betroffenen Personen gehören, entscheiden Sie bitte selbst, ob Sie gerade in der Lage sind, sich mit dem Thema/diesen Themen zu beschäftigen, ob Sie das lieber zu einem späteren Zeitpunkt tun oder vorher bestimmte Maßnahmen ergreifen wollen.

Kurzzusammenfassung

Das Recht auf Privatsphäre ist durch Artikel 12 der Allgemeinen Erklärung der Menschenrechte und Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte geschützt. Digitale Technologien ermöglichen Staaten und Unternehmen jedoch eine immer weitreichendere Erfassung, Speicherung und Auswertung personenbezogener Daten. Insbesondere *Gesichtserkennung*, *biometrische Datenerfassung*, *künstliche Intelligenz* und automatisiertes *Profiling* können tief in die Privatsphäre eingreifen und zugleich Meinungs-, Presse-, Versammlungs- und Vereinigungsfreiheit beeinträchtigen.

Die Vereinten Nationen beschäftigen sich seit 2013 intensiv mit dem Schutz der Privatsphäre im digitalen Zeitalter. Der Menschenrechtsrat hat mehrfach entsprechende Resolutionen verabschiedet und 2015 das Mandat der Sonderberichterstatterin für das Recht auf Privatsphäre geschaffen. 2024 wurde dieses Mandat erneut verlängert. Die UN betont insbesondere die Bedeutung von Rechtmäßigkeit, *Notwendigkeit*, *Verhältnismäßigkeit*, unabhängiger Kontrolle und wirksamen *Rechtsmitteln* bei der digitalen Erfassung und Verwendung von Daten

Gleichzeitig bestehen weiterhin Lücken bei der Regulierung neuer *Überwachungstechnologien*. Der Menschenrechtsrat steht daher vor der Frage, welche internationalen Mindeststandards für staatliche digitale *Überwachung* notwendig sind, wie besonders invasive Anwendungen, beispielsweise biometrische *Massenüberwachung* begrenzt werden können und wie Transparenz, Kontrolle und effektive *Rechtsmittel* für Betroffene gewährleistet werden können.

Diskussionspunkte

- Welche internationalen Mindeststandards sollten für staatliche digitale *Überwachung* gelten, damit Eingriffe in das Recht auf Privatsphäre rechtmäßig, notwendig und verhältnismäßig bleiben?

- Unter welchen Voraussetzungen sollte der Einsatz biometrischer *Überwachungstechnologien* wie *Gesichtserkennung* zulässig sein, und welche besonders invasiven Anwendungen sollten eingeschränkt oder verboten werden?

- Wie können Staaten verhindern, dass digitale *Überwachung* zur Einschränkung der Meinungs-, Informations- und Pressefreiheit eingesetzt wird, insbesondere gegenüber Journalist*innen, Menschenrechtsverteidiger*innen und politischen Oppositionellen?

- Welche unabhängigen Kontrollmechanismen sind notwendig, um staatliche *Überwachungsmaßnahmen* wirksam zu überprüfen und Missbrauch zu verhindern?

- Wie viel Transparenz müssen Staaten über ihre *Überwachungsmaßnahmen* gewährleisten, und unter welchen Umständen darf das Informieren Betroffener aus Gründen der nationalen Sicherheit eingeschränkt werden?

- Welche wirksamen *Rechtsmittel* sollten Personen zur Verfügung stehen, die durch staatliche digitale *Überwachung* in ihren Menschenrechten verletzt wurden?

- Welche internationalen Mechanismen können sicherstellen, dass Menschenrechtsstandards auch auf neue *Überwachungstechnologien* wie *künstliche Intelligenz*, automatisierte Datenauswertung und biometrische Identifizierung wirksam angewendet werden?

Einleitung


Bild 1

Stellen wir uns eine Demonstration in einer Großstadt vor. Hunderte Menschen versammeln sich, diskutieren und halten Plakate in die Höhe. Über ihnen befinden sich Kameras. Einige davon können Gesichter erkennen, Personen

identifizieren und Bewegungen verfolgen. Die Demonstrierenden wissen möglicherweise nicht, ob ihre Daten tatsächlich erfasst werden. Dennoch kann allein die Möglichkeit einer *Überwachung* beeinflussen, wie frei Menschen sich bewegen, äußern oder an politischen Aktivitäten teilnehmen.

Digitale *Überwachung* kann für Staaten durchaus hilfreich sein, etwa bei der Strafverfolgung oder der Gefahrenabwehr. Gleichzeitig ermöglichen *künstliche Intelligenz (KI), biometrische Daten* und automatisierte Datenauswertung eine immer umfassendere Erfassung und Analyse menschlichen Verhaltens, was durchaus auch Gefahren für die Rechte des Einzelnen birgt. Damit stellt sich eine zentrale menschenrechtliche Frage:

Wie können Staaten legitime Sicherheitsinteressen verfolgen, ohne das Recht auf Privatsphäre und andere Menschenrechte unverhältnismäßig einzuschränken?

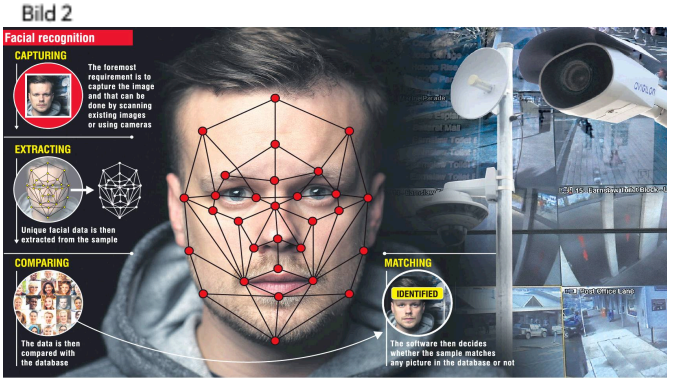
Für den Menschenrechtsrat ist daher insbesondere relevant , welche internationalen Mindeststandards für staatliche digitale *Überwachung* notwendig sind und wie ihre Einhaltung gewährleistet werden kann.

Hintergrund und Grundsätzliches

Das Recht auf Privatsphäre ist ein grundlegendes Menschenrecht. Artikel 12 der Allgemeinen Erklärung der Menschenrechte (AEMR) schützt Menschen vor willkürlichen Eingriffen in ihre Privatsphäre, Familie, Wohnung und Korrespondenz. Auch Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte (IPbpR) schützt vor rechtswidrigen und willkürlichen Eingriffen in die Privatsphäre. Staatliche *Überwachung* ist dadurch jedoch nicht grundsätzlich verboten. Entscheidend ist vielmehr, ob ein Eingriff rechtmäßig, notwendig und verhältnismäßig ist.

Die Digitalisierung hat die Möglichkeiten staatlicher und privater Akteur*innen, bei unter anderem der Strafverfolgung oder der Datenerfassung, erheblich erweitert. Neben klassischer *Videoüberwachung* können heute beispielsweise *biometrische Daten* erfasst, Gesichter automatisiert erkannt,

Bild 2



Kommunikationsdaten ausgewertet und aus verschiedenen Datenquellen detaillierte Profile erstellt werden. KI ermöglicht es, große Datenmengen automatisiert auszuwerten, Muster zu erkennen und Verhalten zu analysieren. Dadurch können Eingriffe in die Privatsphäre deutlich umfangreicher und schwerer nachvollziehbar werden.

Besonders deutlich wird dies bei der *Gesichtserkennung*. Kameras können Personen automatisiert identifizieren und ihre Bewegungen verfolgen. Dadurch entstehen neben Risiken für die Privatsphäre auch mögliche Auswirkungen auf Meinungs-, Versammlungs-, Vereinigungs- und Bewegungsfreiheit. Zudem können unterschiedliche Fehlerraten zwischen Bevölkerungsgruppen, das heißt, dass die *Gesichtserkennungssysteme* nicht bei allen Personengruppen gleich zuverlässig funktionieren, das Risiko von Fehlidentifizierungen und Diskriminierung erhöhen.

Neben Staaten spielen bei diesem Thema auch Unternehmen eine wichtige Rolle. Sie entwickeln und betreiben Technologien zur Erhebung und Auswertung großer Datenmengen. Während Staaten die primäre Verantwortung für den Schutz der Menschenrechte tragen, müssen auch Unternehmen diesbezüglich zur Verantwortung gezogen werden.

Aktuelles

2013 · A/RES/68/167
Erste Resolution zur Privatsphäre

2015 · A/HRC/RES/28/16
Mandat der Sonderberichterstatterin geschaffen

2018 · A/HRC/39/29
OHCHR-Bericht zu Big Data und KI

2023 · A/HRC/RES/54/21
Aktuellste eigenständige HRC-Resolution

2024 · A/HRC/RES/55/3
Mandat verlängert, KI und Biometrie ergänzt

2025 · A/HRC/RES/58/23 & 59/15
Schutz für Journalist*innen und Aktivist*innen

Die Vereinten Nationen beschäftigen sich seit mehr als einem Jahrzehnt mit dem Schutz der Privatsphäre im digitalen Zeitalter. 2013 verabschiedete die Generalversammlung die Resolution A/RES/68/167 zum Recht auf Privatsphäre im digitalen Zeitalter. 2014 folgte ein Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte (Office of the High Commissioner for Human Rights, OHCHR). 2015 schuf der Menschenrechtsrat mit A/HRC/RES/28/16 das Mandat der Sonderberichterstatterin für das Recht auf Privatsphäre. Seitdem

wurden weitere Resolutionen zu dem Thema verabschiedet. Die bisher jüngste eigenständige Resolution des Menschenrechtsrats ist A/HRC/RES/54/21 aus dem Jahr 2023.

Eine besondere Bedeutung hat A/HRC/RES/55/3 aus dem Jahr 2024. Mit ihr verlängerte der Menschenrechtsrat das Mandat der Sonderberichterstatterin. Die Resolution nennt ausdrücklich *Überwachung, KI,* automatisierte Entscheidungsfindung, Machine Learning, *Profiling*, Tracking und biometrische Technologien einschließlich *Gesichtserkennung*. Sie weist darauf hin, dass diese Technologien ohne angemessene Schutzmaßnahmen nicht nur die Privatsphäre, sondern auch andere Menschenrechte beeinträchtigen können.

Auch darüber hinaus thematisieren die Vereinten Nationen zunehmend die Verbindung zwischen digitaler *Überwachung* und anderen Menschenrechten. Die Resolution A/HRC/RES/58/23 von 2025 befasst sich mit Menschenrechtsverteidiger*innen *und* neuen *Technologien. A/HRC/RES/59/15 von 2025 behandelt die Sicherheit von* Journalist*innen. Damit wird deutlich, dass der Schutz der Privatsphäre auch für die Arbeit von Journalist*innen, Menschenrechtsverteidiger*innen und anderen zivilgesellschaftlichen Akteur*innen relevant ist.

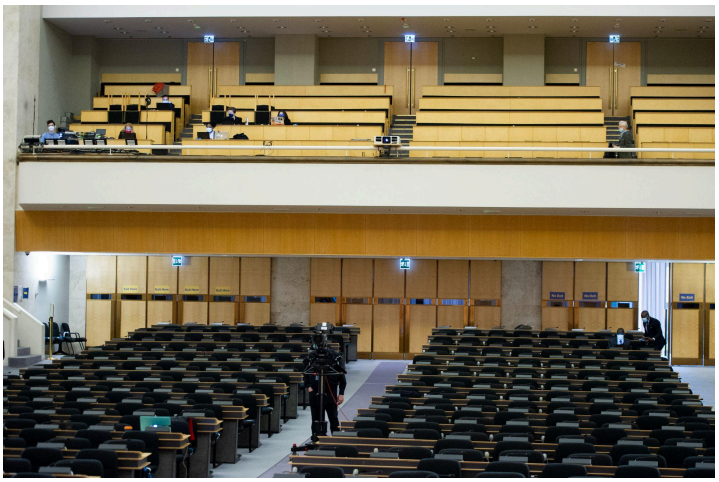


Bild 3

Probleme und Lösungsansätze

Trotz der bestehenden internationalen Menschenrechtsstandards besteht weiterhin eine Lücke zwischen den technologischen Möglichkeiten und ihrer menschenrechtlichen Regulierung. Die zentrale Herausforderung besteht darin, allgemeine Grundsätze wie Rechtmäßigkeit, *Notwendigkeit* und *Verhältnismäßigkeit* auf immer neue *Überwachungstechnologien* anzuwenden.

Besonders umstritten ist der Einsatz biometrischer *Überwachung.* Während gezielte *Überwachung* einzelner Personen unter bestimmten Voraussetzungen gerechtfertigt

sein kann, erfasst biometrische *Massenüberwachung* potenziell große Teile der Bevölkerung. Der Menschenrechtsausschuss hat deshalb Bedenken hinsichtlich der Vereinbarkeit solcher Maßnahmen mit Artikel 17 IPbpR geäußert und die Bedeutung unabhängiger Kontrolle und gerichtlicher Überprüfung hervorgehoben.

Eine mögliche Lösung sind internationale Mindeststandards für staatliche *Überwachung*. Diese könnten verlangen, dass jede Maßnahme auf einer klaren gesetzlichen Grundlage beruht, einem legitimen Ziel dient und nur eingesetzt wird, wenn weniger eingriffsintensive Alternativen nicht ausreichen. Für besonders invasive Technologien könnten zusätzliche Voraussetzungen oder Einschränkungen gelten.

Dabei stellt sich auch die Frage, welche Anwendungen überhaupt akzeptabel sind. Während eine gezielte *Gesichtserkennung* zur Identifizierung einer konkret gesuchten Person möglicherweise anders bewertet werden kann als eine flächendeckende *Überwachung* öffentlicher Räume, könnten bestimmte Formen biometrischer *Massenüberwachung* aufgrund ihrer Eingriffsintensität besonders strengen Grenzen unterliegen.

Ein weiterer Ansatz ist die unabhängige Kontrolle. Gerichte, Datenschutzbehörden, parlamentarische Kontrollorgane oder unabhängige Menschenrechtsinstitutionen könnten überprüfen, ob *Überwachungsmaßnahmen* rechtmäßig und verhältnismäßig sind. Vor der Einführung neuer Technologien könnten außerdem *Menschenrechtsfolgenabschätzungen* durchgeführt werden. Dabei würde geprüft werden, welche Auswirkungen eine Technologie auf Privatsphäre, Nichtdiskriminierung und weitere Menschenrechte haben kann.

Auch Transparenz ist bei einer möglichen digitalen *Überwachung* entscheidend. Betroffene wissen häufig nicht, ob und in welchem Umfang sie überwacht wurden. Ohne entsprechende Informationen ist es schwierig, eigene Rechte geltend zu machen. Staaten könnten daher verpflichtet werden, über den Einsatz bestimmter *Überwachungstechnologien* zu informieren und Betroffene unter geeigneten Voraussetzungen nachträglich über eine *Überwachung* zu benachrichtigen. Gleichzeitig muss berücksichtigt werden, dass eine sofortige Information laufende Ermittlungen gefährden kann.

Schließlich müssen wirksame *Rechtsmittel* gewährleistet werden. Betroffene sollten die Möglichkeit haben, mutmaßlich rechtswidrige *Überwachung* überprüfen zu lassen und gegebenenfalls die Löschung unrechtmäßig erhobener Daten oder eine Entschädigung zu verlangen.

Eine weitere Herausforderung besteht darin, dass einmal erhobene Daten für andere Zwecke verwendet werden können. Internationale Standards könnten deshalb eine

klare *Zweckbindung* und *Datenminimierung* vorsehen: Daten sollten nur für einen festgelegten legitimen Zweck und nur in dem Umfang erhoben und gespeichert werden, in dem sie tatsächlich erforderlich sind.

Der Menschenrechtsrat steht damit vor der Aufgabe, bestehende Menschenrechtsstandards auf eine sich schnell verändernde technologische Umgebung anzuwenden. Dabei stehen unterschiedliche Ansätze zur Debatte – von strengeren internationalen Vorgaben und Einschränkungen besonders invasiver Technologien bis hin zu einer Regulierung, die ihren Einsatz unter klar definierten Voraussetzungen weiterhin ermöglicht. Entscheidend ist, einen Ausgleich zwischen legitimen Sicherheitsinteressen und dem Schutz der Menschenrechte zu finden.

Glossar

- **Biometrische Daten:** Personenbezogene Daten, die sich auf körperliche oder verhaltensbezogene Merkmale einer Person beziehen und zur Identifizierung genutzt werden können, beispielsweise Gesicht, Fingerabdrücke oder Iris.
- **Gesichtserkennung:** Technologie, die anhand charakteristischer Merkmale eines Gesichts eine Person automatisch identifizieren oder mit gespeicherten Bildern abgleichen kann.
- **Künstliche Intelligenz (KI):** Technologien, die Aufgaben ausführen, für die typischerweise menschliche kognitive Fähigkeiten wie Mustererkennung, Klassifikation oder Entscheidungsfindung erforderlich sind.
- **Menschenrechtsfolgenabschätzung:** Systematische Prüfung, welche Auswirkungen eine geplante Maßnahme, Technologie oder Regelung auf die Menschenrechte haben kann.
- **Notwendigkeit:** Grundsatz, nach dem ein Eingriff in ein Menschenrecht zur Erreichung eines legitimen Ziels tatsächlich erforderlich sein muss und keine gleich geeignete, weniger eingriffsintensive Alternative bestehen darf.
- **Profiling:** Automatisierte Verarbeitung personenbezogener Daten, um bestimmte Eigenschaften, Interessen, Verhaltensweisen oder mögliche zukünftige Handlungen einer Person zu analysieren oder vorherzusagen.
- **Rechtsmittel:** Möglichkeiten, mit denen Betroffene eine mutmaßliche Rechtsverletzung überprüfen und gegebenenfalls Abhilfe oder Entschädigung verlangen können.
- **Überwachung:** Systematische Beobachtung, Erfassung oder Auswertung von Personen, Kommunikation, Bewegungen oder Verhalten durch staatliche oder private Akteur*innen.
- **Verhältnismäßigkeit:** Grundsatz, nach dem ein Eingriff in ein Menschenrecht nicht weiter gehen darf, als es zur Erreichung eines legitimen Ziels erforderlich ist. Dabei müssen Nutzen und Schwere des Eingriffs angemessen zueinander stehen.

Recherchehinweise

Um die Position des eigenen Staates zum Recht auf Privatsphäre und digitaler *Überwachung* zu bestimmen, sollte zunächst geprüft werden, welchen internationalen Menschenrechtsverträgen der Staat beigetreten ist, insbesondere ob er Vertragsstaat des Internationalen Pakts über bürgerliche und politische Rechte (IPbpR) ist. Anschließend empfiehlt es sich, nationale Gesetze zu Datenschutz, Nachrichtendiensten, Strafverfolgung und digitaler *Überwachung* zu untersuchen. Besonders relevant sind Regelungen zum Einsatz von *Gesichtserkennung* und biometrischen Daten sowie zur Speicherung und Weitergabe personenbezogener Daten.

Darüber hinaus sollte betrachtet werden, ob der Staat in internationalen Foren Maßnahmen zum Schutz der digitalen Privatsphäre unterstützt oder abgelehnt hat. Hierfür eignen sich insbesondere Abstimmungsverhalten, Stellungnahmen und Redebeiträge bei Resolutionen des Menschenrechtsrats und der Generalversammlung. Auch nationale Außen-, Innen- und Justizministerien können Hinweise auf die staatliche Position liefern.

Für die Haltung zu neuen Technologien lohnt sich außerdem die Suche nach nationalen Strategien oder Gesetzen zu künstlicher Intelligenz, biometrischer Identifizierung und staatlicher *Überwachung*. Dabei sollte insbesondere untersucht werden, ob ein Staat eher auf weitreichende Sicherheitsbefugnisse, strenge menschenrechtliche Grenzen oder einen regulierten Mittelweg setzt.

Besonders wichtige Dokumente für die Recherche sind A/HRC/RES/54/21 (2023), A/HRC/RES/55/3 (2024) sowie aktuelle Berichte der Sonderberichterstatterin für das Recht auf Privatsphäre. Ergänzend können Berichte des OHCHR und relevante Stellungnahmen internationaler Menschenrechtsorganisationen herangezogen werden.

Wichtige Dokumente

1. A/HRC/RES/54/21 – 2023

UN-Dokument A/HRC/RES/54/21

Human Rights Council: *Right to privacy in the digital age.*
Warum wichtig: Die aktuellste eigenständige Resolution des Menschenrechtsrats zum Recht auf Privatsphäre im digitalen Zeitalter; verabschiedet am 12. Oktober 2023 ohne Abstimmung.

2. A/HRC/RES/55/3 – 2024

UN-Dokument A/HRC/RES/55/3

Human Rights Council: *Mandate of Special Rapporteur on the right to privacy.*
Warum wichtig: Verlängert das Mandat der Sonderberichterstatterin und benennt ausdrücklich Überwachung, KI, automatisierte Entscheidungsfindung, Machine Learning, Profiling, Tracking und biometrische Technologien einschließlich Gesichtserkennung.

3. A/HRC/51/17 – 2022

UN-Dokument A/HRC/51/17

Special Rapporteur on the right to privacy: *The right to privacy in the digital age.*
Warum wichtig: Behandelt insbesondere Verschlüsselung, Privatsphäre und Überwachung und zeigt, wie digitale Kommunikation und neue Technologien bestehende Datenschutzprobleme verschärfen.

4. A/HRC/39/29 – 2018

OHCHR-Bericht A/HRC/39/29

Office of the High Commissioner for Human Rights: *The right to privacy in the digital age.*
Warum wichtig: Einer der grundlegenden OHCHR-Berichte zum Thema. Er erklärt die menschenrechtlichen Risiken von Big Data und neuen Technologien und entwickelt konkrete Anforderungen an staatliche Überwachung.

Quellenverzeichnis

Office of the United Nations High Commissioner for Human Rights (2022): The right to privacy in the digital age. A/HRC/51/17, (4.8.2024), *Behandelt gezielt Hacking-Tools, Verschlüsselung und öffentliche Überwachung – gut geeignet, um die Probleme-Sektion zu vertiefen.* (Englisch) https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age

Office of the United Nations High Commissioner for Human Rights (2018): The right to privacy in the digital age. A/HRC/39/29, (3.8.2018), *Grundlegender Bericht zu Big Data und KI-Risiken für die Privatsphäre.* (Englisch) https://digitallibrary.un.org/record/1640588

Office of the United Nations High Commissioner for Human Rights (2014): The right to privacy in the digital age. A/HRC/27/37, (30.6.2014), *Erster ausführlicher OHCHR-Bericht zum Thema, Ausgangspunkt der UN-Befassung nach dem Snowden-Skandal.* (Englisch)

https://digitallibrary.un.org/record/777869

United Nations General Assembly (2013): The right to privacy in the digital age. A/RES/68/167, (18.12.2013), *Erste GA-Resolution zum Thema, Grundstein der gesamten UN-Regulierungsdebatte.* (Deutsch verfügbar) https://digitallibrary.un.org/record/764407

United Nations General Assembly (2016): The right to privacy in the digital age. A/RES/71/199, (19.12.2016), *Folgeresolution, ermutigt den Menschenrechtsrat, das Thema weiter zu vertiefen.* (Deutsch verfügbar) https://digitallibrary.un.org/record/858023

United Nations Human Rights Council (2025): Human rights defenders and new and emerging technologies. A/HRC/RES/58/23, (4.4.2025), *Verknüpft digitale Überwachung mit dem Schutz von Menschenrechtsverteidiger*innen.* (Englisch) https://docs.un.org/en/A/HRC/RES/58/23

United Nations Human Rights Council (2024): Mandate of Special Rapporteur on the right to privacy. A/HRC/RES/55/3, (3.4.2024), https://digitallibrary.un.org/record/4045553

United Nations Human Rights Council (2023): Right to privacy in the digital age. A/HRC/RES/54/21, (12.10.2023), *Jüngste eigenständige HRC-Resolution zum Thema, ohne Abstimmung verabschiedet; enthält konkrete Forderungen zu biometrischer Massenüberwachung.* (Englisch) https://digitallibrary.un.org/record/4025243

United Nations Human Rights Council (2025): The safety of journalists. A/HRC/RES/59/15, (7.7.2025), *Zeigt die Verbindung zwischen Überwachung und Pressefreiheit – relevant für Diskussionspunkt 3.* (Englisch) https://digitallibrary.un.org/record/4087010

Bildquellen

Bild 1

Kameras im öffentlichen Raum – Symbolbild. Foto: Mike Mozart, CC BY 2.0, via Wikimedia Commons
Quelle: https://nypost.com/2019/09/05/activists-pushing-for-federal-facial-recognition-ban/

Bild 2

Biometrische Gesichtserkennung am Flughafen Houston, USA (U.S. Customs and Border Protection, 2018). Foto: Donna Burton / U.S. Customs and Border Protection, gemeinfrei (Werk der US-Bundesregierung)
Quelle: https://www.tvguy.com.au/security-cameras/

Bild 3

Eröffnung der 46. Sitzung des Menschenrechtsrats, Palais des Nations, Genf (22. Februar 2021). UN Photo/Violaine Martin
Quelle: https://www.flickr.com/photos/unisgeneva/50968155968/

Grafik

Zeitleiste: Wichtige UN-Resolutionen und -Berichte zum Recht auf Privatsphäre im digitalen Zeitalter, 2013–2025. Eigene Darstellung; Erstellt mit Claude, Sonnet 5, Anthropic