

# Offener Brief: Wir fordern ein weltweites Verbot von Technologien zur biometrischen Erkennung

Wir, die Unterzeichnenden, fordern ein vollständiges Verbot des Einsatzes von Gesichtserkennungs- und biometrischen Fernidentifizierungssystemen, die Massenüberwachung und diskriminierende gezielte Überwachung von Individuen ermöglichen. Diese Werkzeuge sind in der Lage, Menschen auf Schritt und Tritt zu verfolgen, zu identifizieren, auszusondern und nachzuverfolgen. Diese Verfahren untergraben unsere Menschenrechte und bürgerlichen Freiheiten - einschließlich des Rechts auf Privatsphäre und Datenschutz, des Rechts auf freie Meinungsäußerung, des Rechts auf Gleichheit und Nichtdiskriminierung und des Rechts auf Versammlungs- und Vereinigungsfreiheit (was dazu führt, dass Protest kriminalisiert wird und eine abschreckende Wirkung (chilling effect) auf die Wahrnehmung von Grundrechten hat).

Wir haben bereits gesehen, wie Gesichtserkennung und biometrische Fernerkennungstechnologien verwendet wurden, um eine Litanei von Menschenrechtsverletzungen zu ermöglichen. In [China](#), den [Vereinigten Staaten](#), [Russland](#), [England](#), [Uganda](#), [Kenia](#), [Slowenien](#), [Myanmar](#), den [Vereinigten Arabischen Emiraten](#), [Israel](#) und [Indien](#) hat die Überwachung von Demonstrant:innen und Zivilist:innen ihr Grundrecht auf Privatsphäre und ihr Recht auf Versammlungs- und Vereinigungsfreiheit verletzt. Die unrechtmäßigen Verhaftungen von unschuldigen Personen in den [Vereinigten Staaten](#), [Argentinien](#) und [Brasilien](#) haben deren Grundrechte auf Privatsphäre, ein faires Verfahren und Bewegungsfreiheit untergraben. Die Überwachung ethnischer und religiöser Minderheiten und anderer marginalisierter und unterdrückter Gruppen in [China](#), [Thailand](#) und [Italien](#) hat ihre Rechte auf Privatsphäre, auf Gleichheit und Nicht-Diskriminierung verletzt.

Diese Technologien bedrohen sind inhärent so konzipiert, dass sie die Rechte von Menschen bedrohen und haben entsprechend bereits erheblichen Schaden verursacht. Keine technischen oder rechtlichen Schutzmaßnahmen könnten die Bedrohung, die sie darstellen, jemals vollständig beseitigen. Wir sind daher der Meinung, dass sie niemals in öffentlichen oder öffentlich zugänglichen Räumen eingesetzt werden sollten - weder von Regierungen noch vom privaten Sektor. Das Missbrauchspotenzial ist zu groß und die Folgen sind zu schwerwiegend.

**Wir fordern ein Verbot**, denn auch wenn ein Moratorium die Entwicklung und den Einsatz dieser Technologien vorübergehend stoppen und Zeit gewinnen könnte, um Beweise zu sammeln und eine demokratische Debatte zu organisieren, zeichnet sich schon heute ab, dass diese Untersuchungen und Debatten nur noch stärker aufzeigen werden, **dass der Einsatz dieser Technologien in öffentlich zugänglichen Räumen mit unseren Menschen- und Bürgerrechten unvereinbar ist und endgültig verboten werden muss.**

## Der Umfang unseres Aufrufs

Die Begriffe "Gesichtserkennung" und "biometrische Fernidentifizierung" umfassen eine breite Palette von Technologien, vom Gesichts-Authentifizierungssystem, das das Telefon einer Person entsperrt oder den Zugang zu bestimmten Orten autorisiert, über Technologie, die den Gang einer Person identifiziert, bis hin zu Systemen, die vorgeben, die Geschlechtsidentität oder den emotionalen Zustand einer Person zu erkennen.

**Unsere Forderung nach einem Verbot bezieht sich insbesondere, aber nicht ausschließlich, auf die Verwendung der Technologien zur Identifizierung oder Unterscheidung einer Person aus einer größeren Menge von Personen,** auch bekannt als Gesichts- oder biometrische "Identifizierung" (sogenanntes "one-to-many matching"). Wir sind besorgt über den Einsatz dieser Technologien, die Personen anhand ihres Gesichts, ihres Gangs, ihrer Stimme, ihres persönlichen Aussehens oder anderer biometrischer Merkmale identifizieren, aussondern oder verfolgen. Diese Überwachung wirkt sich unverhältnismäßig stark auf die Menschenrechte und bürgerlichen Freiheiten von religiösen, ethnischen und rassifizierten Minderheiten, politischen Dissidenten und anderen Randgruppen aus. Wir erkennen gleichzeitig auch an, dass in bestimmten Fällen Gesichts- und andere biometrische "Authentifizierungs"-Systeme (sogenanntes "one-to-one matching") in einer Weise aufgebaut und verwendet werden können, die ebenfalls problematische Formen der Überwachung ermöglicht. Dies kann z. B. durch die Schaffung großer, zentralisierter biometrischer Datenbanken geschehen, die für andere Zwecke wiederverwendet werden können.

Obwohl einige Anwendungen der Gesichtserkennung und der biometrischen Fernidentifizierung behaupten, die Privatsphäre von Personen zu schützen, indem sie keine Verbindung zu deren rechtlichen Identitäten herstellen, können sie dennoch verwendet werden, um Personen im öffentlichen Raum zu identifizieren oder Rückschlüsse auf deren Eigenschaften und Verhalten zu ziehen. In all diesen Situationen spielt es keine Rolle, ob die Daten anonymisiert werden, um persönlich identifizierbare Informationen zu schützen, oder ob sie nur lokal (d.h. "am Rande") verarbeitet werden; die Beeinträchtigung unserer Rechte erfolgt in jedem Fall, weil diese Werkzeuge im Kern für die Überwachung von Menschen in einer Weise konzipiert sind, die mit unseren grundlegenden Rechten unvereinbar ist.

Darüber hinaus basieren viele Anwendungen der Gesichts- und biometrischen Klassifizierung, die Rückschlüsse und Vorhersagen über Dinge wie das Geschlecht, die Emotionen oder andere persönliche Eigenschaften von Menschen machen, auf schwerwiegend fehlerhaften wissenschaftlichen Grundlagen. Das bedeutet, dass die Schlüsse, die sie über uns ziehen, oft ungültig sind und in einigen Fällen sogar [eugenische Theorien der Phrenologie und Physiognomie](#) operationalisieren. Dadurch wird Diskriminierung aufrechterhalten und eine zusätzliche Ebene des Schadens hinzugefügt: Wir werden sowohl überwacht als auch falsch charakterisiert/eingeordnet.

**Unsere Forderung nach einem Verbot umfasst den Einsatz dieser Technologien, wenn sie zur Überwachung in öffentlich zugänglichen Räumen und in Räumen, die Menschen nicht vermeiden können, eingesetzt werden.** Während der Einsatz dieser Technologien durch Strafverfolgungsbehörden Aufmerksamkeit und Kritik auf sich gezogen hat, kann ihr Einsatz durch private Akteur:innen die gleiche Bedrohung für unsere Rechte darstellen. Insbesondere, wenn private Akteur:innen im Rahmen von öffentlich-privaten Partnerschaften tatsächlich im Auftrag von Regierungen und öffentlichen Stellen Überwachungsmaßnahmen durchführen oder den Behörden auf andere Weise aus einer solchen Überwachung gewonnene Informationen zur Verfügung stellen.

Wir haben auch eine besorgniserregende Entwicklung bei privaten Anbietern von Gesichtserkennungssystemen beobachtet, die [Datenbanken von "verdächtigen" Personen](#) zusammenstellen und zusammenführen und diese mit mehreren Kunden teilen. Dadurch entstehen faktisch "landesweite Datenbanken", die von privaten Unternehmen gemeinsam genutzt werden. Diese werden nach dem Ermessen ungeschulter Mitarbeiter:innen zusammengestellt, unterliegen keiner Aufsicht und können in allen Einrichtungen, von denen sie genutzt werden, zur Diskriminierung von Personen führen, die auf Überwachungslisten erscheinen.

Der Einsatz dieser Technologien zur Überwachung von Menschen in Stadtparks, Schulen, Bibliotheken, Arbeitsplätzen, Verkehrsknotenpunkten, Sportstadien, Wohnsiedlungen und sogar in Online-Räumen wie Social-Media-Plattformen stellt eine existenzielle Bedrohung für unsere Menschenrechte und bürgerlichen Freiheiten dar und muss gestoppt werden.

## Warum ein Verbot?

Gesichtserkennungs- und biometrische Fernidentifizierungssysteme weisen in ihrer derzeitigen Form erhebliche technische Mängel auf, wie z. B. Gesichtserkennungssysteme, die rassistische Vorurteile widerspiegeln und bei Menschen mit dunklerer Hautfarbe weniger genau sind. Technische Verbesserungen an diesen Systemen werden die Bedrohung, die sie für unsere Menschenrechte und bürgerlichen Freiheiten darstellen, jedoch nicht beseitigen.

Während das Hinzufügen von ausgewogeneren Trainingsdaten oder andere Maßnahmen zur Verbesserung der Genauigkeit einige aktuelle Probleme mit diesen Systemen beheben können, wird es sie letztendlich nur als Überwachungsinstrumente perfektionieren und sie bei der Untergrabung unserer Rechte dadurch noch effektiver machen.

Diese Technologien stellen in zweierlei Hinsicht eine Bedrohung für unsere Rechte dar:

Erstens werden die Trainingsdaten - die Datenbanken mit Gesichtern, mit denen die Eingabedaten verglichen werden, und die biometrischen Daten, die von diesen Systemen verarbeitet werden - in der Regel **ohne das Wissen, die Zustimmung oder die wirklich freie Entscheidung einer Person erlangt**, was bedeutet, dass diese Technologien sowohl eine massenhafte als auch diskriminierende gezielte Überwachung von Grund aus fördern.

Zweitens: Solange Menschen in öffentlich zugänglichen Räumen unmittelbar identifiziert, ausgesondert oder verfolgt werden können, werden ihre Menschenrechte und bürgerliche Freiheiten untergraben. Schon die Vorstellung, dass solche Technologien in öffentlich zugänglichen Räumen eingesetzt werden könnten, erzeugt einen Abschreckungseffekt, der die Menschen daran hindert, ihre Rechte wahrzunehmen.

Trotz fragwürdiger Behauptungen, dass diese Technologien die öffentliche Sicherheit verbessern, wird jeder mögliche Nutzen durch die systematische Verletzung unserer Rechte bei weitem aufgewogen werden. Wir sehen immer mehr Beweise dafür, wie diese Technologien **missbraucht** und mit wenig bis gar keiner Transparenz eingesetzt werden.

Jede Untersuchung und Analyse der bisherigen Polizeiarbeit zeigt, dass der experimentelle Einsatz von Überwachungstechnologien immer wieder einkommensschwache und marginalisierte Gruppen kriminalisiert, darunter auch Communities of Color - dieselben Personengruppen, die traditionell mit strukturellem Rassismus und Diskriminierung konfrontiert sind. Der Einsatz von **Gesichtserkennungs- und biometrischen Fernidentifizierungssystemen bildet keine Ausnahme** und muss aus diesem Grund gestoppt werden, bevor eine noch gefährlichere Überwachungsinfrastruktur geschaffen wird oder sich dauerhaft etabliert.

Die bloße Existenz dieser Technologien, ob in den Händen der Strafverfolgungsbehörden oder privater Unternehmen (oder in öffentlich-privaten Partnerschaften), wird immer Anreize für eine schleichende Ausweitung der Funktionen und eine verstärkte Überwachung des öffentlichen Raums schaffen, was eine abschreckende Wirkung auf die freie Meinungsäußerung hat. Da ihre bloße Existenz unsere Rechte untergräbt und eine wirksame Aufsicht über diese Technologien nicht

möglich ist, um Missbrauch auszuschließen, gibt es keine andere Möglichkeit, als ihre Verwendung in öffentlich zugänglichen Räumen vollständig zu verbieten.

## Wie wird ein Verbot aussehen?

Es gibt einige Überwachungstechnologien, die einfach so gefährlich sind, dass sie unweigerlich weit mehr Probleme verursachen, als sie lösen. Wenn es um Gesichtserkennung und ferngesteuerte biometrische Technologien geht, die Massenüberwachung und diskriminierende, gezielte Überwachung ermöglichen, ist das Missbrauchspotenzial zu groß und die Folgen zu schwerwiegend.

Es gibt keinen Raum für Zweifel: Der Schutz von Menschenrechten und bürgerlichen Freiheiten erfordert ein Verbot des Einsatzes dieser Technologien in öffentlich zugänglichen Räumen durch nationale, staatliche, provinzielle, kommunale, lokale und andere Regierungen, einschließlich aller ihrer Untergliederungen und Behörden - und insbesondere ihrer Strafverfolgungs- und Grenzkontrollbehörden, die bereits über ausreichende personelle und technologische Ressourcen verfügen, um die Sicherheit ohne diese Technologien aufrechtzuerhalten.

Als globales Netzwerk zivilgesellschaftlicher Organisationen erkennen wir an, dass jedes Land andere Wege hat, um Lösungen zu entwickeln, um Menschenrechten im Rahmen ihrer jeweiligen verfassungsmäßigen, konventionellen oder gesetzlichen Systeme Vorrang einzuräumen.

Was auch immer die Mittel sein mögen – das Ergebnis muss ein vollständiges Verbot des Einsatzes dieser Technologien zur Überwachung, Identifizierung, Verfolgung, Klassifizierung und Verfolgung von Menschen in öffentlich zugänglichen Räumen sein.

Aus all diesen Gründen fordern wir, dass:

---

### 1. Politische Entscheidungsträger-innen und Gesetzgeber-innen auf allen Regierungsebenen in der ganzen Welt:

- a. alle öffentlichen Investitionen in die Nutzung von Gesichtserkennungs- und ferngesteuerten biometrischen Technologien stoppen, die Massenüberwachung und diskriminierende gezielte Überwachung ermöglichen;
- b. umfassende Gesetze, Statuten und/oder Vorschriften verabschieden, die:
  - i. die Verwendung dieser Technologien zur Überwachung öffentlicher und öffentlich zugänglicher Räume, einschließlich öffentlicher Verkehrsmittel, durch oder im Namen von nationalen, bundesstaatlichen, staatlichen, provinziellen, kommunalen, lokalen und/oder anderen politischen Unterabteilungen von Regierungen, einschließlich ihrer Agenturen, Abteilungen, Sekretariate, Ministerien, Exekutivbüros, Gremien, Kommissionen, Büros oder ihrer Auftragnehmer-innen und/oder anderer Unterabteilungen und Behörden, verbieten; mit besonderem Augenmerk auf jede Art von Strafverfolgungs-, Kriminalermittlungs-, Grenzkontroll- und Nachrichtendiensten;
  - ii. den Einsatz dieser Technologien durch private Stellen in öffentlichen Räumen, öffentlich zugänglichen Räumen und öffentlichen Unterkünften – wo ein solcher Einsatz eine Massenüberwachung oder diskriminierende gezielte Überwachung ermöglichen könnte, verbieten, einschließlich, aber nicht beschränkt auf den

Einsatz in Parks, Schulen, Bibliotheken, Arbeitsplätzen, Verkehrsknotenpunkten, Sportstadien und Wohnanlagen;

- iii. staatlichen Stellen, insbesondere Strafverfolgungsbehörden, die Nutzung von und den Zugriff auf Daten und Informationen, die aus der Nutzung dieser Technologien durch private Unternehmen und andere private Akteure abgeleitet werden, verbieten, es sei denn, dies geschieht zu Zwecken von Audits oder Compliance-Kontrollen;
  - iv. Personen vor dem Einsatz dieser Technologien schützen, wenn dieser in Zusammenhang mit Entscheidungen bezüglich ihrer wirtschaftlichen, sozialen und kulturellen Rechte erfolgt, einschließlich Wohnen, Beschäftigung, Sozialleistungen und Gesundheitsversorgung;
  - v. die Verwendung dieser Technologien und der daraus abgeleiteten Informationen als Beweismittel ausschließen, um Menschen strafrechtlich zu verfolgen oder anzuklagen, um sie zu inhaftieren oder anderweitig festzuhalten; und
  - vi. den staatlichen Zugriff auf biometrische Informationen, die von privaten Unternehmen gespeichert werden, einschränken;
- c. Regeln und Vorschriften aufstellen, die die Beschaffung dieser Technologien durch Regierungs- und staatliche Stellen für Verwendungszwecke verbieten, die eine Massenüberwachung und diskriminierende gezielte Überwachung ermöglichen;
- d. den Einsatz von Gesichtserkennungs- und biometrischen Fernidentifizierungssystemen zur Massenüberwachung oder diskriminierenden gezielten Überwachung religiöser, ethnischer und rassifizierter Minderheiten sowie politischer Dissident:innen und anderer Randgruppen beenden;
- e. die Offenlegung des Einsatzes dieser Technologien gegenüber denjenigen Personen fordern, die ihnen unwissentlich ausgesetzt waren und denen keine Möglichkeit gegeben wurde, ihr Recht auf ein ordnungsgemäßes Verfahren zur Anfechtung des Einsatzes der Technologie auszuüben; und
- f. angemessene Wiedergutmachung für Personen leisten, die durch den Einsatz dieser Technologien geschädigt wurden;

---

2. **Gerichte und Justizbeamte** die existenziellen Bedrohungen für Menschenrechte anerkennen, die sich aus der Nutzung dieser Technologien ergeben, und handeln, um die durch ihre Nutzung verursachten Schäden zu verhindern und, wenn nötig, zu beheben; und

---

3. **Verwaltungsbehörden**, einschließlich Datenschutz- und Verbraucherschutzbehörden, ihre volle Autorität zum Schutz der Privatsphäre und der Verbraucherrechte nutzen, einschließlich der Aufforderung an Unternehmen, den Einsatz dieser Technologien zu stoppen.

---

Schließlich erkennen wir an, dass die existenzielle Bedrohung, die von Gesichtserkennungs- und biometrischen Fernidentifizierungssystemen ausgeht, nicht nur von Ländern und Regierungen aller Art, sondern auch von anderen wichtigen Akteuren auf internationaler und nationaler Ebene angegangen werden sollte.

Aus diesem Grund rufen wir zu Folgendem auf:

---

**1. Internationale Organisationen, wie das Büro des Hochkommissars der Vereinten Nationen für Menschenrechte (OHCHR)**, sollten die derzeitige Entwicklung und Nutzung von Gesichtserkennungs- und biometrischen Fernidentifizierungssystemen zur Überwachung von Gemeinschaften auf der ganzen Welt verurteilen;

---

**2. Private Einrichtungen**, die Gesichtserkennungs- und biometrische Fernidentifizierungssystemen entwickeln oder einsetzen, sollten:

- a. sich öffentlich verpflichten, die Entwicklung, den Verkauf und den Einsatz von Gesichtserkennungs- und biometrischen Fernidentifizierungssystemen einzustellen, die Massenüberwachung und diskriminierende, gezielte Überwachung ermöglichen;
- b. die Produktion von Technologien zur Gesichtserkennung und biometrischen Fernerkennung, die Massenüberwachung und diskriminierende gezielte Überwachung ermöglichen, unverzüglich einstellen und alle unrechtmäßig erworbenen biometrischen Daten, die zum Aufbau von Datenbanken verwendet werden, sowie alle Modelle oder Produkte, die auf solchen Daten aufbauen, löschen;
- c. Transparenzberichte herausgeben, die alle ihre öffentlichen Aufträge (einschließlich derer, die ausgesetzt sind, laufen oder in Vorbereitung sind) für die Bereitstellung dieser Technologien detailliert aufführen; und
- d. eng mit Arbeitnehmer:innen zusammenarbeiten, die sich an ihrem Arbeitsplatz organisieren, um die Entwicklung von Gesichtserkennungs- und biometrischen Fernidentifizierungssystemen, die eine Massenüberwachung und diskriminierende gezielte Überwachung ermöglichen, anzufechten. Sie sollten ferner von Vergeltungsmaßnahmen gegen Arbeitnehmer:innen absehen, die sich an ihren Arbeitsplätzen organisieren, um die Entwicklung von Gesichtserkennungs- und biometrischen Fernidentifizierungssystemen, die Massenüberwachung und diskriminierende gezielte Überwachung ermöglichen, anzufechten oder abzulehnen;

---

**3. Beschäftigte von Technologieunternehmen** sollten sich mit der Unterstützung ihrer Gewerkschaften an ihren Arbeitsplätzen gegen die Entwicklung oder den Verkauf von Gesichtserkennungs- und biometrischen Fernerkennungs-Technologien organisieren, soweit dies möglich ist;

---

**4. Investor:innen und Finanzinstitutionen** sollen:

- a. eine menschenrechtliche Sorgfaltspflicht bei ihren laufenden und zukünftigen Investitionen in Unternehmen, die Gesichtserkennungs- und biometrische Fernerkennungs-Technologien entwickeln und verkaufen, durchzuführen, um herauszufinden, wo diese Technologien mit den Menschenrechten unvereinbar sind und Massenüberwachung und diskriminierende gezielte Überwachung ermöglichen; und,
- b. die Unternehmen, in die sie investieren, dazu aufzufordern, die Schaffung, Entwicklung, den Verkauf oder die anderweitige Bereitstellung dieser Technologien einzustellen, um Massenüberwachung und diskriminierende gezielte Überwachung zu verhindern;

---

**5. Geberorganisationen** werden aufgerufen, die Finanzierung von Rechtsstreitigkeiten und die Interessenvertretung durch Nichtregierungs- und zivilgesellschaftliche Organisationen zu gewährleisten, die vor Gericht Wiedergutmachung für Schäden fordern, und sich aktiv an der

Politikgestaltung auf lokaler, staatlicher, provinzieller, nationaler, föderaler, supranationaler, regionaler und internationaler Ebene beteiligen.

---

## Schlussfolgerung

Wir bitten die Zivilgesellschaft, Aktivist:innen, Akademiker:innen und andere Interessenvertreter:innen aus der ganzen Welt, diesen Brief zu unterzeichnen und sich dem Kampf anzuschließen, um sicherzustellen, dass der Einsatz dieser Technologien in öffentlich zugänglichen Räumen jetzt und für immer verboten wird, damit Menschenrechte und bürgerlichen Freiheiten geschützt werden.

Wenden Sie sich an [banBS@accessnow.org](mailto:banBS@accessnow.org), um weitere Informationen darüber zu erhalten, wie Sie diese Initiative unterstützen können, und besuchen Sie [accessnow.org/ban-biometric-surveillance](https://accessnow.org/ban-biometric-surveillance), um die vollständige Liste der Unterzeichner:innen zu sehen und Ihren Namen der Liste hinzuzufügen.

Diese Erklärung wurde von Access Now, Amnesty International, European Digital Rights (EDRI), Human Rights Watch, Internet Freedom Foundation (IFF) und dem Instituto Brasileiro de Defesa do Consumidor (IDEC) verfasst.