

/ Positionspapier

Verbot des Einsatzes von biometrischen Erkennungssystemen im öffentlich zugänglichen Raum

/ Hintergrund

Was sind biometrische Erkennungssysteme?

Biometrische Erkennungssysteme werden einerseits zur *Authentifizierung* von Individuen eingesetzt (one-to-one matching). Ein Beispiel dafür ist der Abgleich von biometrischen Daten, wie er bei der Grenzkontrolle am Flughafen Zürich eingesetzt wird.¹ Hierfür wird nicht zwingend auf eine Datenbank zurückgegriffen, sondern z.B. der Pass einer Person mit ihrem Gesicht abgeglichen und verifiziert. Auch Private verwenden Systeme zur Authentifizierung, etwa zur Kontrolle des Covid-Zertifikates in Hotels² oder als Zutrittsregelung für Mitglieder von Fitnesszentren. **Andererseits kommen biometrische Erkennungssysteme auch zur *Identifizierung eines Individuums aus einer Masse heraus zum Einsatz (one-to-many matching)*, wobei auf eine Datenbank von biometrischen Daten zurückgegriffen wird. Die folgenden Ausführungen beziehen sich auf diesen zweiten Anwendungsfall.**

Eine immer häufiger verwendete Form biometrischer Erkennungssysteme ist die **Gesichtserkennung**. Es gibt jedoch auch Systeme zur Identifizierung von Personen anhand ihres Ganges, ihrer Augen, ihrer Stimme oder anderer biometrischer Daten.

Wo werden biometrische Erkennungssysteme eingesetzt?

Gesichtserkennungs- und andere biometrische Erkennungssysteme werden heute mit alarmierender Geschwindigkeit in ganz Europa getestet und eingesetzt. Sie sind in Stadien, Flughäfen, Spielcasinos und selbst in Schulen zu finden. Polizeibehörden setzen sie zur Strafverfolgung ein und in mehreren Staaten wurden die Systeme auch während der COVID-19-Pandemie zur Kontrolle von Social Distancing Massnahmen verwendet.³ Auch private Anbieter stellen Systeme zur Verfügung, die als App oder online zur Identifikation von Personen genutzt werden können.

In der Schweiz werden Gesichtserkennungssysteme zu Identifizierungszwecken von einigen Kantonspolizeien zu Strafverfolgungszwecken eingesetzt, so etwa in den Kantonen Aargau, Neuenburg, Schaffhausen, St. Gallen und Waadt.⁴

Eine besondere Herausforderung liegt darin, dass grundsätzlich nur wenig Transparenz darüber besteht, wo und von wem biometrische Erkennungssysteme eingesetzt werden. Dies stellt für eine faktenbasierte öffentliche Debatte zum Thema ein gewichtiges Hindernis dar.

¹ Siehe auch [Regierungsratsbeschluss Nr. 447/2021](#).

² [TagesAnzeiger, 23.11.2021](#).

³ [AlgorithmWatch, AutomatingSociety Report 2020](#); [Digitale Gesellschaft 2021](#); [Ragazzi, Francesco, et al., Biometric and Behavioural Mass Surveillance in EU Member States, Report for the Greens/EFA in the European Parliament, 2021](#).

⁴ [TagesAnzeiger, 17.04.2021](#); [SRF Rundschau 26.01.2022](#).

Rechtliche Ausgangslage

Im revidierten schweizerischen Datenschutzgesetz (nDSG), das 2023 in Kraft tritt, gelten biometrische Daten als besonders schützenswert, sofern sie eine natürliche Person eindeutig identifizieren. **Für die Bearbeitung solcher Daten – beispielsweise durch biometrische Erkennungssysteme – gibt es keine umfassende Erlaubnis:** Für ihre Verwendung ist eine gesetzliche Grundlage (in einem Gesetz im formellen Sinn⁵) erforderlich. **Gleichzeitig existiert aber auch kein explizites Verbot für ihren Einsatz.** Es wäre somit grundsätzlich möglich, die gesetzlichen Grundlagen für die Bearbeitung von besonders schützenswerten Personendaten zu schaffen.

Das nDSG gilt nur für Bundesbehörden und private Akteure. Kantone werden vom nDSG nicht erfasst. Allerdings ist auch für den Einsatz von biometrischen Erkennungssystemen durch kantonale Behörden eine ausreichende gesetzliche Grundlage notwendig. Obwohl umstritten ist, ob die existierenden Rechtsgrundlagen dafür ausreichend sind, **setzen einige Kantone beispielsweise Gesichtserkennungssysteme bereits im Strafverfolgungskontext ein.** Auf dem Gebiet führende Rechtswissenschaftler*innen sind der Auffassung, dass eine solche Grundlagen **nicht gegeben** ist und der Einsatz daher rechtswidrig erfolgt.⁶

Der Grund, warum die Bearbeitung von besonders schützenswerten Daten eine gesetzliche Grundlage in einem Gesetz im formellen Sinne erfordert, liegt darin, dass **eine Bearbeitung solcher Daten durch biometrische Erkennungssysteme als schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) betrachtet wird.** Solch ein Eingriff in die Grundrechte durch Bundesbehörden oder kantonale Behörden kann zudem nur dann gerechtfertigt sein, wenn er auf einer gesetzlichen Grundlage beruht, verhältnismässig ist, durch ein hinreichendes öffentliches Interesse gerechtfertigt ist und den Kern der Grundrechte unberührt lässt (Art. 36 BV).⁷

Seit Beginn der Kampagne [gesichtserkennung-stoppen.ch](https://www.gesichtserkennung-stoppen.ch) wurden **auf kommunaler und kantonomer Ebene mehrere politische** Vorstösse eingereicht, die ein Verbot von biometrischen Erkennungssystemen im öffentlich zugänglichen Raum fordern.

Vorstösse wurden angenommen:

- Gemeinderat Zürich: [Postulat 2021/451](#) und [Motion 2021/450](#)
- Gemeinderat St-Gallen: [Motion](#)
- Grosser Rat Kanton Basel-Stadt: [Anzug 22.5022](#)
- Gemeinderat Lausanne: [Projet de règlement](#); [Projet de règlement](#), [Postulat](#)

Vorstösse sind noch in Bearbeitung:

- Kantonsrat Zürich: [Motion 2022/1473](#)
- Grosser Stadtrat Luzern: [Motion](#)

/ Warum fordern wir ein Verbot?

- / **Erstens können Gesichtserkennungssysteme oft diskriminierend wirken, da sich gezeigt hat, dass sie beispielsweise Menschen dunkler Hautfarbe oder Frauen weniger gut erkennen.** Dies führt bei diesen Gruppen zu einer höheren Anzahl an falschen positiven Treffern – was, zum Beispiel im Strafverfolgungskontext, relevante Auswirkungen

⁵ Ein Gesetz im formellen Sinne meint ein durch das Parlament im Gesetzgebungsprozess als Gesetz beschlossener Erlass.

⁶ [Plädoyer, 02.12.2021](#), Simmler Monika & Canova Giulia, Gesichtserkennungstechnologie: Die «smarte» Polizeiarbeit auf dem Prüfstand, Sicherheit & Recht 3/2021, 105.

⁷ [Interpellation Glättli/N, 21.3580](#).

auf Individuen haben kann. Grund dafür ist, dass die Daten, mit denen die Systeme trainiert wurden, nicht repräsentativ sind bzw. überproportional Daten von Menschen weisser Hautfarbe und Männern enthalten.

- / Gleichzeitig ist es aber so, dass eine Verbesserung der Genauigkeit auf technologischer Ebene die Problematik nicht beseitigt. Denn, zweitens, **kann der Einsatz von biometrischen Erkennungssystemen zur Identifizierung von Personen im öffentlich zugänglichen Raum eine biometrische Massenüberwachung ermöglichen, die im Kern mit Grundrechten wie der Privatsphäre, der Meinungsäusserungs- und der Versammlungsfreiheit in Konflikt steht.** Diese biometrische Massenüberwachung, die unsere Grundrechte bedroht und fundamentale demokratische Prinzipien unterwandert, gilt es zu verhindern.

Biometrische Massenüberwachung bezeichnet das anlasslose, unterschiedslose oder stichprobenartige Beobachten, Verfolgen und sonstige Verarbeiten von biometrischen Daten von Individuen oder Gruppen im öffentlich zugänglichen Raum. **Wenn Menschen im öffentlichen Raum jederzeit identifiziert und überwacht werden können, verletzt dies nicht nur ihr Recht auf Privatsphäre, sondern hat auch eine abschreckende Wirkung, die sie vom Wahrnehmen anderer Grundrechte wie der Meinungsäusserungs- oder Versammlungsfreiheit abhält.** Das heisst, sie werden möglicherweise davon abgeschreckt, an Demonstrationen teilzunehmen oder bestimmte Lokale aufzusuchen, die beispielsweise Hinweise auf ihre politische Gesinnung oder sexuelle Orientierung geben könnten. Für bereits benachteiligte oder von Diskriminierung betroffene Personen und Gruppen sowie für politische Aktivist*innen zeigen sich diese Auswirkungen von biometrischer Massenüberwachung typischerweise in verstärkter Form.

Bereits das Vorhandensein dieser technischen Infrastruktur im öffentlich zugänglichen Raum schafft die Voraussetzungen, um eine solche biometrische Massenüberwachung vorzunehmen. Für Einzelpersonen ist nicht ersichtlich, in welchen Situationen, in welchem Ausmass und von welchen Akteuren eine biometrische Erkennung vorgenommen wird, so dass die erwähnten abschreckenden Effekte auf die Grundrechte sich auch dann zeigen, wenn einzelne Personen in einer bestimmten Situation vom System gar nicht erfasst und identifiziert werden. Das heisst, selbst wenn ein vorhandenes System nur in sehr eng begrenzten Szenarien tatsächlich zur Identifizierung von Personen verwendet werden würden: Die Möglichkeit, dass dies jederzeit ohne Wissen der Betroffenen (und unter Umständen auch nachträglich) geschehen könnte, bedeutet, dass die Bevölkerung im öffentlichen Raum jederzeit damit rechnen muss, identifiziert zu werden. Dies kann ihr Verhalten konditionieren, also dazu führen, dass die Menschen ihre Aktivitäten und Bewegungen im öffentlichen Raum entsprechend anpassen. Aus diesem Grund hätte bereits das Schaffen der Möglichkeit ein erhebliches Potential, sie in der Ausübung von Grundrechten wie der Versammlungs- und Meinungsäusserungsfreiheit schwerwiegend zu beeinträchtigen.

Der Einsatz von biometrischen Erkennungssystemen zu Identifizierungszwecken im öffentlich zugänglichen Raum kann somit nicht auf grundrechtskonforme Weise geschehen, sondern ist inhärent inkompatibel mit zentralen, auf Verfassungsebene sowie international garantierten Menschenrechten. Die Freiheiten, die von biometrischer Massenüberwachung bedroht sind, sind für die Teilnahme am öffentlichen Leben und am öffentlichen Diskurs in einer demokratisch organisierten Gesellschaft unabdingbar. Biometrische Massenüberwachung stellt somit nicht nur einen Eingriff in die Grundrechte der Überwachten dar, sondern **beschädigt auch die demokratische Öffentlichkeit als Ganzes.** Die Einschränkungen der Grundrechte, die biometrische

Erkennungssysteme im öffentlichen Raum mit sich bringen würden, sind damit **nicht verhältnismässig**.

/ Forderungen

- / **Wir fordern ein Verbot des Einsatzes von biometrischen Erkennungssystemen zu Identifizierungszwecken im öffentlich zugänglichen Raum der Schweiz. Dieser kann eine anlasslose, willkürliche oder gezielt diskriminierende biometrische Massenüberwachung ermöglichen, die nicht mit unseren Grundrechten vereinbar ist.**
 - Diese Forderung umfasst den Einsatz durch **jegliche Art von Akteuren** im öffentlich zugänglichen Raum, d.h. sowohl öffentliche Behörden als auch private Akteure.
 - Die Forderung bezieht sich sowohl auf den Einsatz von **Echtzeit-Erkennungssystemen** als auch auf den **nachträglichen Einsatz** von biometrischen Erkennungssystemen auf Foto- oder Videoaufnahmen.
 - Die Forderung nach einem Verbot bezieht sich insbesondere auf **Fern-Erkennungssysteme**, da durch diese Personen unwissentlich überwacht werden und sich so die abschreckenden Effekte kontinuierlich zeigen – unabhängig davon, ob eine Überwachung tatsächlich gerade stattfindet. Das Verbot soll aber auch andere biometrische Erkennungssysteme erfassen, wenn ihr Einsatz im öffentlichen Raum das Potential zur Massenüberwachung mit sich bringt.
 - Diese Forderung umfasst den **öffentlich zugänglichen Raum**, das heisst jenen Raum, der Einzelpersonen ohne weitere Schranken zugänglich ist. Dazu gehören nebst öffentlichen Strassen, Gehwegen und Plätzen auch Parks, der öffentliche Verkehr inklusive Bahnhöfen und Haltestellen, Schulen, Universitäten, Freizeitsportanlagen, Stadien, öffentliche Bibliotheken oder Einkaufszentren. Diese Liste ist exemplarisch und nicht abschliessend zu verstehen.
- / **Dieses Verbot ist sowohl rechtlich flächendeckend zu verankern als auch durch entsprechende politische Entscheide der Entscheidungsträger*innen sicherzustellen.**
 - Beide Prozesse sollen von einer inklusiven, partizipativen und evidenzbasierten **öffentlichen Debatte** begleitet werden, in der wir als Gesellschaft die Möglichkeit haben, diese roten Linien beim Einsatz von biometrischen Erkennungssystemen zu diskutieren und demokratisch zu legitimieren.
- / **Zu diesem Zweck fordern wir die Gemeinden dazu auf, ...**
 - ... ein Verbot des Einsatzes von biometrischen Erkennungssystemen zu Identifizierungszwecken im öffentlich zugänglichen Raum zu erlassen und den Einsatz **durch ihre kommunalen Verwaltungsbehörden rechtlich zu untersagen**.
 - ... den **politischen Entscheid** zu treffen, dafür zu sorgen, dass biometrische Erkennungssysteme zu Identifizierungszwecken im öffentlich zugänglichen Raum auf ihrem Gemeindegebiet nicht zum Einsatz kommen. Auch wenn zum Erlass eines umfassenden rechtlichen Verbots keine ausreichende kommunale Gesetzgebungskompetenz vorhanden ist (da sich z.B. ein Einsatz durch die Polizei auf das kantonale Polizeigesetz stützen würde), sendet dieser politische Entscheid ein wichtiges Signal.⁸

⁸ Vgl. die Verbote in den Städten San Francisco oder Portland OR, siehe unten.

- / **Die Kantone fordern wir auf,**
 - ... sicherzustellen, dass **biometrische Erkennungssysteme zu Identifizierungszwecken im öffentlich zugänglichen Raum nicht zum Einsatz** kommen.
 - ... **davon abzusehen, gesetzliche Grundlagen für den Einsatz biometrischer Erkennungssysteme zu schaffen.**

- / **Auf Bundesebene fordern wir**
 - ... den **Gesetzgeber** auf, ein explizites Verbot des Einsatzes von biometrischen Erkennungssystemen zu Identifizierungszwecken im öffentlich zugänglichen Raum zu erwirken.
 - ... **Exekutive und Verwaltung** auf, sich auch in den relevanten multilateralen Gremien und Verhandlungen für ein solches Verbot einzusetzen.

/ Weitergehende Begründung

Warum reichen die derzeitigen gesetzlichen Grundlagen nicht aus?

Die oben dargelegte rechtliche Ausgangslage zeigt, dass zum heutigen Zeitpunkt der Einsatz von biometrischen Erkennungssystemen zu Identifizierungszwecken im öffentlichen Raum **grundsätzlich in der Schweiz nicht erlaubt ist**. Aus folgenden Gründen erweist sich diese datenschutzrechtliche Regelung allerdings als **nicht ausreichend**:

- **Sie lässt gleichzeitig die beiden Möglichkeiten offen, dass**
 - (i) **die Systeme in Zukunft zum Einsatz kommen, nämlich indem die entsprechenden gesetzlichen Grundlagen geschaffen werden.** Das Datenschutzrecht stellt besondere Anforderungen an den Einsatz biometrischer Erkennungstechnologien, verbietet diese aber nicht grundsätzlich, sondern macht den Einsatz abhängig vom Vorhandensein einer ausreichenden gesetzlichen Grundlage. Aufgrund ihres inhärenten Widerspruchs mit grundrechtlich verbürgten Freiheiten und der Unmöglichkeit, ihren grundrechtskonformen Einsatz sicherzustellen, ist es angezeigt, sie im öffentlich zugänglichen Raum grundsätzlich zu untersagen.
 - (ii) **die Systeme de facto trotzdem zum Einsatz kommen, obwohl die gesetzlichen Grundlagen nicht vorhanden oder nicht ausreichend sind (was gemäss Einschätzung mehrerer Expert*innen heute bereits passiert).** Um Rechtsklarheit zu schaffen und diesen Einsatz im öffentlichen Raum, der eine Massenüberwachung herbeiführen kann, zuverlässig zu verhindern, ist somit ein explizites Verbot angezeigt. Der Gesetzgeber ist angehalten, mit der erforderlichen Klarheit zu verdeutlichen, dass der Einsatz biometrischer Erkennungssysteme im öffentlich zugänglichen Raum nicht rechtens erfolgen kann.

- Wichtig ist hier auch zu erwähnen, dass bei einem erstmaligen Einsatz von neuen Technologien oft zwar zunächst Datenschutzkonformität und der Zweckbindungsgrundsatz eingehalten werden. Ist die technische Infrastruktur, d.h. hier die biometrischen Erkennungssysteme im öffentlich zugänglichen Raum, jedoch einmal vorhanden, **droht oftmals ein «Mission Creep»: Die Technologie wird im Laufe der Zeit und mit zunehmender Etablierung dann doch auch für andere Zwecke und Bedürfnisse eingesetzt.** Da dies einzig eine Anpassung der bereits vorhandenen Rechtsgrundlage bedarf (nicht aber die Schaffung einer neuen Rechtsgrundlage), wird so der ursprüngliche Zweckbindungsgrundsatz doch umgangen. Vor

diesem Hintergrund setzen wir uns dafür ein, dass keine gesetzlichen Grundlagen geschaffen werden, die den Einsatz biometrischer Erkennungssysteme erlauben würden.

- Neue Technologien können oftmals in **Pilotversuchen** getestet werden, was vorübergehend ohne entsprechende Rechtsgrundlage zulässig ist. **Nach einer Einführung im Rahmen eines Pilotprojektes fällt der Schritt zur definitiven Verankerung jedoch leichter und wird öffentlich weniger wahrgenommen und kaum diskutiert.** Die Risiken, die mit dem Einsatz biometrischer Erkennungssysteme verbunden sind, wiegen zu schwer, um die Gefahr einer solchen schleichenden Einführung durch die Hintertür akzeptieren zu können.
- **Die Risiken gehen über datenschutzrechtliche Aspekte hinaus.** Biometrische Massenüberwachung bedroht eben auch die Privatsphäre als solches sowie die Meinungsäusserungs- und Versammlungsfreiheit. Eine Datenschutzbehörde ist für datenschutzrechtliche Vorgaben, nicht jedoch für eine generelle Folgenabschätzung bezüglich der Auswirkungen auf Grundrechte, Demokratie und Gemeinwohl zuständig. Diese Risiken können von der datenschutzrechtlichen Prüfung nicht abgedeckt werden.

Warum soll biometrische Erkennung nicht gezielt zur Strafverfolgung genutzt werden können?

Das an sich legitime Bedürfnis nach Sicherheit darf nicht dazu führen, dass Grundrechte ausgehöhlt werden. Dem staatlichen Handeln werden aus guten Gründen – auch bei der Strafverfolgung und dem Schutz der öffentlichen Sicherheit – grundrechtliche Schranken gesetzt. Straftaten müssen polizeilich und juristisch verfolgt und die öffentliche Sicherheit geschützt werden können – aber dies darf nur mittels geeigneter und verhältnismässiger Massnahmen erfolgen. Dem Staat stehen dafür bereits heute umfassende Mittel zur Verfügung. Eine Einschränkung von Grundrechten kann zu diesem Zweck nur rechtfertigbar sein, wenn sie auf einer gesetzlichen Grundlage beruht, im öffentlichen Interesse geschieht, verhältnismässig ist und den Kern der Grundrechte unberührt lässt (Art. 36 BV).

Der Einsatz von automatischer Gesichtserkennung und anderen biometrischen Überwachungssystemen zur Identifizierung im öffentlichen Raum ermöglicht jedoch eine biometrische Massenüberwachung, die, wie oben dargelegt wurde, über eine rechtfertigbare und verhältnismässige Einschränkung von Grundrechten hinaus geht. Dies sprengt damit den Rahmen, innerhalb dessen Massnahmen die Sicherheit erhöhen, ohne dabei unsere Freiheit zu gefährden und unsere Rechte unverhältnismässig einzuschränken.

Gegen den Einsatz biometrischer Erkennungssysteme in der Strafverfolgung spricht auch, dass diese nie fehlerfrei funktionieren. So erkennen beispielsweise Gesichtserkennungssysteme dunkelhäutige und weibliche Gesichter in der Tendenz weniger gut. Das führt dazu, dass diese Menschen öfter verwechselt werden, dass es also zu sogenannten **«falsch positiven» Treffen** kommt, bei denen das System meldet, eine Person identifiziert zu haben, tatsächlich aber eine falsche Identität erkennt. Für die so fälschlicherweise erkannten Menschen kann das gravierende Auswirkungen haben – von einer ungerechtfertigten Kontrolle, der irrtümlichen Verdächtigung, bis hin zur willkürlichen Festnahme.

Warum reicht ein Moratorium nicht aus?

Ein Moratorium ist nicht ausreichend, um die Gefahr einer biometrischen Massenüberwachung abzuwenden. Einerseits macht die automatische Gesichtserkennung zwar langsame Fortschritte, wird jedoch kaum je völlig fehlerfrei funktionieren. Andererseits – und das ist zentral – sind zwar bei der Treffergenauigkeit und Zuverlässigkeit der Technologie Verbesserungen zu

erwarten, diese ändern aber nichts an der Tatsache, dass selbst ein absolut verwechslungsfreier Einsatz Grundrechte verletzen würde. Technische Weiterentwicklungen würden die Systeme nur zu noch effektiveren Überwachungsinstrumenten machen. Im öffentlich zugänglichen Raum eingesetzt schränken sie die Grundrechte unverhältnismässig ein, auch – oder gerade wenn – sie genauer funktionieren.

Was tut sich anderswo?

Aufgrund der **rasanten Zunahme von biometrischen Erkennungssystemen in ganz Europa** ist zu erwarten, dass sich diese Entwicklung ohne gesetzgeberische und zivilgesellschaftliche Interventionen auch in der Schweiz fortsetzen würde.

- Verschiedene **Städte weltweit**, darunter San Francisco, Portland OR, oder Nantes haben den Einsatz von Gesichtserkennungssystemen im öffentlichen Raum verboten.
- Seit Februar 2021 ruft auch eine Koalition von zivilgesellschaftlichen Organisationen unter dem Namen **«Reclaim Your Face»** zu einem Verbot in Europa auf. Auf EU-Ebene tut sie dies u.a. im Rahmen einer Europäischen Bürgerinitiative.
- Im Juni 2021 hat sich eine internationale Koalition von über 200 zivilgesellschaftlichen Organisationen unter dem Namen **«Ban Biometric Surveillance»** in einem offenen Brief für ein entsprechendes Verbot ausgesprochen.⁹
- Auf **EU-Ebene** verbietet die **Datenschutzgrundverordnung** grundsätzlich die Verarbeitung biometrischer Daten, die eine Person eindeutig identifizieren, wobei eine Reihe von Ausnahmen vorgesehen sind (Art. 9). Die **Strafverfolgungsrichtlinie** lässt sie unter bestimmten Bedingungen für Strafverfolgungszwecke zu (Art. 10). Im April 2021 hat die Europäische Kommission ihren Entwurf für eine **Verordnung zu Künstlicher Intelligenz (AI Act)** vorgelegt. Sie schlägt vor, den Einsatz von biometrischen Fernerkennungssystemen in Echtzeit im öffentlichen Raum durch Strafverfolgungsbehörden zu verbieten, wobei eine Reihe von Ausnahmen vorgesehen sind. Die KI-Verordnung wird derzeit im EU-Parlament und im EU-Rat verhandelt. Im Oktober 2021 hat sich das **Europäische Parlament in einem nicht-bindenden Bericht** für ein Verbot des Einsatzes von biometrischen Erkennungssystemen durch Strafverfolgungsbehörden im öffentlich zugänglichen Raum ausgesprochen.
- Im September 2021 hat sich auch das **UNO-Hochkommissariat für Menschenrechte** in einem **Bericht** dafür ausgesprochen, die Verwendung von biometrischen Erkennungssystemen im öffentlich zugänglichen Raum wesentlich einzuschränken oder zu verbieten.
- Im Dezember 2021 hat sich die neue **Regierungskoalition in Deutschland** in ihrem **Koalitionsvertrag** dafür ausgesprochen, «biometrische Erkennung im öffentlichen Raum (...) europarechtlich auszuschließen».

Kampagne gesichtserkennung-stoppen.ch

Es ist entscheidend, dass die Leitplanken und roten Linien Einsatz von biometrischen Erkennungssystemen im Rahmen eines gesellschaftspolitischen Diskurses festgelegt und klare Regeln geschaffen werden, bevor diese im breiten Stil eingesetzt werden.

Vor diesem Hintergrund haben die drei zivilgesellschaftlichen Organisationen **AlgorithmWatch Schweiz**, **Amnesty International Schweiz** und **Digitale Gesellschaft Schweiz** die Kampagne **gesichtserkennung-stoppen.ch** ins Leben gerufen.

⁹ Auch die drei Trägerorganisationen der Kampagne gesichtserkennung-stoppen.ch sind Mitglied der «Reclaim Your Face» Koalition und haben den offenen Brief «Ban Biometric Surveillance» mitunterzeichnet.

Die Kampagne wird von [Personen aus Politik, Zivilgesellschaft und Wissenschaft](#) unterstützt.

Weitere Informationen: www.gesichtserkennung-stoppen.ch | office@gesichtserkennung-stoppen.ch