GMS GESELLSCHAFT MINDERHEITEN IN DER SCHWEIZ
SOCIETE POUR LES MINORITES EN SUISSE
SOCIETA PER LE MINORANZE IN SVIZZERA
SOCIETAD MINORITADS EN SVIZRA

GMS Standpunkt

24. August 2022

Der folgende Text wurde von Angela Müller, Head of Policy & Advocacy bei AlgorithmWatch Schweiz, verfasst. Er erschien erstmals unter dem Titel «Gesichtserkennung im öffentlichen Raum gehört verboten» als Gastbeitrag in der NZZ am Sonntag vom 17. Juli 2022. Für die Veröffentlichung als GMS-Standpunkt wurde er an einigen Stellen leicht ergänzt.

Warum wir Gesichtserkennung in einer Demokratie nicht wollen können

Wenn der öffentliche Raum mit Hilfe von Gesichtserkennung oder anderen biometrischen Erkennungssystemen überwacht wird, ist das eine Gefahr für die Grundrechte. Und für die Demokratie.

In der Ukraine hilft eine Technologie zur Gesichtserkennung dabei, Vermisste zu suchen oder Tote zu identifizieren, wie der Vizeregierungschef kurz nach Kriegsbeginn bestätigte. Der Konzern Clearview.AI stellt dem Land das entsprechende System kostenlos zur Verfügung. Russland nutzt solche Technologien über den militärischen Kontext hinaus. In Moskau können nicht nur Metro-Tickets via Gesichtsscan bezahlt werden. Die fast 200 000 Überwachungskameras der Metropole dienen auch dazu, Demonstrierende bei Protesten, etwa zur Unterstützung des Oppositionellen Alexei Nawalny, zu identifizieren.

Russland und die Ukraine sind nicht allein. In ganz Europa werden heute biometrische Fern-Erkennungssysteme eingesetzt – auch im zivilen Kontext. Gemeint sind damit nicht Systeme zur Authentifizierung, mit denen wir etwa das Smartphone entsperren, sondern Systeme, die uns anhand unserer biometrischen Daten, wie dem Gesicht oder der Stimme, aus einer Masse heraus identifizieren können, indem sie auf eine Datenbank zurückgreifen. In der Schweiz werden diese Systeme von einigen Polizeikorps verwendet. Auch Fussballstadien und Supermärkte liebäugeln damit.

Auf den ersten Blick scheint dies ein Instrument zu sein, das wir für eine effizientere Strafverfolgung und für die Gewährleistung von Sicherheit nutzen sollten. Doch so einfach ist die Sache nicht. In den USA wurden etwa mehrere Menschen irrtümlich verhaftet, weil ein Gesichtserkennungssystem sie falsch identifiziert hatte. Oft handelt es sich dabei um dunkelhäutige Menschen. Deren Gesichter sind in den Trainingsdaten, mit denen die Systeme entwickelt wurden, oft untervertreten – mit der Folge, dass die Systeme dunkelhäutige Gesichter weniger gut erkennen. Dasselbe gilt für nicht-männliche Gesichter.

Eine Verbesserung der Technologie löst das Problem aber nicht. Denn unabhängig davon, wie gut oder schlecht sie funktioniert: Wenn sie im öffentlich zugänglichen Raum eingesetzt wird, wenn auf öffentlichen Plätzen, in Bahnhöfen, Stadien oder Einkaufszentren die Infrastruktur vorhanden ist, um Personen jederzeit automatisiert zu identifizieren, berührt das uns und unsere demokratische Öffentlichkeit im Kern. Es verletzt nicht nur unser aller Recht auf Privatsphäre, sondern kann uns auch davon abhalten, unsere Meinung zu äussern oder uns zu versammeln.

Das blosse Wissen, dass wir potenziell erkannt – und damit verfolgt und überwacht – werden könnten, wird unser Verhalten konditionieren: Es kann uns davon abschrecken, Orte oder Anlässe aufzusuchen, die Hinweise auf unsere politische Gesinnung, sexuelle Orientierung oder Religion geben könnten. Quellen könnten davor zurückweichen, Journalist:innen zu treffen, Mandatsträger:innen könnten auf private Treffen verzichten, Sans-Papiers den öffentlichen Raum gänzlich meiden. Ob in einer bestimmten Situation eine tatsächliche Überwachung erfolgt oder nicht, ist dafür nicht einmal entscheidend – da die Systeme aus der Ferne funktionieren, ist für uns nicht ersichtlich, wann und wo sie zum Einsatz kommen. Dazu kommt: Typischerweise sind bereits benachteiligte, von Diskriminierung betroffene Menschen und

Angehörige von Minderheiten vermehrt Überwachungsmassnahmen ausgesetzt – etwa werden diese in Nachbarschaften mit einer hohen Verbrechensrate öfters eingesetzt. Deren Bewohner:innen wären entsprechend auch verstärkt von den Folgen biometrischer Überwachung betroffen. Dasselbe gilt für Menschen, die sich politisch exponieren.

Müssen wir diese Massnahmen allenfalls trotzdem in Kauf nehmen – im Interesse der öffentlichen Sicherheit? Die Gewährleistung von Sicherheit ist eine staatliche Kernaufgabe. Dem staatlichen Handeln sind allerdings Schranken gesetzt – aus guten Gründen. Es gäbe einige Mittel, welche die Strafverfolgung effizienter machen könnten – und die von autoritären Staaten auch gerne eingesetzt werden: Sie reichen von der Nutzung invasiver Technologien bis hin zur Folter. In einem liberalen Rechtsstaat ist jedoch der Orientierungspunkt klar: Es sind die verfassungsmässig geschützten Grundrechte, die uns zeigen, wo die Linie zu ziehen ist und welcher Mittel sich der Staat bedienen darf – und welcher eben nicht, weil sie mit unserer Freiheit, Autonomie und Würde nicht vereinbar sind. Im öffentlichen Raum schränken Gesichtserkennungssysteme unsere Grundrechte auf eine Weise ein, die nicht verhältnismässig ist – und berühren damit auch die Teilnahme am öffentlichen Leben und Diskurs, was für eine gesunde Demokratie unabdingbar ist.

Ein Verbot von biometrischen Systemen zur Identifikation im öffentlich zugänglichen Raum ist angezeigt. Vor diesem Hintergrund ist auch die Zivilgesellschaft aktiv geworden. Auf europäischer Ebene wirbt die Kampagne «Reclaim Your Face» für ein EU-weites Verbot, international fordern über 200 Organisationen ein globales Verbot. In der Schweiz haben die NGOs AlgorithmWatch Schweiz, Amnesty International und die Digitale Gesellschaft die Kampagne «Gesichtserkennung stoppen» lanciert, um ein Verbot von biometrischer Erkennung im öffentlich zugänglichen Raum zu erwirken. Eine erste Petition wurde von über 10 000 Personen unterzeichnet. Politiker:innen von links bis rechts haben den Handlungsbedarf erkannt und unterstützen die Kampagne. Seit ihrem Beginn wurden etwa in Zürich, Lausanne oder Basel Vorstösse für ein solches Verbot eingereicht, die auch bereits Wirkung zeigten: So will die Stadt Zürich biometrische Identifizierungssysteme für ihre Behörden verbieten.

Wollen wir alle, als Einzelpersonen und als Gesellschaft, von der Nutzung neuer Technologien profitieren, müssen wir gemeinsam Rahmenbedingungen dafür gestalten – und da rote Linien ziehen, wo die Technologie uns nicht mehr nützt, sondern schadet. Mit Gesichtserkennung im öffentlichen Raum würden Voraussetzungen geschaffen für etwas, was wir nicht wollen können – weder für uns selbst noch für unsere Demokratie.

Dr. iur. des. Angela Müller, Head of Policy & Advocacy, AlgorithmWatch Schweiz
Angela Müller leitet den Bereich Policy & Advocacy bei AlgorithmWatch Schweiz, einer Non-Profit-Organisation, die sich mit den Auswirkungen algorithmischer Systeme auf Mensch und Gesellschaft beschäftigt und sich dafür einsetzt, dass deren Nutzung Grundrechte, Demokratie und Rechtsstaatlichkeit achtet. Sie hat politische Philosophie studiert und eine rechtswissenschaftliche Dissertation zum Thema Menschenrechte im Kontext von Globalisierung und neuen Technologien verfasst.

Die GMS Gesellschaft Minderheiten in der Schweiz wurde 1982 gegründet von Sigi Feigel und Alfred A. Häsler, ist politisch und religiös neutral und setzt sich für Leben, Recht, Kultur und Integration alter und neuer Minderheiten in der Schweiz ein. Sie steht allen offen, die für Minderheiten eintreten (http://www.gms-minderheiten.ch).

Rückfragen an infogms@gra.ch.