Ich kenne dich!

Gesichtserkennung. Während Echtzeit-Überwachung weltweit immer häufiger zum Einsatz kommt, wird über die rechtlichen Rahmenbedingungen oft erst nachgedacht.

Im Jänner 2020 ließ eine Meldung Datenschützer aufhorchen. Das Start-up Clearview AI hatte eine riesige Datenbank zur Gesichtserkennung aufgebaut. Klammheimlich hatte das Unternehmen aus dem Silicon Valley über drei Milliarden Fotos von Personen aus dem Netz gesaugt. Es bediente sich (und tut dies noch immer) vornehmlich in Sozialen Netzwerken wie Facebook, Instagram oder YouTube. Über eine Smartphone-App konnten Nutzer die Bilder auch selbst hochladen. Der Algorithmus glich sie mit dem bestehenden Material ab – und spuckte dann aus, was er zu bieten hatte: weitere Bilder der Person und Informationen über sie.

Spionieren, angeben, Spaß haben

Der Firmengründer Hoan Ton-That reagierte. Er machte die Datenbank für die Öffentlichkeit wieder unzugänglich und ließ ausrichten, dass der Dienst nur mehr amerikanischen Behörden zur Verbrechensbekämpfung zur Verfügung stünde. Doch US-Medien deckten auf, dass der Australier es mit der Wahrheit nicht so genau genommen hatte. Bald wurde bekannt, dass auf der Kundenliste auch Organisationen autokratischer Regimes im Nahen Osten und Unternehmen standen. Etlichen Privatleuten soll es dadurch möglich gewesen sein, die Datenbank zu nutzen. Ein Besitzer einer US-Handelskette etwa spionierte den neuen Freund seiner Tochter mithilfe von Clearview aus. Ein anderer vermögender Herr wiederum prahlte auf einer Party mit dem Programm. Er hielt anderen Gästen sein Handy vor die Nase und erklärte, dass er nun ganz einfach Dinge über sie herausfinden könne. Geschäftsleute wurden, offenbar in der Hoffnung auf eine Firmenbeteiligung, mit kostenlosen Testversionen geködert und nutzten sie zum Spionieren, Angeben und um Spaß zu haben.
Der Fall zeigt: Technisch gesehen ist die Überwachung von Personen durch künstliche Intelligenz bereits möglich – zumal auch die Großen der Branche längst an vergleichbaren Technologien arbeiten.

Tech-Konzerne mischen mit

Amazon etwa hat eine Software namens Rekognition entwickelt. Ihre Stärke ist, dass sie Gesichter aus den unterschiedlichsten Winkeln erkennt. Viele Überwachungskameras liefern ja von oben aufgenommene Bilder. Auch Microsoft hat sein eigenes System. Von IBM wurde bekannt, dass das Unternehmen über 100 Millionen Bilder der privaten Datenbank Flickr ohne Zustimmung der Nutzer analysiert hatte – offenbar, um die Algorithmen zu trainieren. Im Sommer 2020 verlautbarte IBM allerdings, die Geschäftssparte aufzugeben. Anders bei Facebook: Das Soziale Netzwerk unterhält schon seit Jahren eine Software zur automatischen Gesichtserkennung. In den USA musste Facebook deswegen bereits Strafen in Millionenhöhe bezahlen und liefert sich ein Katz-und-Maus-Spiel mit den Behörden. Erst deaktiviert Zuckerbergs Netzwerk die Programme, dann setzt es sie wieder ein. In der EU ließ sich Facebook den Einsatz der Technologie perfiderweise im Zuge des Inkrafttretens der neuen Datenschutzgrundverordnung (DSGVO) erlauben. Damals wurden den Nutzern die neuen, der DSGVO angepassten Bedingungen zur Einwilligung vorgelegt – mit einer klitzekleinen Klausel im Text, die auf den Einsatz der Gesichtserkennung hinwies.
Google dagegen hält sich auf dem Gebiet zurück. Es sei voller Risiken, erklärte Unternehmenschef Sundar Pinchai und forderte Regierungen auf, rasch Regeln zum Einsatz dieser Technologie aufzustellen.

EU: Gesetzesentwurf

Die EU hat sich der Sache bereits angenommen. Die EU-Kommission prüft den Entwurf eines Arbeitspapieres über den Umgang mit künstlicher Intelligenz. Darin vorgesehen ist auch ein Verbot des Einsatzes automatisierter Gesichtserkennung – sprich: Massenüberwachung im öffentlichen Raum – für die nächsten drei bis fünf Jahre. Bis dahin, so heißt es, sollten die Auswirkungen der Technologie besser eingeschätzt werden können.
Einzelne Staaten testen derweil, wo und wie ihnen die sogenannte Face Recognition Technology nützlich sein kann. Die österreichische Polizei etwa hat mit 1. August 2020 still und leise eine Gesichtserkennungs-Software in den Regelbetrieb aufgenommen. Nach einem Monat Probephase kommt nun das System der deutschen Firma Cognitec Systems in der EDV des Bundesministeriums für Inneres zur Anwendung, 2021 sollen auch die Landeskriminalämter Zugriff erhalten. Konkret heißt das, dass die Polizei bei schweren Straftaten wie Banküberfällen Fotos aus Videos der Überwachungskameras generiert. Die neue Software misst bestimmte Merkmale in den Gesichtern und gleicht sie dann mit den Datenbanken der Polizei ab.

Deutschland rudert zurück

In Deutschland gab es Anfang 2020 einen Gesetzesentwurf, der einen Schritt weiter Richtung Echtzeitüberwachung ging. Dieser sollte der Polizei eine automatisierte Gesichtserkennung an Orten wie Bahnhöfen oder Flughäfen ermöglichen. Ziel war es, Menschen zu fassen, die zur Fahndung oder polizeilichen Beobachtung ausgeschrieben sind. Der Passus wurde jedoch wieder gestrichen. Es gäbe noch juristische Fragen und Fragen der gesellschaftlichen Akzeptanz, erklärte das Innenministerium dazu.
Weniger zimperlich agieren die Sicherheitsverantwortlichen in London. Anfang 2020 gab die Metropolitan Police of London bekannt, dass sie Echtzeit-Gesichtserkennung einsetzt, um Kriminelle im öffentlichen Raum zu identifizieren. Damit preschten die Engländer in Gefilde vor, wie wir es sonst vorwiegend aus China kennen. Im Land der aufgehenden Sonne sind bereits Hunderte Millionen Kameras installiert. Die Technologie, mit der sie verbunden sind, soll bereits auf einem ziemlich akkuraten Level arbeiten und nicht nur für den polizeilichen Bereich vorgesehen sein. Vielmehr schwebt der Regierung vor, die Bevölkerung mittels Big Data möglichst genau zu rastern.

Inder finden die Technik cool

In Indien herrscht offenbar ein ähnlicher Zugang zum Thema. Das Land, das nach China die zweithöchste Bevölkerungszahl aufweist, plant ebenfalls ein landesweites Gesichtserkennungs-System mit einer zentralen Datenbank für die Behörden. Es soll Bilder von Videoaufnahmen automatisch abgleichen können und Alarm schlagen,

wenn es eine gesuchte Person findet. Die Bevölkerung soll dem Vorhaben gegenüber vorwiegend positiv gestimmt sein. Eine Mehrheit findet derlei Systeme Berichten zufolge cool und trendy und freut sich über das dadurch steigende Sicherheitsgefühl.

Fleckerlteppich in den USA

Ein durchmischtes Bild zeigt sich in den USA. Während Behörden in zahlreichen Städten entsprechende Systeme einsetzen, haben einige Bundesstaaten und Städte den Einsatz von Gesichtserkennung per Gesetz verboten – darunter das Tech-Eldorado San Francisco. Im Land der unbegrenzten Möglichkeiten wird in der Sache wohlgemut experimentiert, wie sich etwa am Schulsektor zeigt. So haben im Südwesten der USA im Zuge von Corona Dutzende Schulen ihre Eingänge mit automatischen Fieberscannern ausgestattet. Beim Kauf der Geräte wurden sie vom Anbieter darauf hingewiesen, dass diese nach dem Ende der Pandemie keineswegs nutzlos seien. Denn dank der eingebauten Gesichtserkennungstechnologie könne man die Gebäude künftig vor unerwünschten Eindringlingen schützen oder die An- und Abwesenheit der Schüler erheben.

Schleichende Einführung?

Wegen Fällen wie diesen befürchten Datenschützer, dass Corona wie ein Booster wirken könnte, der solchen Systemen zu einem schleichenden Eingang in unseren Alltag verhilft. Der chinesische Anbieter Shenzhen Weiguan Views Technology etwa wirbt aktuell für Lösungen an Toren und Zugangskontrollen. Die Geräte sollen binnen einer Sekunde Temperatur und Identität einer Person erkennen. Sie eigneten sich optimal für Gemeinden, Bürohäuser, Hotels, Schulen, landschaftlich reizvolle Orte oder Verkehrsknotenpunkte, schwärmt das Unternehmen in einer Werbebroschüre. Und wer glaubt, dass die derzeit allgegenwärtigen Gesichtsmasken eine Identifikation erschweren, der unterschätzt die Schnelligkeit, mit der sich solche Systeme anpassen. So sollen die führenden Algorithmen bereits gelernt haben, sich auf die Analyse der Augen zu fokussieren, und auch dann Trefferquoten von über 95 Prozent erzielen.

Fehleranfällig, ungenau, rassistisch

Wobei 95 Prozent eben nur 95 Prozent sind. In den restlichen fünf Prozentpunkten liegt eines der großen Probleme der Gesichtserkennung. Denn auch wenn es sich auf den ersten Blick nur um einen kleinen Restwert handeln mag – im Fall einer Massenüberwachung sind es viele, die nicht oder fälschlicherweise erkannt werden. Außerdem haben Tests ergeben, dass die Algorithmen Frauen und dunkelhäutige Menschen weniger leicht erkennen als den „weißen Mann". Sucht die Software etwa nach einer schwarzen Frau, dann kommt es sehr wahrscheinlich zu einer höheren Zahl an sogenannten False Alarms, also zu mehreren Identifikationen von weiblichen Personen, die nicht die gesuchte sind. Bürgerrechtler prangern den systemischen Rassismus in der Technik an. Er soll auch einer der Gründe sein, warum IBM die Sparte ganz aufgegeben hat und Amazon und Microsoft die Zusammenarbeit mit polizeilichen Behörden vorerst ausgesetzt haben.

Foto: B-Media/Shutterstock.com

Rat und Hilfe für Verbraucher in Europa ECC-Net
Finanziell unterstützt durch die Europäische Union

Dieser Artikel wurde aus den Mitteln des Verbraucherprogramms der Europäischen Union (2014 – 2020) gefördert.