

Die Verbrecherjagd der Zukunft

Ermittler des Bundes gleichen Fahndungsbilder bald mit einer Million Fotos ab. Eine Strafrechtsprofessorin hat Bedenken. Eine Kontroverse über Freiheit und Sicherheit.

Andreas Maurer

Es geschieht nachts in einer Unterführung. Ein dunkel gekleideter Mann greift eine Frau an. Er bedroht sie mit einem Messer und raubt sie aus. Die Frau erstattet Anzeige bei der Polizei. Diese sichert die Bilder einer Überwachungskamera. Darauf ist das Gesicht des Täters erkennbar. Es ist die einzige Spur.

Mit den heutigen technologischen Möglichkeiten bringt dieses Überwachungsbild alleine die Ermittlungen nicht weiter. Denn das Foto kann nicht mit der nationalen Polizeidatenbank abgeglichen werden. Heute kann diese nur nach Namen oder Fingerabdrücken durchsucht werden. Eine Gesichtserkennung hingegen bietet die Software nicht.

Das soll sich demnächst ändern. Der Bundesrat hat einen Kredit von 25 Millionen Franken bewilligt, um eines der wichtigsten Systeme der Bundespolizei Fedpol zu erneuern. Es hat einen sperrigen Namen: Automatisiertes Fingerabdruck-Identifikationssystem, kurz Afis. Der amtliche Begriff ist irreführend. Denn in der Datenbank sind nicht nur Fingerabdrücke gespeichert, sondern auch eine Million Gesichtsbilder von 400 000 Personen.

Es sind die Fotos aller Verdächtiger, die in jüngster Zeit in einem Strafverfahren «erkennungsdienstlich erfasst» wurden. Das sind die typischen Polizeifotos, die man aus Krimis kennt: eine Aufnahme von vorne, eine von der Seite und manchmal kommt noch eine dritte hinzu. Bei Straftätern werden die Bilder bis zu dreissig Jahre lang gespeichert. In der Polizeidatenbank sind zudem auch die Aufnahmen aller registrierter Asylsuchender hinterlegt. Diese bleiben zwei Jahre lang abrufbar.

Kommunikationsabteilung von Fedpol ist nervös

Mit dem Projekt «Afis 2026» beschafft Fedpol nun eine Software, mit der sie diese Datenbank mit Gesichtserkennungstechnologie durchsuchen kann. In einem Youtube-Video erklärt Fedpol, wie die Fahndung im fiktiven Fall des eingangs geschilderten Raubüberfalls künftig ablaufen soll. Das Foto der Überwachungskamera wird von der Software mit der Afis-Datenbank abgeglichen. Das System gibt dabei mehrere Treffer an.

Ein Expertenteam der Polizei prüft die Liste möglicher Verdächtiger und findet dabei den gesuchten Räuber – so die Vorstellung im Werbevideo. Der Fedpol-Krimi endet mit einem Happy End. Eine Stimme aus dem Off erklärt, dass auch wei-



So erklärt die Bundespolizei die künftige Fahndungsmöglichkeit in einem Videoclip: Ein unbekannter Mann überfällt eine Frau (1). Sein Gesicht ist auf einer Aufnahme einer Überwachungskamera festgehalten (2). Die Polizei gleicht das Foto mit ihrer Datenbank ab und erhält dabei mehrere mögliche Treffer (3). Darunter ist auch der gesuchte Räuber und so wird er verhaftet (4). Bilder: Screenshots/Fedpol

tere Verbrechen damit gelöst werden könnten: Terrorismus, Entführung oder Kreditkartenmissbrauch.

Einerseits wirbt Fedpol damit, wie wichtig die Technologie für die Verbrecherjagd der Zukunft sein wird. Andererseits betont die Polizeibehörde aber auch, dass sie das technologische Potenzial nur sehr beschränkt nutzen wird. Denn den Aufschrei um vermeintliche Gesichtserkennungstechnologie an SBB-Bahnhöfen hat die mediale Stimmung im Land deutlich gemacht. Sofort entstehen Ängste vor einer überbordenden Überwachung wie in China.

Die PR-Strategen von Fedpol versuchen es deshalb mit einem sprachlichen Trick. So behaupten sie in einer Medienmitteilung, sie würden gar keine Gesichtserkennung einführen, sondern nur einen Gesichtsabgleich. Damit ist gemeint, dass Fotos nur mit der Polizeidatenbank Afis abgeglichen werden, aber nicht mit weiteren Quellen. Nicht mit der Datenbank der Identitätskarten und Reisepässe. Nicht mit Bildern in Social Media. Und auch nicht mit Live-Überwachung – zum Beispiel laufenden Kameras an Flughäfen oder Grenzübergängen.

Auch ein Gesichtsabgleich funktioniert aber mit Gesichtserkennungstechnologie. Das Gesicht wird vermessen und als Raster aus Datenpunkten dargestellt. Es ist deshalb schlicht falsch, zu behaupten, es handle sich dabei nicht um Gesichtserkennung. Richtig ist: Ein Gesichtsabgleich ist eine Anwendungsfeld davon. Zudem

behauptet Fedpol in der Mitteilung, Systeme für Gesichtserkennung seien in der Schweiz ohnehin «gesetzlich verboten». Auch das ist falsch. Ein Verbot existiert nicht. Es fehlen aber die gesetzlichen Grundlagen für eine weitgehende Nutzung als die geplante.

Auf Nachfrage räumt ein Fedpol-Sprecher ein, dass die gewählte Formulierung nicht korrekt sei. Der kommunikative Fehler der Kommunikationsabteilung zeigt die Nervosität der Behörden bei diesem Thema auf. Grund dafür besteht tatsächlich. Denn die gesetzlichen Grundlagen für das Projekt mögen zwar vorhanden sein, aber

sie sind dünn. Es gibt dazu nur eine Verordnung des Bundesrats aus dem Jahr 2013, die ein paar vage Vorgaben macht.

Strafrechtsprofessorin fordert Gesetzesgrundlage

Monika Simmler ist Strafrechtsprofessorin der Universität St. Gallen und auf Gesichtserkennung spezialisiert. Die geplanten Gesichtsabgleiche stuft sie als schweren Grundrechtseingriff ein, weil besonders schützenswerte Personendaten bearbeitet werden. «Dafür genügt eine Pauschalermächtigung auf Verordnungsebene nicht», sagt sie. Die Rechtsgrundlagen seien zu allgemein gehalten. Simmler

fordert eine Regelung auf Gesetzesstufe, auch aus demokratiepolitischen Gründen. Dann müssten die Grenzen des geplanten Gesichtserkennungssystems in einer Debatte geklärt werden und können nicht mehr einfach vom Bundesrat alleine gesetzt werden.

Die Expertin lobt die Kommunikation des Bundes aber auch. Denn bisher war unklar, ob es rechtlich in Ordnung ist, dass einige Kantone schon heute Gesichtserkennungstechnologie für Ermittlungen einsetzen. Diese Frage wird nun geklärt: «Aus rechtlicher Sicht ist es erfreulich, dass der Bundesrat klar festhält, dass alle anderen Arten der Nutzung von Gesichtserkennungstechnologie durch den Staat keine gesetzliche Grundlage haben, also unrechtmässig sind.» Dies nehme jenen Kantonspolizeien, die bereits heute damit arbeiten, den Wind aus den Segeln. Die Nutzung sei nur durch Fedpol erlaubt.

Die Schweiz führt mit der Software-Beschaffung etwas ein, was Nachbarländer schon lange machen. In Deutschland, Österreich und Frankreich sind ähnliche Systeme bereits im Einsatz. Es gibt aber auch demokratische Länder, die viel weiter gehen. In England sind Kameras im Einsatz, die eine Live-Gesichtserkennung durchführen. In den USA darf die Polizei in vielen Staaten Gesichtserkennungstechnologie nutzen, um die Fotos Verdächtiger auch mit der Datenbank der Führerscheine und Ausweise abzugleichen. Mehr als 64 Millionen Amerika-

ner sind davon betroffen. Wenn in der Schweiz hingegen bei einem Verbrechen ein Überwachungsfoto des Täters existiert, muss die Polizei Glück haben. Sie kommt nur weiter, wenn der Gesuchte schon polizeibekannt ist. Sie darf nicht wie das FBI auf die Ausweisdatenbank mit den Passfotos aller 8,7 Millionen Einwohner zugreifen.

FDP-Sicherheitspolitikerin Maja Riniker sagt: «Ich persönlich finde, dass die Polizei mehr Möglichkeiten zur Nutzung von Gesichtserkennung haben sollte.» Ermittler sollten auch Social Media durchsuchen können, findet sie. Da sei sie ganz pragmatisch: «Wer das nicht will, soll keine Fotos von sich hochladen.»

In ganz schweren Fällen würde sie es auch befürworten, dass die Polizei zeitlich limitiert für eine Fahndung Videoüberwachungskameras auf öffentlichem Grund mit Gesichtserkennung nutzen dürfte. Sie geht aber davon aus, dass diese Anliegen derzeit nicht mehrheitsfähig seien. «Ich habe den Eindruck, dass die Gesellschaft seit den Coronamassnahmen staatskritischer geworden ist», sagt sie. Auch das knappe Ja zum Antiterrorgesetz PMT habe gezeigt, dass weitergehende Massnahmen derzeit wenig Chancen haben dürften.

Trefferquote ist auf über 99 Prozent gestiegen

Mit dem technologischen Fortschritt könnte sich dies allerdings in Zukunft ändern. Vor zehn Jahren wurden bei einem Gesichtsabgleich mit Fotos in guter Qualität weniger als 80 Prozent richtig erkannt. Das sorgte für Kritik. In Strafverfahren würde dann nämlich in jedem fünften Fall eine Person zu Unrecht verdächtigt. Inzwischen liegt die Trefferquote aber bei mehr als 99 Prozent.

Ein Problem bleibt allerdings die Erkennung dunkelhäutiger Gesichter. Diese werden unzuverlässiger identifiziert als helle. Je dunkler die Haut ist, desto mehr Mühe hat die Software. Das liegt hauptsächlich daran, dass ein sehr dunkler Hautton den gleichen Effekt hat wie ein unterbelichtetes Foto: Die Konturen sind schlechter erkennbar. Diesbezüglich sind die Programme jedoch ebenfalls besser geworden. Der Unterschied bei der Identifizierung dunkler und heller Gesichter ist nur noch marginal.

Die Verbesserung der Technologie nennt Fedpol denn auch als Grund für die geplante Einführung. Jetzt sei die Zeit auch in der Schweiz reif dafür.

«Eine Pauschalermächtigung auf Verordnungsebene genügt für diesen schweren Grundrechtseingriff nicht.»



Monika Simmler
Strafrechtsprofessorin

«Ermittler sollten auch Social Media durchsuchen können. Wer das nicht will, soll keine Fotos von sich hochladen.»



Maja Riniker
Sicherheitspolitikerin