Ctrl-Alt-R

Gefangen in der Schleuse

Theoretisch ist die Nutzung des automatisierten Gesichtsscanners am Flughafen Zürich freiwillig. Doch unsere Autorin machte bei ihrer Ankunft eine andere Erfahrung.

Von Adrienne Fichter, 18.07.2022

Man landet am Flughafen Zürich, ist müde und erschöpft, wird womöglich mit dem Flughafenbus zum Terminal zurückverfrachtet, wo man sich durch ein kleines Labyrinth kämpfen muss, bevor man (falls aus dem Nicht-Schengen-Raum einreisend) vor der letzten Hürde steht: der Passkontrolle.

Genau da hatte ich jüngst ein unschönes Erlebnis.

Ein tüchtiger Kantonspolizist wies alle Neuankömmlinge an, den Pass auf einen Scanner zu legen. Im Sog mitgehend und gerädert von der Reise, hinterfragte ich die Anweisung nicht, sondern ich gehorchte wie alle anderen und legte brav meinen biometrischen Pass auf. Kurz darauf fand ich mich in einer Situation wieder, die ich seit Jahren zu vermeiden versuche.

Die Schleuse vor mir öffnete sich, und ich stand im Zwischenschacht von Schleuse 1 und Schleuse 2, im Niemandsland quasi. Oder anders gesagt: Ich war an jenem Punkt des offiziellen Grenzübertritts, wo die Behörden dank des Pass-Scans soeben erfahren haben, dass offiziell eine Adrienne Fichter in die Schweiz einreisen möchte. Doch noch haben sie keine Gewissheit darüber, ob die Passinhaberin, die vorgibt, Adrienne Fichter zu sein, tatsächlich auch Adrienne Fichter ist.

Hier kommt die Technik ins Spiel. Denn um die nächste Tür zu öffnen, die mir offiziell den Weg in die Schweiz freigeben soll, musste ich in eine Kamera schauen. Wohl wissend, dass nun mein Gesicht anhand sämtlicher Datenpunkte (wie etwa des Augenabstands) vermessen wird, versuchte ich verzweifelt, das System auszutricksen. Ich schaute nach links, nach rechts, nach oben, doch das System kannte keine Gnade: Die Tür blieb geschlossen. Erst beim Frontalblick in die Kamera öffnete sich Sesam.

Danach sah ich rechts von mir einen Schalter mit zwei sich unterhaltenden Kantonspolizisten. Sie hatten dank der digitalen Gesichtsscanner-Helfer nichts zu tun, was ihnen wohl gerade recht war. Verstört lief ich weiter zur Gepäckausgabe und überlegte, was hier gerade passiert war.

In dieser Situation war einiges schiefgelaufen. Nicht nur aus Kundinnensicht.

Doch zuerst zum Grundsätzlichen: Dass die Schweiz mit Gesichtserkennungssystemen experimentiert, ist nicht neu. Seit 2017 sind solche Systeme im Einsatz. Die Nutzung dieser *automated border control* ist freiwillig, wie Flughafen und Kantonspolizei Zürich stets betonen.

Was genau macht dieser Gesichtsscanner? Florian Frei, Sprecher der Kantonspolizei Zürich, schreibt dazu: «Durch das Auflegen des Reisepasses auf die Scanfläche vor dem Gate wird das auf dem Chip gespeicherte Gesichtsbild ausgelesen. Gleichzeitig wird (...) die Bild-Seite des Passes gescannt.»

Dann erfolgt das Live-Gesichtsbild im Zwischenschacht. Es existieren also für einen kurzen Moment drei Gesichtsbilder von mir. Diese werden miteinander abgeglichen. Ist die Kongruenz da, öffnet sich die Tür. Anwendungen zur Gesichtserkennung dieser Art gehören zu den fortgeschrittenen Systemen von *Machine-learning*-Algorithmen (haben aber auch klar diskriminierende Potenziale und je nachdem hohe Fehlerquoten bei nicht weissen Menschen).

Nach Auskunft der Kantonspolizei werden die erhobenen Gesichtsdaten umgehend gelöscht, was plausibel ist. Schliesslich geht es um die Authentifizierung einer Bürgerin und nicht um die Identifizierung. Oder anders ausgedrückt: Die Grenzbehörden wollen nur wissen, ob ich die Person bin, die ich zu sein vorgebe.

Was dabei aber schiefgelaufen ist: Die Kantonspolizisten verletzten einige datenschutzrechtliche Prinzipien. Denn ich hätte dieser Aufnahme eines Live-Gesichtsbilds bei Schleuse 2 explizit zustimmen sollen. Warum? Weil in dem Fall biometrische Daten verarbeitet werden.

Das bestätigt auch der oberste Datenschützer der Schweiz, Adrian Lobsiger: «Biometrische Daten, die mit dem Zweck bearbeitet werden, jemanden zu identifizieren, sind gemäss neuem Datenschutzgesetz besonders schützenswert. Die Einwilligung muss explizit erfolgen.»

Von einer informierten Einwilligung aus freien Stücken kann jedoch nicht die Rede sein. Es gab keine klare Signalisierung, dass Passagiere zwischen automatisiertem Gesichtsscanner und «menschlicher» Passkontrolle wählen dürften. Es gab einzig eine Anweisung des Kantonspolizisten, den Pass aufzulegen.

Und weil deswegen niemand weiss, was ihn oder sie nach der Öffnung der Schleuse 1 erwartet, weil die entsprechende Information fehlt, gibt es auch in dem Sinn keine Zustimmung. Der kleine Zwischenraum, der direkt zum Schalter geführt hätte, war kaum sichtbar oder zumindest nicht deutlich genug gekennzeichnet. Im Datenschutzjargon nennt man das ein *dark pattern*.

Die Medienanfrage bei der Kantonspolizei förderte noch etwas anderes zutage: Das verwendete System mit dem Namen Gemalto ABC stammt vom französischen Rüstungskonzern Thales. Er bewirbt sein Produkt mit dem Slogan «Less waiting time, better security». Auch der Pariser Flughafen arbeitet damit.

Doch Gemalto ABC wird im nächsten Jahr abgelöst durch ein Produkt der deutschen Firma Secunet Security Networks AG. Sie hat gemäss der Beschaffungsplattform des Bundes Simap.ch die Ausschreibung in Höhe von über 35 Millionen Franken gewonnen. Grund für die Ablösung: Thales konnte die neuen Anforderungen des Schengen-Assoziierungsabkommens nicht erfüllen.

Der Hintergrund: Die Schweizer Grenzbehörden müssen digital aufrüsten, weil die Schweiz als Schengen-Staat auf die von der EU aufgebaute Datenbank Entry/Exit System (EES) mit biometrischen Daten zugreifen wird. Die EU und die Schweiz möchten damit das Problem der *overstayers* (eingereiste

Ausländerinnen aus Drittstaaten, die länger als drei Monate in der Schweiz verbleiben) lösen, um die illegale Einreise zu verhindern. Und – offiziell – um Terrorismus zu bekämpfen.

Doch bleibt es bei einer Einführung von EES auch bei der blossen Authentifizierung? Dient unser Gesichtsbild weiterhin nur der einfachen Überprüfung? Schliesslich sollen dadurch Datenflüsse zwischen der Schweiz und einem EU-weiten Zentralsystem für den Personenabgleich ermöglicht werden.

Die Antwort lautet: Jein.

Die Daten werden wohl gelöscht, es sei denn, die einreisende Person stammt aus einem Drittstaat. In diesem Fall werden bei der ersten Einreise in die Schweiz die Gesichtsdaten bei der automatisierten Passkontrolle gespeichert. Dadurch soll die Aufenthaltsdauer einer Touristin aus dem Nicht-Schengen-Raum genau gemessen werden können.

Das mulmige Gefühl bleibt also. Denn der Ausbau des digitalen Grenzschutzes ist ein Fakt. Die Frage ist, wie lange überhaupt noch die Wahlmöglichkeit bestehen wird, von den menschlichen Augen einer Kantonspolizistin überprüft zu werden. Oder ob man nicht eher Richtung Schleuse und automatisierte Passkontrolle *genudged* wird. Hersteller von Gesichtserkennungssystemen wie Thales preisen jedenfalls ihre Produkte als «unvermeidbar» an, weil sie «verlässlich», «effizient» und «einfach einsetzbar» seien.

Immerhin räumen Kantonspolizei und Flughafen Zürich ein, dass die Situation an der Passkontrolle in meinem Fall nicht optimal gelaufen sei. Eine Flughafensprecherin schreibt: «Wir werden dem von Ihnen beschriebenen Vorfall nachgehen und intern sowie unsere Partner entsprechend sensibilisieren.»

Ich bleibe dran.