Biometric Go – Das digitale Passfoto

Veröffentlicht: 26.04.2026

Wenn der Staat beginnt, die Gesichter seiner Bürger selbst zu erfassen, ist das kein Fortschritt, sondern ein epochaler Dammbruch. Was bislang ein Passbild war – angefertigt von einem Fotografen, als statisches Bild, das lediglich Identität dokumentierte –, verwandelt sich ab Mai 2025 in Deutschland in ein biometrisches Raster.

Biometric Go, so der Name des Systems, ersetzt die vertraute Aufnahme durch ein digitales Verfahren, das Gesichter nicht einfach abbildet, sondern sie zerlegt, vermisst, mathematisch codiert und nach internationalen Standards verschlüsselt. Offiziell heißt es, diese Maßnahme diene der „Stärkung der Sicherheit“. In Wahrheit ist es der letzte Schliff am digitalen Pranger, der den Bürger endgültig zur wandelnden Datei macht.

Die politische Rhetorik spricht von Modernisierung und Effizienz. Doch die Wahrheit liegt tiefer: Mit Biometric Go geht es nicht mehr um das Bild im Pass, sondern um die Frage, ob Identität in Zukunft noch etwas Menschliches sein darf – oder ob sie nur noch maschinenlesbar existiert. Der Staat fragt nicht mehr: „Wer bist du?“ Er prüft algorithmisch: „Darfst du sein, was du vorgibst zu sein?“

Und die Entwicklung, sie kommt nicht aus dem Nichts. Seit Jahren arbeitet die EU daran, biometrische Verfahren zu vereinheitlichen. Die Grundlage bilden die Normen der International Civil Aviation Organization (ICAO), einer UNO-Organisation, die weltweit Standards für maschinenlesbare Reisedokumente (MRTDs= Machine Readable Travel Documents) festlegt.

Gesichter, Iris-Scans, Fingerabdrücke und demnächst vielleicht die DNA – alles wird in Datenstrukturen gegossen, die von Maschinen verstanden werden, und nicht mehr von Menschen. Biometric Go ist lediglich die nationale Umsetzung eines längst transnationalen Projekts. In Zukunft wird der Pass und alle anderen Dokumente - die man an dieser Stelle als Sklaven Dokumente definieren könnte - eine biometrische Formel enthalten, ein Template, das wie ein digitaler Fingerabdruck des Gesichts funktioniert.

Offiziell wird erklärt, die Rohdaten würden nach der Übertragung gelöscht. Doch wer daran glaubt, glaubt womöglich auch an den Weihnachtsmann. Dich damit öffnet sich ein neues Kapitel: Das Gesicht ist nicht mehr Symbol der Individualität, sondern Schlüssel im Identitätstracking. Wer sich einen neuen Ausweis oder Reisepass holt, übergibt nicht nur ein Foto, sondern den Rohstoff für eine Infrastruktur, die weit über den Pass oder Ausweis hinausgeht. Biometric Go ist nicht isoliert, sondern eingebettet in eine umfassende Strategie, die auf Identitätstracking und digitale Berechtigungen hinausläuft. Schon heute wird offen davon gesprochen, dass biometrische Identifikatoren in Zukunft den Zugang zu öffentlichen Dienstleistungen, zum Verkehr und sogar zu sozialen Leistungen steuern sollen.

Und Parallel bereitet die EU das Entry/Exit-System (EES) vor, das ab 2025 an den Außengrenzen der Union verpflichtend eingeführt wird – zunächst für visumpflichtige

Reisende, doch später natürlich für alle. Reisende werden dort per Gesichtsscan erfasst, ihre Bewegungen lückenlos protokolliert und ihre Aufenthaltsdauer algorithmisch überwacht. Wer länger bleibt, als erlaubt, erscheint sofort im System. Und die Technik ist dieselbe, die nun im Bürgeramt getestet wird. Biometric Go ist damit nicht nur Verwaltungsmodernisierung, sondern Testlauf für ein europa- später weltweites Kontrollnetz. Und dieses Netz beschränkt sich nicht auf Grenzen.

Wer heute lernt, dass der Zugang zum Flughafen über biometrische Systeme funktioniert, gewöhnt sich daran, dass morgen auch der Zugang zum Nahverkehr, zu Bankdiensten, Arbeitsplätzen oder eben zu Kino, Theater, Supermarkt – ja, selbst zum Schwimmbad – auf dieselbe Weise gesteuert wird. Gesicht, Iris und Stimme werden zum universellen Berechtigungsschlüssel – und damit auch zur universellen Sperre. Die Daten, die Biometric Go generiert, bleiben nicht im abgeschlossenen Kreis deutscher Behörden. Schon jetzt werden sie nach internationalen ICAO-Normen verarbeitet, die bewusst so gestaltet sind, dass sie weltweit kompatibel bleiben.

Das bedeutet, dass jede nationale Datenbank im Prinzip ein Anschlussknoten in einer weltweiten Infrastruktur ist. Server, Software, Datenleitungen – sie sind nicht national isoliert. Europäische und amerikanische Anbieter teilen sich längst den Markt. Es ist daher keine theoretische Angst, sondern eine reale Gefahr, dass Daten, die unter deutschem Recht erhoben werden, in transatlantischen Systemen landen. Und spätestens an diesem Punkt stellt sich die Frage: Wer garantiert, dass die biometrischen Daten nicht in Systeme integriert werden, die für ganz andere Zwecke geschaffen wurden? Palantir zum Beispiel, ein Unternehmen, das seine Wurzeln in militärischer Datenanalyse im Irak und in Afghanistan hat - und für Massenmorde verantwortlich ist, das sogar inzwischen in zivile Strukturen expandiert.

Deutsche Polizeibehörden arbeiten bereits mit Palantir-Software („Hessendata“, „Gotham“) und füttern ihre Datenbanken, und übertragen daten an die USA - ohne das ein Bürger je zugestimmt hat. Was also hindert diese Systeme daran, biometrische Daten zu verknüpfen mit Verhaltensmustern, Zahlungsvorgängen und Gesundheitsdaten? Ein perfides Beispiel liefert Großbritannien: Dort hat der staatliche Gesundheitsdienst NHS ab 2020 begonnen, sensible

Patientendaten an Palantir zu übergeben.

Was als Plandemie-Maßnahme begann, entwickelte sich 2023 zu einem 330-Millionen-Pfund-Vertrag über die „Federated Data Platform“ – eine zentrale Dateninfrastruktur, die sämtliche Gesundheitsinformationen von Millionen Bürgern bündelt und auswertbar macht. Kritiker sprechen längst von einem Einfallstor für Big Tech - in die intimsten Sphären menschlichen Lebens. Denn wenn Gesundheitsdaten erst einmal in die Hände eines Konzerns wie Palantir geraten, gibt es keine Garantie mehr, dass sie nicht mit Bewegungsprofilen, Finanzinformationen oder biometrischen Mustern verknüpft werden – mit dem Ziel, Menschen gezielt zu sanktionieren, zu blockieren oder zu entrechten.

Ob Reiseverbote, der Ausschluss vom öffentlichen Leben oder – in letzter Konsequenz – die algorithmisch legitimierte Tötung: Alles ist denkbar in einem System, dessen CEO selbst offen erklärte: „We kill people based on data“ (Wir bringen Menschen auf der Grundlage von Daten um). Gerade in diesem Kontext wird deutlich, wie gefährlich dieses Unternehmen ist – und wie verantwortungslos jene Regierungen handeln, die ihre eigenen Datenbanken mit Informationen füttern, die am Ende ihre Bürger gefährden. Bürger, die so selbst zum Ziel dieses Systems werden können.

Sobald sie einmal erfasst sind, können sie über internationale Standards wie die ICAO-Normen, in jeden beliebigen Datenverbund eingespeist werden – und dann ist der Schritt von der Ausweisstelle zur globalen Überwachungsarchitektur nicht mehr weit. Das Bürgeramt wird so zur Schnittstelle einer viel größeren Maschinerie. Der Termin, der bislang eine bürokratische Notwendigkeit war, wird zum Ritual der freiwilligen Entmündigung. Sechs Euro kostet das neue Bild.

Doch was wir dafür bezahlen, ist der Verlust der Anonymität. Der Mechanismus ist perfide: Man suggeriert Bequemlichkeit und Sicherheit. Doch in Wahrheit werden wir in ein Raster gedrängt, aus dem es - wie gesagt - kein Zurück gibt. Wer sein Gesicht abgibt, gibt auch die Hoheit darüber auf.

Ab diesem Moment sind wir maschinenlesbar – nicht mehr als Bürger, sondern als Datenpaket. Biometrische Daten können jederzeit mit anderen Datensätzen verknüpft werden. Bewegungsprofile, Konsumdaten, Gesundheitsdaten und Kommunikationsmuster – sie alle werden miteinander verschmolzen. Damit wird der Mensch nicht mehr identifiziert, er ist seine ID. Die Einführung von Biometric Go reduziert den Menschen auf einen verwertbaren, vergleichbaren, normierten Datensatz.

Die politische Rhetorik spricht von Barrierefreiheit und Inklusion, doch in Wahrheit ist es die Einführung einer Architektur der Kontrolle. Was angeblich den Schwachen helfen soll, macht am Ende alle schwach – weil niemand mehr außerhalb des digitalen Systems existieren kann und darf. Und während man dir versichert, dein Foto werde nach der Übertragung gelöscht, werden die Gesetze stillschweigend angepasst – und am Ende wird es eben doch nicht gelöscht. Wenn überhaupt.

So bleibt es also abrufbar, kombinierbar und auswertbar – nicht für dich, sondern für Behörden, Verwaltungen, Konzerne und alle Geheimdienste, die beispielsweise mit Palantir verbunden sind. Die Freiheit stirbt nicht, indem sie offen verboten wird. Sie stirbt in tausend kleinen Schritten. Ein Scan hier, ein Datensatz dort, eine internationale Norm im Hintergrund, ein Algorithmus im Vordergrund. Am Ende bleibt kein Raum mehr, in dem der Mensch unerkannt existieren kann.

Wer sich freiwillig scannt, darf sich nicht wundern, wenn er bald durchschaubar wird und sich für alles rechtfertigen muss. Dein Gesicht öffnet nicht nur Türen, es kann sie auch verschließen. Eine falsche politische Meinung, ein abweichendes Verhalten, ein algorithmisch „auffälliges“ Bewegungsmuster in Palantir – und dein Zugang zu Diensten, Geld oder Mobilität wird gesperrt. Das klingt nach Dystopie, sagst du dir? doch es ist längst Realität. Amazon testet biometrische Zahlungen per Handfläche, Mastercard integriert Identität in Zahlungsverfahren, Palantir verknüpft Daten aus Militär, Gesundheit und Polizei.

Die Schnittstellen sind vorhanden, die Strukturen wachsen und der Bürger gewöhnt sich daran. Biometric Go ist kein Ziel, sondern das Tor.

Die Freiheit endet nicht mit einem Knall.

Sie endet mit einem Gesichtsscan und deinen Daten.