Die US-Einwanderungsbehörde ICE hat rund 1,5 Millionen Menschen ohne gesicherten Aufenthaltsstatus durch private Auftragnehmer verfolgen, überprüfen und fotografieren lassen. Damit ist eine neue Schwelle überschritten. Der Staat überwacht nicht mehr nur selbst. Er lagert die Suche nach Menschen an Firmen aus. Von **Günther Burbach**.

Ein Mann steht vor seiner Wohnungstür. Draußen warten keine uniformierten Beamten, sondern private Ermittler. Sie haben seinen Namen, sein Geburtsdatum, ein Foto, vielleicht seine Telefonnummer, seine alte Adresse, seine E-Mail-Adresse. Sie sollen herausfinden, ob er wirklich dort wohnt. Wenn nötig, sollen sie ihn fotografieren. Möglichst schnell, denn Schnelligkeit wird bezahlt.

Das klingt nach einem dystopischen Thriller. Tatsächlich beschreibt es ein Programm der US-Einwanderungsbehörde ICE. Nach Recherchen der *Washington Post* begann ICE Ende 2025 ein landesweites „Skip Tracing"-Programm, um rund 1,5 Millionen Menschen ohne gesicherten Aufenthaltsstatus durch private Auftragnehmer verfolgen, überprüfen und fotografieren zu lassen. Die Unternehmen sollen zunächst digitale Spuren nutzen und, wenn nötig, physisch vor Ort auftauchen. Für schnelle Treffer sind finanzielle Anreize vorgesehen.

Aus staatlicher Macht wird ein Geschäftsmodell

Damit ist eine neue Schwelle überschritten. Der Staat überwacht nicht mehr nur selbst. Er lagert die Suche nach Menschen an Firmen aus. Aus staatlicher Macht wird ein Geschäftsmodell. Aus Verwaltung wird Jagdlogik. Aus Daten werden Kopfgeldstrukturen.

Parallel dazu wächst in den USA eine technische Infrastruktur, die das Ganze beschleunigt. Eine aktuelle Recherche des *Guardian* berichtet, dass ICE und die Grenzschutzbehörde CBP im Jahr 2026 Verträge mit Überwachungstechnik-Firmen im Umfang von 513 Millionen Dollar vergeben haben sollen. 2025 waren es demnach etwas über 310 Millionen Dollar, 2013 weniger als 50 Millionen. Genannt werden unter anderem Palantir und Anduril, also Unternehmen, die längst nicht mehr nur Software liefern, sondern an der Schnittstelle von Polizei, Militär, Grenze und Datenanalyse arbeiten.

Hier geht es nicht um ein einzelnes Programm und auch nicht um eine technische Spielerei. Hier entsteht ein Markt, dessen Ware nicht mehr ein Auto, ein Telefon oder eine Maschine ist. Die Ware ist der Mensch: sein Gesicht, seine Adresse, sein Bewegungsmuster, seine Kontakte, sein Aufenthaltsstatus, seine Wahrscheinlichkeit, am nächsten Ort gefunden zu werden.

Der Mensch erscheint als Datensatz

Besonders problematisch ist, dass diese Systeme nicht mehr nur reagieren. Früher suchte man nach einem Verdächtigen, wenn ein konkreter Anlass vorlag. Heute entstehen Datenumgebungen, in denen Personen fortlaufend bewertet, abgeglichen und priorisiert werden. Wer zuerst gefunden werden soll, wer als Risiko gilt, wer in ein Raster fällt, wer in einer Datenbank auftaucht: All das wird zunehmend durch technische Systeme vorbereitet.

Palantir erhielt bereits 2025 einen Auftrag über knapp 30 Millionen Dollar für ein System namens „ImmigrationOS“. Ziel soll es sein, ICE eine nahezu in Echtzeit verfügbare Sicht auf bestimmte Gruppen zu ermöglichen, darunter Menschen mit abgelaufenen Visa oder Personen, die als Ziel von Abschiebungen gelten. Der Name ist bezeichnend. „OS“ steht für Operating System. Es geht also nicht um eine einzelne Anwendung, sondern um eine Betriebslogik. Migration wird in ein Betriebssystem überführt.

Das ist der eigentliche Bruch. Der Mensch erscheint nicht mehr zuerst als Rechtssubjekt, sondern als Datensatz. Er hat nicht mehr nur eine Akte, er wird zu einem Knoten in einem System. Dieses System verknüpft Identität, Bewegung, Behördeninformationen, biometrische Daten, Kontakte und Hinweise aus privaten Datenquellen. Was früher mühsame Recherche war, wird zur maschinellen Sortierung.

Die neue Überwachung ist dabei nicht mehr auf den Staat beschränkt. Sie lebt von privaten Firmen, Datenbrokern, Analyseplattformen, Gesichtserkennung, Drohnen, Handyortung, Finanzdaten, sozialen Medien und biometrischen Abgleichen. Genau darin liegt ihre Gefährlichkeit. Denn je mehr Akteure beteiligt sind, desto unklarer wird die Verantwortung. Wer hat entschieden? Der Beamte? Der Algorithmus? Der Auftragnehmer? Der Datenbroker? Der Softwareanbieter? Der Staat kann sich auf die Technik berufen. Die Firma kann sagen, sie liefere nur Werkzeuge. Am Ende steht ein Mensch da und weiß nicht, gegen welches System er sich eigentlich wehren soll.

Auch die Gesichtserkennung wandert aus dem Labor auf die Straße. Das US-Heimatschutzministerium listet KI-Anwendungen, die mobile Geräte, Gesichter, Fingerabdrücke und Ausweisdokumente erfassen und mit Regierungsdatenbanken abgleichen können. Die App „Mobile Fortify“ wird dabei als Werkzeug beschrieben, das biometrische Informationen in der Einsatzsituation mit vorhandenen Datensätzen vergleicht. Solche Systeme verschieben die Grenze zwischen Kontrolle und Alltag. Ein Gesicht wird zur Abfrage. Eine Begegnung wird zum Datenbankzugriff.

Modernisierung ist hier ein gefährliches Tarnwort

Die offiziellen Begründungen klingen wie immer vernünftig: Identitätsprüfung, Effizienz,

Sicherheit, Entlastung der Behörden, Schutz vor Kriminalität. Das Problem ist nur, dass fast jede Überwachungsinfrastruktur mit solchen Argumenten beginnt. Kaum jemand sagt offen: Wir bauen einen Apparat, der immer mehr Menschen immer leichter auffindbar, bewertbar und steuerbar macht. Stattdessen heißt es: Wir modernisieren Verwaltung.

Doch Modernisierung ist hier ein gefährliches Tarnwort. Was modernisiert wird, ist nicht nur ein Verwaltungsablauf. Modernisiert wird die Zugriffsfähigkeit des Staates. Der Staat muss nicht mehr überall selbst präsent sein. Er muss nur die Datenströme kontrollieren, die technischen Schnittstellen schaffen und die Aufträge vergeben. Die eigentliche Arbeit können Softwarefirmen, Subunternehmer und mobile Erfassungssysteme übernehmen.

Man sollte sich nicht damit beruhigen, dass dies alles in den USA geschieht. Europa ist längst Teil derselben Entwicklung. Frankreich will sich von Palantir in sensiblen Bereichen lösen und auf eigene Anbieter setzen, und zwar ausdrücklich, um neue strategische Abhängigkeiten im digitalen Bereich zu vermeiden. Das zeigt: Das Problem ist nicht nur Datenschutz im engeren Sinn. Es geht um staatliche Souveränität. Wer die Systeme liefert, liefert nicht nur Software. Er liefert die Denkweise, die Datenstruktur und oft auch die Entscheidungslogik.

Deutschland steht vor derselben Frage. Palantir-Systeme wurden in mehreren Bundesländern diskutiert oder eingesetzt. Polizeiliche Datenanalyse wird politisch gern als Fortschritt verkauft. Gleichzeitig bleibt für die Öffentlichkeit oft unklar, welche Daten zusammengeführt werden, welche Prüfmechanismen existieren und welche Rolle private Anbieter tatsächlich spielen. Der Bürger hört Schlagworte wie Effizienz und Sicherheit. Er sieht aber nicht, wie daraus ein neues Machtgefüge entsteht.

Die Lehre aus den USA ist daher nicht: Dort übertreiben sie wieder einmal. Die Lehre lautet: So sieht der Weg aus, wenn man ihn konsequent weitergeht. Erst werden Datensilos geöffnet. Dann werden Systeme vernetzt. Dann werden private Anbieter eingebunden. Dann werden mobile Erfassungsgeräte eingesetzt. Dann entsteht der Wunsch nach Echtzeit. Und irgendwann wirkt es ganz normal, dass ein Staat Menschen durch eine Kombination aus Software, Datenbrokern, biometrischer Erfassung und privaten Auftragnehmern aufspüren lässt.

Eine Jagdstruktur entsteht

Der Begriff „Menschenjagd“ klingt hart, aber er beschreibt die Logik besser als das sterile Wort „Fallbearbeitung“. Wenn Unternehmen Listen bekommen, wenn sie Personen lokalisieren sollen, wenn Fotos verlangt werden, wenn Geschwindigkeit vergütet wird, dann

entsteht eine Jagdstruktur. Die Zielperson wird zur Aufgabe, die erledigt werden muss. Der Mensch verschwindet hinter der Fallnummer.

Das Gefährliche an KI ist in diesem Zusammenhang nicht, dass sie irgendwann ein eigenes Bewusstsein entwickelt. Das ist Science-Fiction. Gefährlich ist, dass sie bestehende Machtverhältnisse beschleunigt. Sie macht nicht automatisch gerechter, was vorher ungerecht war. Sie macht nicht automatisch rechtsstaatlicher, was vorher problematisch war. Sie macht es schneller, breiter und schwerer anfechtbar.

Ein falsch gesetzter Haken in einer Datenbank kann dann Folgen haben. Ein alter Adresseintrag kann eine Kontrolle auslösen. Ein biometrischer Treffer kann einen Verdacht verstärken. Ein Algorithmus kann Prioritäten setzen, ohne dass der Betroffene überhaupt weiß, dass er priorisiert wurde. Wer sich wehren will, muss erst einmal verstehen, woher die Entscheidung kam. Genau das wird immer schwieriger.

Die politische Debatte bleibt dieser Entwicklung weit hinterher. Sie redet über Innovation, Standorte, Wettbewerbsfähigkeit und digitale Verwaltung. Sie redet zu selten über Macht, Haftung, Missbrauch, Fehlerquoten, Kontrollrechte und die Rolle privater Konzerne. Dabei wäre genau das entscheidend. Denn ein demokratischer Staat darf sich nicht in eine Plattform verwandeln, deren technische Grundlagen von Firmen kommen, die selbst kaum demokratisch kontrolliert werden.

Natürlich müssen Ermittler arbeiten können

Es geht auch nicht darum, Polizei und Behörden jede technische Unterstützung zu verbieten. Natürlich müssen Ermittler arbeiten können. Natürlich können Datenanalysen in konkreten Fällen sinnvoll sein. Aber zwischen gezielter Recherche und flächendeckender Vorstrukturierung ganzer Bevölkerungsgruppen liegt eine Grenze. Diese Grenze wird gerade verschoben.

Besonders perfide ist, dass die Systeme meistens zuerst an Gruppen getestet werden, die politisch wenig Schutz haben: Migranten, Asylsuchende, Menschen ohne Aufenthaltsstatus, Protestierende, Arme, Verschuldete. Dort ist der Widerstand schwächer, die öffentliche Empörung geringer, die rechtliche Gegenwehr schwieriger. Was bei ihnen eingeführt wird, kann später auf andere Gruppen übertragen werden. So funktionieren Überwachungsapparate seit jeher. Sie beginnen am Rand und wandern in die Mitte.

Heute trifft es Migranten an der Grenze. Morgen trifft es Demonstranten. Übermorgen trifft es Sozialleistungsbezieher, Versicherte, Patienten, Arbeitnehmer oder Kritiker einer

Regierungspolitik. Sobald die Infrastruktur steht, ändert sich nur noch der Zweck. Die Technik fragt nicht, ob ein Einsatz moralisch vertretbar ist. Sie fragt nur, ob die Daten verfügbar sind.

Deshalb ist der aktuelle Ausbau der KI-Überwachung kein Spezialthema für Technikexperten. Es ist eine Frage des Rechtsstaats. Wer darf Daten zusammenführen? Wer darf Menschen bewerten? Wer darf private Firmen mit staatlicher Zwangsnähe ausstatten? Wer haftet bei Fehlern? Wer kontrolliert die Systeme? Wer kann sie abschalten?

Vertrauen ist fehl am Platz

Die Antwort darf nicht lauten: Vertrauen Sie uns. Genau dieses Vertrauen ist in digitalen Machtfragen fehl am Platz. Ein demokratischer Staat muss beweisen, dass seine Systeme begrenzt, überprüfbar und angreifbar sind. Bürger dürfen nicht zu Objekten werden, die durch technische Infrastrukturen verwaltet werden, ohne die Funktionsweise dieser Infrastrukturen zu kennen.

Der neue Überwachungsapparat kommt nicht mit Stacheldraht und Suchscheinwerfern. Er kommt mit Vertragsnummern, Cloud-Plattformen, mobilen Apps, Datenabfragen, Pilotprojekten, Effizienzversprechen und Sicherheitsrhetorik. Er sieht aus wie Verwaltung. Genau deshalb ist er so gefährlich.

Denn am Ende braucht die moderne Menschenjagd keinen Spitzel an jeder Ecke mehr. Sie braucht Daten, Schnittstellen, private Auftragnehmer und künstliche Intelligenz. Der Rest erledigt sich fast von selbst.

Quellen:

1. The Washington Post: ICE enlisted private contractors to find immigrants for deportation. 30. Januar 2026
2. The Guardian: Inside ICE’s $513m AI surveillance arsenal. 24. Juni 2026
3. U.S. Department of Homeland Security (DHS): Artificial Intelligence Use Case Inventory
4. National Institute of Standards and Technology (NIST): Artificial Intelligence Risk Management Framework
5. Europäische Kommission: AI Act
6. The Guardian: France to replace Palantir with domestic AI company. 16. Juni 2026

Titelbild: Mehaniq / Shutterstock