Kommentar

Schütze uns vor dem Datenschutz

Von Alex Baur — Politiker von links bis rechts machen mit orwellschen Szenarien gegen den biometrischen Pass mobil. Geht es nach ihnen, verkommt der Datenschutz zum Täterschutz.

Um ein Vielfaches sicherer: der biometrische Pass.

Professor Andreas Pfitzmann von der Technischen Universität Dresden schwant Böses: Wenn Fingerabdruck und Gesichtsprofil des Bürgers elektronisch erfasst und via Minichip in den Reisepass eingebaut werden, «haben fremde Geheimdienste und auch Kriminelle nach kurzer Zeit eine grosse Sammlung von deutschen Fingerabdrücken». Dunkle Mächte, warnt Pfitzmann, könnten mit den Fingerprints «falsche Spuren an Tatorten hinterlassen, sei es, um die Polizei in die Irre zu führen oder aber Personen in Notlage zu bringen». So könnten Geheimdienste unbescholtene Bürger zur Kooperation zwingen, nach dem Muster: «Wenn Sie mit uns zusammenarbeiten, sind Sie alle Probleme los.»

Nachzulesen ist das professorale Horrorszenario auf der Website eines Komitees aus Politikern verschiedenster Couleur (SVP, SP, Grüne, CVP), das gegen die Einführung des sogenannten biometrischen Passes in der Schweiz mobilmacht. Der neue Pass sei zu teuer (140 Franken für Erwachsene, Kinder die Hälfte) und anfällig für Missbrauch. Sekundiert wird die bunte Koalition vom eidgenössischen Datenschützer Hanspeter Thür, der die zentrale Speicherung der biometrischen Daten als «beachtliche Gefährdung der Persönlichkeitsrechte» geisselt. Zwar ist die Nutzung der Passdaten zu Fahndungszwecken untersagt, doch, wie Thür gegenüber dem Schweizer Fernsehen erklärte, stimmt ihn gerade das Verbot misstrauisch: Die Erfahrung zeige, dass erhobene Daten früher oder später auch genutzt würden.

Gemäss dem Komitee versagt die elektronische Gesichtserkennung in einem von zehntausend Fällen – was schlimme Konsequenzen für den Betroffenen haben könnte. Die Datenträger seien auch nicht «zu 100 Prozent» fälschungssicher, ein «Identitätsklau» wäre denkbar. Gemeinsam ist den Einwänden, dass sie alle theoretisch denkbar sind. Doch obwohl biometrische Daten seit Jahren erhoben werden, kann das Komitee kein einziges konkretes Fallbeispiel nennen, bei dem jemand effektiv zu Schaden gekommen wäre.

Dass es absolut fälschungssichere Systeme nicht gibt, gehört zu den Binsenweisheiten. Entscheidend ist, dass der neue Pass um ein Vielfaches sicherer ist als seine Vorgänger und überdies ungleich effizienter in der Handhabung. Das Gleiche gilt für die zentrale Speicherung der Daten, die einen unkomplizierten Ersatz im Fall eines Verlusts des Passes erlaubt. Im Katastrophenfall kann ein Fingerabdruck zur Identifizierung von Opfern überdies sehr dienlich sein.

Es stellt sich vielmehr die Frage, warum die biometrischen Daten nicht für die Fahndung genutzt werden dürfen. Sie führt mitten ins Thema.

Dieselben politischen Kreise, die das Bankgeheimnis abschaffen und Kundendaten an Steuerbehörden in aller Welt verschicken wollen, erklären nun den Fingerabdruck zum höchst intimen Schutzobjekt. Dieselben Datenschützer, die den Staat partout verdächtigen, die Daten seiner Bürger zu missbrauchen, beklagen sich über einen vermeintlichen Generalverdacht, dem der datenmässig erfasste Bürger ausgesetzt werde. Bei nüchterner Betrachtung entpuppt sich diese Argumentation als rhetorische Leerformel. Denn ein Fingerprint oder eine DNA-Spur (aus fahndungstechnischer Sicht ist es dasselbe) zeigt einzig und allein, dass eine bestimmte Person in einem Bezug zum Tatort steht.

Perverse Konsequenzen

Das Sammeln und Auswerten von möglichst vielen, an sich wertneutralen Daten gehört zur Kernaufgabe jedes Fahnders. Der Datenschutz hat zu einer perversen Verzerrung geführt. Weil nur noch Daten von notorischen Straftätern gespeichert werden, steigt die Gefahr einer ungerechtfertigten Vorverurteilung. Umgekehrt gilt: Je grösser die Datenmenge, desto objektiver lässt sich ermitteln – auch zur Entlastung von Verdächtigten.

Der eidgenössische Datenschutz beschäftigt mittlerweile zwanzig Beamte. Dazu kommt ein Heer von Datenschützern in den Kantonen und Städten, die ohne klaren Auftrag nach Bereichen suchen, in denen sie ihre Existenzberechtigung beweisen können. So kommt es, dass im Kanton Zürich Fürsorgebehörden von ihren «Klienten» keine detaillierten Bankauszüge mehr verlangen dürfen, selbst wenn Indizien für einen Betrug vorliegen; die erfolgreiche Erfassung von Nummernschildern im Strassenverkehr (in Deutschland bereits verboten) wurde auch in der Schweiz eingeschränkt; Abfallsünder, die ihre Cumulus-Nummer hinterlassen, dürfen nicht mehr identifiziert werden, Überwachungskameras sind so zu installieren, dass die Täter nicht identifizierbar sind; selbst gemeingefährliche Verbrecher dürfen darauf zählen, dass ihre Vorstrafen unwiderruflich gelöscht werden.

Die Liste liesse sich fortsetzen, gemeinsam ist den oft widersprüchlichen Regeln eine bisweilen massive Behinderung der Strafverfolgung mit einem bestenfalls abstrakten Nutzen für die Allgemeinheit. Ein zusehends zum Täterschutz verkommener Datenschutz führt sich selber ad absurdum. Datenschützer Thür spielt sich als Zensor auf und lässt Internetportale verbieten, auf denen Patienten ungefiltert ihre Erfahrungen mit Ärzten publik machten. Nie zuvor in der Menschheitsgeschichte war die Privatsphäre so umfassend geschützt wie heute. Nur – wer schützt uns vor den Datenschützern?

Bild: Siemens