2007/36 Thema

https://jungle.world/artikel/2007/36/eine-bedeutende-sammlung

Eine bedeutende Sammlung

Von **Boris Mayer**

Der Pass sei der edelste Teil eines Menschen, schrieb Bert Brecht einst. So ähnlich sehen das auch die staatlichen Datensammler. Zur Überwachung der Bürgerinnen und Bürger ist ihnen inzwischen jedes Mittel recht.
von boris mayer

Je gläserner der Bürger, desto sicherer ist er auch – so könnte das Motto lauten, unter dem derzeit die deutsche Politik unter Verweis auf Terrorabwehr und innere Sicherheit Gesetzesgrundlagen für immer weiterreichende Überwachungsmaßnahmen schafft. Nicht nur alte Datensammlungen werden durch vereinfachten Zugriff und Vernetzung aufgewertet und ermöglichen ganz neue Quervergleiche, auch neue Datensammlungen werden erstellt. Bislang dürfen personenbezogene Daten grundsätzlich nur dann gespeichert werden, wenn dies zu einem bestimmten Zweck erforderlich ist. Ist ein solcher, gesetzlich geregelter Zweck nicht, noch nicht oder nicht mehr gegeben, müssen diese Daten gelöscht werden.

Unter Vorratsdatenspeicherung versteht man die präventive Speicherung von personenbezogenen Daten ohne Einwilligung der Betroffenen für den Zeitraum von sechs Monaten. Die Bundesregierung plant die Anwendung von einer entsprechenden europäischen Richtlinie, nach der diese Vorratsdatenspeicherung Verbindungsdaten in allen Kommunikationsmitteln zur Pflicht werden soll. Das Gesetz soll am 1. Januar 2008 in Kraft treten, ist aber noch nicht verabschiedet.

Wie eine solche Datensammlung aussehen könnte, zeigt der Einzelverbindungsnachweis auf der Telefonrechnung. Dort ist jeder einzelne Anruf aufgelistet, inklusive Datum, Uhrzeit und Dauer. Allerdings ist dies nach dem Gesetzentwurf nicht alles, was gespeichert werden soll, denn bisher werden zum Beispiel Rufumleitungen, die der Angerufene veranlasst hat, nicht bei dem Anrufenden gespeichert. Bei Handytelefonaten kommen zusätzlich noch die Kennungen der von beiden Teilnehmern genutzten Geräte und die Funkzellen hinzu, in denen sich die Telefonierenden zu Beginn des Telefonats jeweils befinden. Das gilt nicht nur für Telefonate, sondern auch für SMS und MMS.

Ähnlich umfangreich soll nach den Plänen der Bundesregierung auch die Vorratsspeicherung für Internetdaten werden. So soll gespeichert werden, wer wem wann

und von wo aus eine E-Mail schreibt und E-Mails abruft und wer wann, wie lange und von wo aus welche Internetadresse zugewiesen bekommen hat. Und nicht nur die großen Telekommunikationsunternehmen sind von der Pflicht zur Vorratsdatenspeicherung betroffen: Wer einen öffentlichen W-Lan-Zugang anbietet, muss ebenfalls die Daten seiner Nutzer speichern.

Diese Daten sollen drei Zwecken dienen. An erster Stelle steht die Verfolgung von Straftaten, gefolgt von der »Abwehr erheblicher Gefahren für die innere Sicherheit«. Außerdem ist die Datensammlung von Verfassungsschutzbehörden, Bundesnachrichtendienst und Militärischem Abschirmdienst nutzbar. Die anfallende Datenmenge wird enorm sein. Selbst vorsichtige Schätzungen gehen von Investitions- und Unterhaltskosten in dreistelliger Millionenhöhe aus, die von den anbietenden Unternehmen getragen werden sollen – Mehrausgaben, die Konzerne für gewöhnlich an ihre Kunden weitergeben.

Der Nutzen dieser Daten ist allerdings höchst zweifelhaft. Verbrechen können durch die Vorratsspeicherung kaum verhindert werden, und selbst bei der Aufklärung von Straftaten fallen die Daten kaum ins Gewicht: Nach einer Studie des Bundeskriminalamts vom November 2005 hätten 381 Straftaten zusätzlich aufgeklärt werden können, wenn diese Daten vorgelegen hätten – also etwa 0,006 Prozent der jährlich begangenen Straftaten. Die Zahl der unaufgeklärten Delikte würde pro Jahr um beeindruckende 0,014 Prozent sinken.

Auch die geplante Einführung biometrischer Daten in den deutschen Reisepässen wird die Welt wohl nicht zu einem besseren Ort machen. Seit dem Jahr 2003 existiert eine Empfehlung der Uno, zukünftig biometrische Merkmale der Inhaber elektronisch auf Reisedokumenten zu speichern. Diese Empfehlung umfasst die zu verwendende Technik ebenso wie eine vereinheitlichte Datenstruktur, um die weltweite Kompatibilität zu gewährleisten. Gespeichert werden sollen das digitalisierte Lichtbild und, allerdings nur als optionale Erweiterung, Merkmale wie Fingerabdrücke oder Irismuster. Als Technik sollen die so genannten RFID-Chips Verwendung finden. RFID bedeutet »Radio Frequency Identification«, also die Identifizierung über Radiowellen. Diese Chips ermöglichen ein Auslesen der darauf gespeicherten Daten ohne direkten Kontakt zu dem Chip.

Die EU beschloss im Dezember 2004 auf Druck der USA, die Pässe der Mitgliedsstaaten gemäß dieser Empfehlung mit biometrischen Daten auszustatten. Im Juni 2005 stimmte dann das Bundeskabinett für einen Vorschlag des damaligen Innenministers Otto Schily (SPD), der die Einführung eines solchen Reisepasses als »wichtigen Schritt auf dem Weg zur Nutzung der großen Fortschritte der Biometrie für die innere Sicherheit« bezeichnete. Der Grund für die Einführung ist also letztlich die Terrorismusbekämpfung.

Diese Argumentation ist jedoch äußerst umstritten. So gilt schon der alte Reisepass, ohne elektronisch auslesbare Daten, als sehr fälschungssicher. In den Jahren 2001 bis 2006 sind gerade einmal sechs Fälschungen deutscher Pässe festgestellt worden. Kein einziger Fall ist bekannt, in dem ein Terrorist einen deutschen Reisepass genutzt hätte. Zudem schützen biometrische Daten auf Pässen nicht wirklich vor Terroranschlägen – in Spanien sind Fingerabdrücke seit Francos Zeiten Bestandteil der Pässe.

Die Daten auf den Chips im Reisepass sind verschlüsselt gespeichert, aber dennoch gab es schon einige teilweise erfolgreiche Angriffe auf das System. So wurde etwa das Klonen der Daten öffentlich demonstriert. Dabei wurden die Ausweisdaten eins zu eins von einem Original in einen leeren RFID-Chip kopiert. Die Daten wurden dabei zwar nicht verändert, aber damit ist eine Kopie des digitalen Teils des Ausweises im Umlauf. Ein britischer Sicherheitsexperte demonstrierte zudem, dass er unter Verwendung des Geburtsdatums des Inhabers trotz Verschlüsselung auch die restlichen Daten aus dem Pass auslesen konnte. Das Dokument befand sich dabei in einem versiegelten Umschlag, der Besitzer hätte also diesen Vorgang nicht wahrgenommen. Mit diesen beiden Techniken ließe sich zum Beispiel ein Identitätsdiebstahl zunächst unbemerkt vom Opfer durchführen. Abändern kann man die Daten allerdings noch nicht. Die eingesetzte Verschlüsselungstechnik ist nach Meinung von Experten auf absehbare Zeit sicher, doch die Erfahrung zeigt, dass man nicht vorhersagen kann, wie lange es dauern wird, bis eine solche Verschlüsselungstechnik geknackt wird.

Nützlich könnten die biometrischen Passdaten den Behörden vor allem im Hinblick auf die Videoüberwachung sein. Immer wieder ist von Plänen die Rede, zum Beispiel automatisch von Überwachungskameras gefilmte Autokennzeichen zu erkennen und zu speichern. Überall eingesetzt, ergäbe dies ein genaues Bewegungsprofil der Nutzer eines Fahrzeugs. Noch weiter geht die automatische Gesichtserkennung. Im Moment können Gesichter nur erkannt werden, wenn sie optimal ausgeleuchtet sind und derjenige, der erkannt werden soll, direkt in die Kamera blickt. Noch reicht hier die Technik nicht aus, aber das ist nur eine Frage der Zeit, und zudem könnte zur Unterstützung ja auch der mitgeführte RFID-Pass ausgelesen werden.