



## **KLEINES ÜBERWACHUNGS-GLOSSAR**

### **Vorratsdatenspeicherung**

Das im Januar 2008 in Kraft getretene Gesetz zur Vorratsdatenspeicherung sieht die systematische und verdachtsunabhängige Speicherung sämtlicher Telekommunikationsdaten aller BürgerInnen (durch Telekommunikationsanbieter und Internetprovider) vor. Durch die Vorratsdatenspeicherung und ihre spätere Auswertung durch Sicherheitsbehörden kann nachvollzogen werden, wer mit wem wann per Telefon, Handy oder E-Mail in Verbindung gestanden oder das Internet benutzt hat. Bei Handy-Telefonaten und SMS wird auch der jeweilige Standort des Benutzers festgehalten. Mit Hilfe der über die gesamte Bevölkerung gespeicherten Daten können Bewegungsprofile erstellt, geschäftliche Kontakte rekonstruiert und Freundschaftsbeziehungen identifiziert werden. Auch Rückschlüsse auf den Inhalt der Kommunikation, auf persönliche Interessen und die Lebenssituation der Kommunizierenden werden möglich. Die Vorratsdatenspeicherung stellt somit einen gravierenden Eingriff in die Privatsphäre jedes Einzelnen und das Grundrecht auf informationelle Selbstbestimmung dar.

### **Online-Durchsuchungen**

Als Online-Durchsuchung wird der verdeckte staatliche Zugriff auf fremde informationstechnische Systeme über Kommunikationsnetze – also konkret das heimliche Ausspähen von privaten Festplatten – bezeichnet. Das Urteil des Bundesverfassungsgerichts vom 27. Februar 2008, wonach Online-Durchsuchungen nur bei konkreten Gefahren für ein Menschenleben oder den Bestand des Staates zulässig sind, ist als Sieg für den Rechtsstaat und die Privatsphäre jedes Einzelnen zu werten. Durch die Einführung des neuen „Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, kurz IT-Grundrecht, werden die Grundrechte gestärkt und der Totalausspähung ein Riegel vorgeschoben.

### **Automatisches Autokennzeichen-Scanning**

Die verdachtslose Erfassung aller VerkehrsteilnehmerInnen durch mobilen und verdeckten Einsatz von automatischen Kennzeichenlesesystemen darf laut eines Urteils des Bundesverfassungsgerichts vom 11. März 2008 nur in engen Grenzen bei anlassbezogenen Fahndungen eingesetzt werden. Trotzdem hält die Landesregierung in Baden-Württemberg an ihren Plänen zur Einführung dieses Systems fest. Das Kfz-Scanning führt zu Dauerobservation und „allgemeinen Einschüchterungseffekten“ (so das Bundesverfassungsgericht). Zudem verletzt die flächendeckende elektronische Beobachtung das Grundrecht auf informationelle Selbstbestimmung.

### **Video-Überwachung**

Die Video-Überwachung auf öffentlichen Plätzen und „semi-öffentlichen Bereichen“ wie Bahnhöfen, Flughäfen und Häfen ist heute schon vielfach Realität. Zwar kann der gezielte Einsatz von Videoüberwachung an bestimmten Orten der Verkehrsinfrastruktur sinnvoll sein, aber eine flächendeckende Überwachung ist freiheitsfeindlich und mit dem Verhältnismäßig-

keitsprinzip unvereinbar. Videokameras können keine Anschläge verhindern. Deshalb müssen öffentliche Räume grundsätzlich überwachungsfrei sein.

### **Pass mit biometrischen Daten**

Seit 2005 enthalten Reisepässe biometrische Daten auf einem winzigen RFID-Chip: Gesichtsmerkmale und seit dem 1. November 2007 auch zwei Fingerabdrücke werden auf dem Pass gespeichert. Sinn und Zweck soll die erhöhte Sicherheit der Dokumente sein. Nur: Durch den integrierten RFID-Chip können die gespeicherten persönlichen Daten unbemerkt und ohne Zustimmung des Besitzers z.B. durch ein normales Kartenlesegerät ausgespäht werden. Der ePass ist ein unverhältnismäßiger Eingriff in die informationelle Selbstbestimmung und öffnet weiteren Überwachungsmaßnahmen Tür und Tor.

### **Payback-System**

Das Kundenbindungsprogramm Payback bietet Rabatte in Form von Punktegutschriften. Die Payback-Karte wird beim Bezahlvorgang an der Kasse vorgelegt, die eingekauften Produkte personenbezogen gespeichert. Hieraus entsteht der „gläserne Kunde“: Aus den gesammelten Daten lassen sich Rückschlüsse auf den Lebenswandel des Kunden sowie den Erfolg von Werbung ziehen. Beispielsweise werden die Einkäufe eines Payback-Kunden an einer Tankstelle zusammen mit dem Namen und Adresse vermerkt.

### **RFID-Chips**

Die *Radio Frequency Identification* ist die Identifizierung von Lebewesen und Gegenständen mit Hilfe von elektromagnetischen Wellen. RFID-Chips befinden sich beispielsweise auf Eintrittskarten (Fussball-WM 2006), in der Bahncard und sie werden im Einzelhandel z.B. in der Kleidung gebraucht. Die Gefahr der RFID-Technik liegt in dem Verlust der informationellen Selbstbestimmung, da einzelne Personen durch die „versteckten“ RFID-Sender keinen Einfluss mehr darauf haben, welche Informationen über sie preisgegeben werden.

### **Kreditgeschäfte**

Durch das Kreditscoring kann eine Bank die Kreditwürdigkeit eines Kunden automatisiert ermitteln. Aufgrund von persönlichen Daten wird eine Bonitäts-Note errechnet, die die Kreditvergabe erleichtern soll, beispielsweise durch die Schufa. Das Verfahren zur Score-Errechnung ist allerdings undurchsichtig und führt zu detaillierten Persönlichkeitsprofilen von Kunden und so zum „gläsernen Konsumenten“.

### **Fluggastdatenspeicherung**

In einem Passagiernamensregister werden alle Daten und Vorgänge rund um eine Flugbuchung elektronisch aufgezeichnet und gespeichert. Nach US-Vorbild plant derzeit auch die Europäische Union das Sammeln und Austauschen von privaten Kundenangaben wie Flugrouten, E-Mail-Adressen, Kontodaten oder Essgewohnheiten in der gesamten EU zur Terrorbekämpfung.