Herausforderungen für den Datenschutz

Johann Bizer

Zentralität

Das erste Paradigma der automatisierten Datenverarbeitung war die Datenverarbeitung in zentralen Rechenzentren. Die Rohdaten wurden angeliefert, um in den Rechenzentren verarbeitet und der anliefernden Stelle zur Verfügung gestellt zu werden. Die Rechenzentren wurden zentral betrieben, weil die Computer der ersten und zweiten Stunden teuer waren.

Aus diesem Zeitalter der Zentralität stammen die ersten Großprojekte des E-Government wie das Bundeszentralregister oder das Kraftfahrzeugregister. Das Grundmodell ist *ein* Datenbestand in einem zentralen Register, an das die dezentralen Behörden personenbezogene Daten übermitteln bzw. abfragen.

Die Datenschutzdiskussion haben die Risiken zentraler Register für das Persönlichkeitsrecht nachhaltig beeinflusst. Ein zentrales Register birgt die Gefahr, dass in ihm alle relevanten Informationen über eine Person zusammengeführt und abgefragt werden können.

Dezentralität

Das Melderegister verkörpert das Gegenmodell zu einer zentralen Datenhaltung. Die Meldedaten werden dezentral von den kommunalen Meldeämtern geführt. Um den Verwaltungsaufwand für den Datenaustausch bei Umzügen oder der einfachen Melderegisteraukunft zu reduzieren, sollen die Melderegister spätestens zum 1. Januar 2007 miteinander kommunizieren. Dies setzt zum einen eine *Standardisierung* der Datenformate, zum anderen eine *Interoperabilität* der Meldeämter voraus. Mit dem Format XMeld und dem Übermittlungsstandard OSCI-Transport sind beide Voraussetzungen gegeben. Mit dem DVDV (auch „DV Quadrat“) wird ein bundesweites Adressverzeichnis der Meldeämter aufgebaut. Selbst wenn einige Länder ihre Meldeämter zunächst über „Clearingstellen“ miteinander verknüpfen, so zeichnet sich

doch die Entwicklung einer vernetzten dezentralen Datenverarbeitung deutlich ab.

Aus Datenschutzsicht hat das Paradigma der Dezentralität große Vorteile: Es vermeidet mächtige – für das informationelle Selbstbestimmungsrecht übermächtige Datensammlungen – und setzt stattdessen auf kleine Datenbanken, deren Datenverarbeitung lokal verantwortet wird. Die Dezentralität hat zudem den Vorteil einer geringeren Verletzlichkeit der Datenverarbeitung. Gleichzeitig schließt sie die Vorteile eines kostengünstigeren Outsourcing nicht aus, solange die Datenbestände vom Auftragnehmer mandantenfähig verwaltet werden.

Das Modell dezentraler, aber vernetzter Datenverarbeitung entspricht dem Vorbild des Internet – ohne dass sich die Protagonisten des E-Government dem wirklich bewusst sind. Noch schieben wir die gewachsenen Strukturen der Zentralität wie riesige Endmoränen vor uns her, aber schon längst stellt sich die Frage, ob die Implementierung webbasierter E-Government-Anwendungen nicht kostengünstiger und zukunftsträglicher ist als die Mischformen selbstgestrickter proprietärer Entwicklungen.

E-Cards

Die bisherige Polarität von Zentralität und Dezentralität wird durch die Einführung Elektronischer Karten mit Authentifizierungsfunktion vor neue Herausforderungen gestellt: Ob Reisepass, Personalausweis oder Gesundheitskarte – alle Modelle halten sich die Option für die Ablage elektronische Identitätsmerkmale von der Biometrie bis zu Signaturzertifikaten offen. In Umrissen ist bereits heute eine neue Option erkennbar: Entweder die elektronischen Identifikatoren auf den E-Cards spiegeln lediglich die in (de)zentral abgelegten Datenbanken Identitätsdaten einer Person oder aber die E-Cards entwickeln sich zu eigenständigen Trägern dieser Merkmale.

Unter Datenschutzgesichtspunkten zentral wird damit die Frage des Identitätsmanagements: Wird sich der Einzelne im

virtuellen Spinnenetz seiner elektronischen Identität verfangen oder verbleiben für den Einzelnen Chancen, seine Identität über rollenbasierte Pseudonyme gegenüber Dritten zunächst zu schützen? Die Antwort wird dramatische Dimensionen gewinnen, wenn und soweit die Identitätsmerkmale in den elektronischen Netzen „ausgegoogelt“ werden können. Ein solches Szenario ist angesichts staatlicher Sicherheitsinteressen nicht unrealistisch. Nicht nur die Wirksamkeit der Vorratsspeicherung setzt mächtige Suchfunktionen voraus. Für den Datenschutz rücken damit unter der Überschrift von Verknüpfbarkeit und wirksamer Selbstschutzmechanismen neue Themen in den Vordergrund.

Zu diesem Heft

Waltraut Kotschy stellt uns das Konzept der Bürgerkarte Österreichs vor, das derzeit innerhalb der EU große Aufmerksamkeit genießt. Christian Engel skizziert den Weg zum elektronischen Personalausweis, während Henry Krasemann aus einem anderen Blickwinkel die Bedeutung eines selbstgesteuerten Identitätsmanagement thematisiert. Irene Karper beleuchtet einen anderen Aspekt der E-Card, nämlich am Beispiel des Onlinebanking die individuellen Sorgfaltspflichten.

In den Aufsätzen stellen wir einen Beitrag aus dem *BvD* zum Berufsbild des Beauftragten für den Datenschutz zur Diskussion. Stefan Ernst skizziert die Rechtsprechung zum privaten Surfen am Arbeitsplatz als Kündigungsgrund. Thomas Sassenberg und Niclas Bamberg beleuchten die Bedeutung der Betriebsvereinbarung im BDSG und Noogie Kaufmann berichtet uns in einem Fortsetzungsbeitrag aus der Rechtsprechung zum Datenschutz 2005. Schließlich beschreibt Marco Seifert Sicherheitsprobleme im privat genutzten DSL und ihre Lösung.

Dokumentiert werden in diesem Heft die Entschlüsse der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Magdeburg.