Vertrauen vorausgesetzt

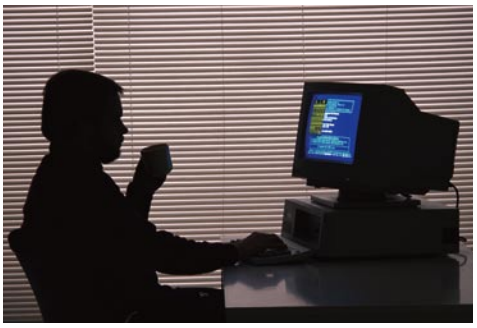
von Thilo Weichert

Die IT eröffnet der Verwaltung zahlreiche neue Möglichkeiten der Kommunikation – doch nur bei einer transparenten und sicheren Verarbeitung und Nutzung ihrer Daten werden die Bürger die neuen E-Government-Angebote auch in Anspruch nehmen.

Viele Staaten und deren Wirtschaft setzen zur Verbesserung von Informationsverarbeitung und Kommunikation auf den Ausbau der IT. Dabei kümmern sich die meisten Länder bisher nur wenig um die Frage, wie diese Technik mit den Anforderungen an eine freiheitliche und demokratische Gesellschaft in Einklang gebracht werden kann. Letztlich entscheidet dies aber nicht nur über die Akzeptanz der Bevölkerung für die neuen Angebote. Die Antwort hierauf stellt auch die Weichen dafür, ob der Weg in die Informationsgesellschaft totalitär oder demokratisch, kontrollierend oder freiheitlich verläuft. Zwar eröffnet die Informationstechnik dem Einzelnen gewaltige Freiheitspotenziale. Zugleich werden aber elektronische Spuren hinterlassen, welche die Kontrolle und die Beeinflussung dieser Freiheit erlauben.

Offensichtlich auch aufgrund der Kontroll- und Überwachungserfahrungen Deutschlands durch zwei Diktaturen in den vergangenen 75 Jahren ist die Gesellschaft in besonderem Maße sensibilisiert für die Gefahren informationeller Fremdbestimmung. Und so ist es die Bundesrepublik, die weltweit eine führende Rolle übernommen hat bei der Entwicklung einer freiheitskompatiblen Technikinfrastruktur. Von Deutschland gingen in den vergangenen vier Jahrzehnten wesentliche Impulse für den informationellen Freiheitsschutz aus: So hat das Land Hessen 1970 das weltweit erste Datenschutzgesetz erlassen. Mit der Schaffung des Rechts auf informationelle Selbstbestimmung erhob mit dem Bundesverfassungsgericht 1983 erstmals ein oberstes Gericht den Datenschutz in den Rang eines Grundrechts. Das Bundesdatenschutzgesetz von 1990 diente als Leitbild für die europäische Datenschutzrichtlinie aus dem Jahr 1995, welche derzeit global die leitende Regulierung des Datenschutzes ist. Und es ist Deutschland, das mit seinem Modell der regulierten Selbstregulierung die künftige Richtung im Datenschutz weist, etwa mit den Instrumenten der unabhängigen staatlichen Datenschutzkontrolle, behördlichen Datenschutzbeauftragten oder neuen Instrumentarien wie Datenschutzgütesiegel und -audit. Auch bei der Entwicklung datenschutzfreundlicher Technologien spielt Deutschland global in der ersten Liga.

Die Sensibilität der Menschen hinsichtlich ihrer Privatsphäre hat angesichts der technischen Bedrohungen eher zugenommen. Hierin liegt sowohl die Chance wie auch



Bürger reagieren sensibel auf Datenmissbrauch.

die Herausforderung, angesichts der rasanten Technikentwicklung freiheitliche Antworten für Technik, Organisation und Recht zu finden. Dabei kommt dem Staat eine zentrale Funktion zu. Diese hat das Bundesverfassungsgericht – wieder weltweit führend – im Februar 2008 erstmals beschrieben als die grundrechtlich begründete Pflicht zur „Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme“. Diese Pflicht besteht zunächst bei der hoheitlichen Kommunikation mit und über den Bürger. Anders als zum Beispiel in Großbritannien, wo beinahe regelmäßig Daten- und Vertraulichkeitsverluste bekannt werden, ist die deutsche Verwaltung aufgefordert und zumeist auch bereit, Datenschutz und Datensicherheit ernst zu nehmen und umzusetzen.

Schließlich werden nur bei einem hinreichenden Vertrauen der

Bevölkerung in die Sicherheit von E-Government-Anwendungen diese auch genutzt. Hierzu bedarf es der sicheren Kommunikation in verschlüsselter Form, der eindeutigen Authentifikation mithilfe von Signaturen und der Sicherung der Zweckbindung in den jeweiligen Anwendungen. Auch bei anwendungsübergreifenden Angeboten muss der Nutzer die Möglichkeit haben, gezielte Zwecke zu verfolgen. Dazu sind Lösungen des Identitätsmanagements erforderlich. Allzu eindeutige Identifikatoren wie etwa die Personalausweisnummer oder die vor Kurzem eingeführte Steuer-ID schüren allerdings zu Recht das Misstrauen der Bürger, insbesondere wenn diese Nummern nicht nur in der Kommunikation mit Behörden genutzt werden, sondern auch in behördenrelevanter Kommunikation zwischen Privaten. Nicht minder Vertrauen zerstörend sind zentrale Anwendungen, bei denen die Betroffenen nicht mehr die Verfügungsgewalt über die eigenen Daten haben. Diese Verfügungsmacht wurde vorbildlich bei der elektronischen Gesundheitskarte und der dazu gehörenden Telematik-Infrastruktur geregelt und wird bisher auch ohne Beanstandung umgesetzt; dennoch ist mangels hinreichender Transparenz der Datenverarbeitung noch viel zur Gewinnung des nötigen Vertrauens zu tun. Hinreichend Anlass zum Misstrauen haben die Bürger beim geplanten zentralen Melderegister mit einem großen Datensatz, der vielen Behörden als Bedarfsträgern zur Verfügung gestellt werden soll oder bei ELENA, dem geplanten Elektronischen Leistungsnachweis.

Auch im laufenden Betrieb ist die Beachtung der Gesetze Voraussetzung, um Vertrauen herzustellen: Als die Medien darüber berichteten, in welchem Ausmaß illegaler Datenhandel in Deutschland verbreitet ist, gerieten zwangsläufig auch die Meldebehörden in den Fokus der öffentlichen Aufmerksamkeit. Als bekannt wurde, dass viele Adresshändler nicht nur aus kriminellen Datenquellen schöpfen, sondern sich auch bei den Meldebehörden bedienen, indem sie die bei der Adressermittlung für Dritte erlangten Daten einfach für eigene Zwecke weiternutzen, waren die Meldebehörden gut beraten, diesem unzulässigen Tun umgehend einen Riegel vorzuschieben.

Viele Privilegien privater Datennutzung haben in unserer Informationsgesellschaft inzwischen ihre Daseinsberechtigung verloren, weil sie allzu sehr zum Datenmissbrauch einladen. Insofern sind die Reaktionen der Politik berechtigt, welche darauf abzielen, dass die Bestimmungsmöglichkeit über Datennutzungen bei den Betroffenen liegen muss. Dies bedeutet, dass die Betroffenen vor einer Datenweitergabe beispielsweise für Werbezwecke ihre aktive Einwilligung erteilt haben müssen, und dass sie dafür über die geplante Verarbeitung umfassend informiert sein müssen.

Überwachung und Fremdbestimmung ist mithilfe moderner IT heute leicht möglich. Möglich ist es aber auch, informationelle Selbstbestimmung, Transparenz und Wahlfreiheit technisch zu realisieren. Dies muss die Zielsetzung sowohl für die Privatwirtschaft wie für die öffentliche Verwaltung sein. Damit wird nicht nur die Bürger- beziehungsweise Kundenzufriedenheit erhöht. Ohne einen selbstbestimmten Einsatz von Informationstechnik würde zumindest mittelfristig die Freiheitlichkeit unserer Gesellschaft verloren gehen.

Dr. Thilo Weichert ist Landesbeauftragter für Datenschutz Schleswig-Holstein und Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) in Kiel.