Neue Technologien und informationelle Selbstbestimmung – Deutschland, Frankreich und die neuen Instrumente im Datenschutz

Sonja Korspeter und Alain Hermann[1]

Mikroelektronik, Kommunikationstechnik und Informationstechnologie werden ständig weiter entwickelt. Damit rückt die Vision einer umfassenden „Informatisierung" und Vernetzung der Welt immer näher, eine Entwicklung, die als allgegenwärtiges Rechnen bezeichnet wird. Funketiquetten auf RFID-Basis, multimediafähige Handys und Chips in Kreditkarten und Ausweispapieren sind dabei nur die ersten Vorboten. Bald lassen sich auch drahtlos miteinander kommunizierende Sensoren millionenfach in die Umwelt einbringen oder unsichtbar in Gegenstände einbauen.

Unterstützt durch neue Technologien der Ortsbestimmung erhalten Alltagsgegenstände damit völlig neue Funktionen: Sie können ermitteln, wo sie sich gerade befinden, welche anderen Gegenstände oder Personen in ihrer Nähe sind und was in der Vergangenheit mit ihnen geschah. Langfristig entsteht so ein „Internet der Dinge", das nachhaltige Auswirkungen auf viele Wirtschaftsprozesse und Lebensbereiche haben dürfte. Dies hat auch die EU-Kommission erkannt und im Jahr 2009 das Dokument „Internet der Dinge – Aktionsplan für Europa" veröffentlicht.

Die allgegenwärtige Datenverarbeitung erfordert eine Infrastruktur zur Erhebung und situationsadäquaten Auswertung personenbezogener Daten, die zugleich eine potentiell perfekte Überwachung ermöglicht. Interesse an derartigen Daten haben nicht nur Anbieter von Waren und Dienstleistungen, Arbeitgeber, Versicherungen, Auskunfteien oder Ermittlungsbehörden, sondern möglicherweise auch ein neugieriger Nachbar oder ein eifersüchtiger Liebhaber. Wenn technologische Innovationen die Welt lebenswerter machen sollen, so betont auch Alexander Roßnagel, Professor für Wirtschaftsrecht an der Universität Kassel, muss es gelingen, die Potentiale zur Verwirklichung der Träume von den Potentialen zur Realisierung der Alpträume zu trennen. Freiheit, Entfaltung und Demokratie zu fördern und – auch gegen technische Sachzwänge – zu schützen, ist die Aufgabe des Staates. Gegenwärtig erfüllen die europäische Rahmengesetzgebung und die Gesetze in Deutschland und Frankreich diese Aufgabe des Datenschutzes, doch es wird immer deutlicher, dass sie künftig nicht mehr ausreichen werden.

Bewusstsein für die Bedeutung des Datenschutzes

Die von den beiden Autoren erstellte Übersicht in Abbildung 1 zeigt die Entwicklung des Bewusstseins für Datenschutz in der Bevölkerung in Deutschland und Frankreich, wo ähnliche Trends beobachtet werden können: Das Thema Datenschutz gewinnt Ende der siebziger Jahre / Anfang der achtziger Jahre in der Öffentlichkeit an Bedeutung, obwohl die technologischen Möglichkeiten zur Überwachung im Vergleich zu den heutigen Standards noch sehr limitiert

[1] Sonja Korspeter ist Politikberaterin des European Milk Board. Alain Hermann arbeitet als Ingenieur für die Firma Procter & Gamble. Der Text gibt ausschließlich die persönliche Meinung der Autoren wieder.

waren. Zudem werden in dieser Zeit die nationalen Datenschutzbehörden eingerichtet. In den neunziger Jahren nimmt die Bedeutung des Themas in der öffentlichen Diskussion etwas ab, bevor in Folge der Terroranschläge in den USA im Jahr 2001 und der anschließenden Gesetzesänderungen eine erneute Sensibilisierung der Bevölkerung für den Datenschutz beobachtet werden kann. Doch nach wie vor können die Entwicklung der Gesetze und des Verhaltens der Bürger mit den rasenden technischen Entwicklungen (Street View, soziale Netzwerke, Smartphones, Geodatensysteme…) nicht Schritt halten.

Daher geht es heute darum, die Aufklärung der Öffentlichkeit voranzutreiben und das Bewusstsein für Datenschutz schnellstmöglich weiter zu entwickeln, damit Menschen und Organisationen mit den Chancen und Risiken der aktuellen und künftigen technologischen Möglichkeiten verantwortungsvoll umzugehen lernen.

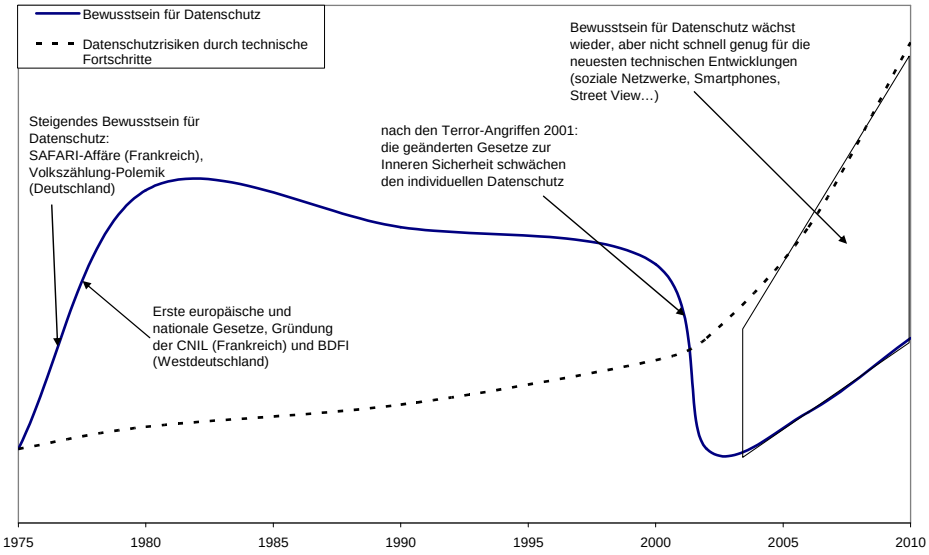

Abb 1: Entwicklung des Bewusstseins für Datenschutz in Frankreich und (West)deutschland (1975-2010) (eigene Darstellung)

Die Studie „Die Einstellung der Deutschen zum Thema Datenschutz“ des Allensbacher Instituts zeigt, dass das Bewusstsein für die Sensibilität persönlicher Daten in der Bevölkerung durchaus wächst. Allerdings zeigt sie auch, dass noch große Wissenslücken darüber bestehen, was mit den eigenen Daten passiert und wo die Grenzen ihrer legitimen Verwertung durch Dritte liegen. In Deutschland wie in Frankreich zeigt sich aber auch eine neue Tendenz zur bewussten Aufgabe von Privatheit. Rainer Kuhlen beschreibt diesen Trend in seinem Buch über Informationsethik.[2] Im Zeitalter von E-Commerce, Facebook und anderen personalisierten Dienstleistungen wird Privatheit nach Meinung Kuhlens zunehmend nicht mehr als absolute Voraussetzung für ein selbstbestimmtes Leben angesehen, sondern mehr und mehr zu einem aushandelbaren und partiell aufgebbaren Gut. Wenn genügend materielle Anreizangebote (z.B. Rabatte durch

[2] Kuhlen, Rainer: Informationsethik. Umgang mit Wissen und Information in elektronischen Räumen, Konstanz 2004.

Kundenkarten, Preisnachlässe bei Autoversicherungen mit direktem Einblick auf die Fahrweise des Autos) oder Komfortvorteile vorhanden sind, so zeigen sich immer mehr Personen bereit, freiwillig auf ihre Privatheitsrechte zu verzichten. Gerade jüngere Menschen geben in sozialen Netzwerken wie Facebook und in Internetforen bereitwillig Informationen über sich selbst preis.

Neue Herausforderungen des Datenschutzes

Wirksamer Datenschutz ist unerlässlich, um die Entstehung einer „gläsernen" Gesellschaft ohne Privatsphäre für den Einzelnen zu verhindern. Denn eine solche Entwicklung würde dazu führen, dass die Menschen aus Angst davor, dass ihre Daten missbraucht und sie selbst „durchschaubar" werden, langfristig weniger Informationen austauschen und sich mehr und mehr aus dem sozialen und politischen Leben zurückziehen. Der Handel ist gefährdet, wenn Firmen befürchten müssen, dass ihre vertraulichen Daten in falsche Hände geraten. Schon heute verursacht mangelnde Datensicherheit wirtschaftliche Schäden. Eine globale Studie des Anti-Virus-Herstellers Symantec aus dem Jahr 2010 zeigt, dass kleine und mittlere Betriebe in Folge von Datenmissbrauch einen durchschnittlichen Verlust von 188.000 Dollar pro Jahr erleiden.

Die Ziele, die mit dem zunehmenden Einsatz von Datenverarbeitung verfolgt werden, stehen häufig im Widerspruch zu den Grundsätzen des Datenschutzrechts. Bei einer Überarbeitung des Datenschutzrechts muss daher berücksichtigt werden, dass in den meisten Fällen die Datenerhebung von den Anwendern gewollt wird. Vorratsdatenspeicherung und Profilbildung wird von Millionen „Facebook-Friends" eindeutig gewünscht. Die bestehenden Prinzipien des Datenschutzes – Transparenz, Zweckbindung und seit einigen Jahren auch Erforderlichkeit und Datensparsamkeit – müssen daher überarbeitet werden.

Wir sehen drei Aktionsfelder, in denen gehandelt werden muss, damit auch in Zukunft das Internet und die mit ihm verknüpften neuen Möglichkeiten Freiheit und wirtschaftliche Aktivität fördern.

Anpassung des Datenschutzrechts

Die nationale Gesetzgebung im Bereich des Datenschutzes wird durch europäische Normen (zuletzt 2006/24/CE) bestimmt. Auf Ebene der Mitgliedstaaten sind institutionell nur geringe Unterschiede zu erkennen. Alle großen Länder haben ähnliche Datenschutzbehörden, wie die CNIL (Commission Nationale de l'Informatique et des Libertés) in Frankreich oder den BFDI (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit) in Deutschland. Allerdings, wie Alex Türk, der Präsident der CNIL, betont, sollte die Zusammenarbeit über Ländergrenzen hinweg vertieft werden, um die technischen und juristischen Erfahrungen beider Länder besser zusammenzuführen. Nur so könnten die Behörden den ständig neuen technologischen Anforderungen standhalten.[3]

[3] Alex Türk: 28th Conference of Data Protection and Privacy Commissioners, London November 2006.

An erster Stelle muss eine Anpassung der Datenschutzgesetze stehen, die technikneutral den Schutz der persönlichen Daten festschreibt. Hierzu zählt beispielsweise die Reglementierung der Profilbildung insofern, dass Profilbildung nicht komplett verboten, aber transparent und beeinflussbar gestaltet werden muss. Nutzer sollten möglichst weitgehend darüber informiert sein, durch wen, wie und für welchen Zweck die eigenen Daten verarbeitet werden und wie sie gegebenenfalls unkompliziert und direkt über das Internet Einspruch gegen die Nutzung erheben können. Auch der voreingestellte Datenschutz kann gesetzlich verankert werden. Anbieter von Produkten und Diensten müssten dabei sicherstellen, dass die Grundeinstellung ein Höchstmaß an Schutz der persönlichen Daten bietet und dass diese nur durch den Anwender bewusst veränderbar ist.

Selbstdatenschutz

Über die gesetzliche Ebene hinaus müssen Maßnahmen in einem weiteren Bereich stark ausgeweitet werden. So wie der Terrorismus nicht ausschließlich durch die Sicherheitsbehörden bekämpft werden kann, sondern die Wachsamkeit der Bevölkerung gefordert ist, kann der Datenschutz nicht nur durch Behörden gewährleistet werden. Der „Selbstdatenschutz" ist das wirksamste Datenschutzinstrument. Wenn die Bürger ihre Daten nur bewusst und mit großer Sorgfalt weitergeben, reduziert sich das Risiko des Datenmissbrauchs deutlich. Mit der geplanten Gründung einer Stiftung zur Finanzierung von Bildungsangeboten zum Umgang mit Daten zeigt die Bundesregierung, dass sie die Bedeutung des Selbstdatenschutzes erkannt hat. Auch in die Lehrpläne der Schulen sollte die Befähigung zum Umgang mit den eigenen Daten als Lernziel aufgenommen werden. Die Bundeszentrale für politische Bildung und die Landesämter für Datenschutz könnten auf die einzelnen Zielgruppen abgestimmte Lehrmaterialien herausgeben.

Die französische CNIL bietet allen Bürgern und Unternehmen auf ihrer Webseite umfangreiches Informationsmaterial über ihre Rechte und Pflichten sowie Ratschläge, wie private und vertrauliche Daten geschützt werden können. Die Webseite www.jeunes.cnil.fr erklärt Jugendlichen zwischen zehn und sechzehn Jahren, wie ihre Daten, die sie jetzt preisgeben, gespeichert werden und möglicherweise später gegen sie benutzt werden können. Es gibt also bereits mehrere vielversprechende Aufklärungsinitiativen, die Wirkung entfalten: Das Ergebnis einer Umfrage aus dem Jahr 2007 zeigt, dass fünfzig Prozent der befragten Franzosen die CNIL kennen. Der Bekanntheitsgrad der CNIL ist damit in den letzten Jahren gestiegen (34 Prozent im Jahr 2004), doch er muss weiter erhöht werden: Nur 26 Prozent der Franzosen haben den Eindruck, ausreichend über ihre Rechte informiert zu sein. Die Datenschutzbehörden müssen noch stärker in den Medien präsent sein, damit die Öffentlichkeit besser über die Risiken der neuen Technologien informiert ist und bewusster mit ihren Daten und denen anderer umgeht.

Die Bürger können als Verbraucher außerdem Druck auf Anbieter und Hersteller ausüben, damit diese akzeptable Datenschutzstandards einhalten. In den letzten Jahren haben beispielsweise die „Bio" und „Fair Trade" Gütesiegel stark an Bedeutung gewonnen und sind ein Beweis dafür, dass Verbraucher bereit sind, Firmen zu belohnen, deren Produkte gemäß bestimmter Standards

hergestellt werden.

Selbstregulierung datenverarbeitender Wirtschaftsbereiche

Hier liegt aus unserer Sicht der dritte Handlungsbereich, in dem sich ein Paradigmenwechsel abzeichnen könnte: Firmen sollten Datenschutz künftig als wirtschaftliche Chance statt als Einschränkung betrachten und den Schutz privater Daten schon in frühen Entwicklungsphasen ihrer Produkte berücksichtigen. Ziel wäre dabei ein eingebauter Datenschutz schon beim Design, durch den sich Unternehmen positiv von Konkurrenten abheben können.

Das Projekt EuroPriSe (European Privacy Seal – Europäisches Datenschutz-Gütesiegel) bietet IT-Firmen auf freiwilliger Basis an, ihre Produkte von unabhängigen Datenschutzexperten überprüfen zu lassen. Zertifizierte Firmen erhalten so einen Wettbewerbvorteil. Medien und Datenschutzbehörden können dazu beitragen, solche Projekte in der Bevölkerung bekannt zu machen, so dass Verbraucher über ihre Kaufentscheidungen datenschutzkonforme Produkte unterstützen können.

Die Zusammenarbeit auf europäischer bzw. internationaler Ebene wird künftig in einer Welt der allgegenwärtigen Datenverarbeitung für den Erfolg beim Schutz der persönlichen Daten entscheidend sein. Wikileaks, Google Street View, Minisensoren – auch wenn die nationale Gesetzgebung in diesen Fällen greifen kann, machen Daten vor Grenzen nicht Halt und es ist von zentraler Bedeutung für den künftigen Datenschutz, dass hohe, internationale Standards für den Umgang mit Daten vereinbart werden. Deutschland und Frankreich, mit ihren fest etablierten Datenschutzbehörden und der hohen Sensibilität der Bevölkerungen für Fragen des Datenschutzes, sollten bei diesem Thema eine Führungsrolle übernehmen und mit einer eindeutigen Gesetzgebung, Aufklärungsarbeit und der Förderung der Firmenverantwortung ein Beispiel setzen.