Exklusiv-Interview mit Peter Schaar

Bundesbeauftragter für den Datenschutz

Hartz IV und die Einführung der LKW-Maut sind herausragende politische Ereignisse Anfang 2005. Je nach Sichtweise werden hier datenschutzrechtliche Bedenken geäußert. Arbeitslose fühlen sich vom Staat ausgehorcht, Logistikunternehmen monieren vereinzelt, dass der Grundsatz der „datenfreien Fahrt" nicht mehr gewährleistet ist. Wie würden Sie heute das Rechtsbewusstsein in der Gesellschaft beurteilen, Datenschutz sinnvoll zu betreiben, Datenmissbrauch zu verhindern, Standards zu sichern und neue zu schaffen?

Peter Schaar: Das Grundrecht auf informationelle Selbstbestimmung ist ein unverzichtbarer Teil unserer Staats- und Gesellschaftsordnung. Dies hat das Bundesverfassungsgericht in seinem Volkszählungsurteil vom 15. Dezember 1983 unmissverständlich klargestellt. Datenschutz ist also nicht die Idee irgendwelcher Außenseiter, die sich dafür rechtfertigen müssten, dass ihre Forderungen sinnvoll und berechtigt sind, sondern ein Verfassungsgebot, das Gesetzgeber, Verwaltung und Rechtsprechung bindet. Im Einzelfall notwendige Beschränkungen des informationellen Selbstbestimmungsrechts müssen ihrerseits gerechtfertigt werden. Eingriffe und Beschränkungen des Grundrechts müssen geeignet, hinreichend bestimmt, erforderlich und verhältnismäßig sein.

Das Rechtsbewusstsein in der Gesellschaft ist zwiespältig. Auf der einen Seite sind die Bürgerinnen und Bürger sehr datenschutzbewusst, soweit sie sich selbst unmittelbar betroffen fühlen. Auf der anderen Seite wird diese Betroffenheit aber vielfach nicht wahrgenommen. Viele gehen mit ihren persönlichen Daten leichtfertig um und beachten Hinweise auf Gefahren und Missbrauchsmöglichkeiten eher wenig. Erst wenn sie selbst Opfer werden, entdecken sie den Datenschutz. Das macht es nicht immer einfach, die Anliegen des Datenschutzes in wirtschaftlichen und gesellschaftlichen Prozessen zu verankern und in der politischen Debatte durchzusetzen. Insgesamt wächst aber die Bedeutung des Datenschutzes.

Peter Schaar

Gleichzeitig wird heute – gerade vor dem Hintergrund von Bedrohungen durch den politischen Islamismus – zunehmend über die Frage diskutiert, ob es sinnvoll ist, Risiken und Gefahren für die Gesellschaft durch mehr Überwachungs- und Kontrollmöglichkeiten beizukommen oder nicht. Sind mit dem Einsatz neuer Technologien, wie biometrische Daten, RFID Chips, bundesweites Abrufen von persönlichen Bankdaten durch Finanzämter und andere Behörden Gefährdungen der Rechte des Einzelnen verbunden, oder anders formuliert, auf was sollte geachtet werden, dass eine solche Entwicklung nicht eintritt?

Peter Schaar: In der öffentlichen Diskussion dieser Fragen wird oft der Eindruck erweckt, es gäbe stets einen Zielkonflikt zwischen Datenschutz und anderen wichtigen Zielen, wie etwa innere Sicherheit und Kriminalitätsbekämpfung. Diesen Konflikt halte ich nicht für unüberwindbar. Es geht nicht um eine Wahl zwischen Datenschutz und innerer Sicherheit, sondern darum, hier zu einem angemessenen Ausgleich zu kommen oder sogar Lösungen zu finden, die beides ermöglichen. Als Grundrecht sichert das Recht auf informationelle Selbstbestimmung den Bürgerinnen und Bürgern einen Freiraum. Selbstverständlich kann und muss dieser Freiraum beschränkt werden, darauf habe ich bereits hingewiesen. Eingriffe, die dem Schutz vor terroristischen Anschlägen oder der Verhinderung und Aufklärung von Straftaten dienen sollen, sind vertretbar, soweit sie erforderlich und verhältnismäßig sind.

In der Diskussion geht es genau darum, ob vorgeschlagene zusätzliche Überwachungs- oder Kontrollmöglichkeiten tatsächlich das leisten werden, was versprochen wird, und ob die gleichen Ziele nicht mit weniger einschneidenden Mitteln erreicht werden können. Deswegen halte ich es auch für wichtig, dass zusätzliche Eingriffsbefugnisse vorab geprüft, zeitlich befristet und vor einer Verlängerung von unabhängigen Gutachtern bewertet werden. Es geht also nicht um Datenschutz oder innere Sicherheit, sondern um Verbesserung der inneren Sicherheit in datenschutzgerechter Weise. Auch wenn dies derzeit kaum realistisch erscheint, kann ich mir durchaus vorstellen, dass bestimmte einmal eingeführte Freiheitsbeschränkungen wieder zurückgenommen werden, insbesondere wenn sich die Gefährdungslage entschärft hat.

Auf Drängen der USA kommt es in der Europäischen Union noch in diesem Jahr zur Einführung von Pässen mit biometrischen Merkmalen. Welche Bedeutung hat dies aus datenschutzrechtlicher Sicht?

Peter Schaar: Mit der EU-Pass-Verordnung sollen das digitalisierte Passbild und Fingerabdrücke als biometrische Merkmale in die Reisedokumente der EU-Bürger aufgenommen werden. Soweit die Sicherheitsmerkmale in den Pässen der EU-Bürger weiter vereinheitlicht werden sollen, kann ich dies nur begrüßen. Allerdings muss die Ansicht, biometrische Merkmale in einem Chip würden die Pässe fälschungssicher machen, zumindest hinsichtlich der deutschen Pässe relativiert werden, denn der deutsche Reisepass gilt in Bezug auf Fälschungssicherheit als eines der hochwertigsten Dokumente der Welt.

EU-weit ist vorgesehen, die biometrischen Merkmale ab diesem Herbst in einem integrierten Funkchip zu speichern. Diese Technik beinhaltet Risiken in der praktischen Umsetzung. Noch ist nicht hinreichend geklärt, wie verhindert wird, dass der Inhalt des Chips beim Auslesen durch ein Lesegerät abgehört wird. Auch die Digitalisierung des Lichtbilds ist risikobehaftet, denn es könnte dazu genutzt werden, in einer Datenbank oder auf Videoaufnahmen nach einem Referenzbild zu suchen und damit die personenbezogene Überwachung zu ermöglichen. Auch wenn dies zurzeit noch nicht beabsichtigt ist, wird die Technik für eine solche Nutzung immer leistungsfähiger. Umso wichtiger ist es, dass die biometrischen Daten nicht in zentralen Dateien gespeichert werden sollen. Ich begrüße deshalb die entsprechenden Beschlüsse des Bundestages und des EU-Parlaments. Eine derartige Datenbank würde das Risiko des Missbrauchs und der Zweckentfremdung der sensiblen Daten erheblich erhöhen.

Elektronische Funketiketten sollen zunächst logistische Aufgaben im Handel erleichtern. Müssen bestehende Gesetze bei der Einführung der RFID-Chips für weitere Zwecke geändert werden? Kollidieren hier die Interessen von Wirtschaft und Handel sowie Datenschutzerfordernisse?

Peter Schaar: Die Radio Frequency Identification (RFID) dringt in immer weitere Bereiche unseres Lebens vor. Bald werden RFID-Chips in vielen Konsumgütern eingesetzt werden. Auch bei der Eintrittskarte zur Fußball-WM sollen die Funkchips genutzt werden. Denkbar und nicht unrealistisch ist die Verwendung dieser Technologie zur Überwachung von Kindern bis zur medizinischen Kontrolle und Versorgung von Patienten.

Die vielen Anwendungsmöglichkeiten sind kaum absehbar und genau darin liegt das Problem. Die RFID-Chips werden vom geltenden Gesetz nur zum Teil erfasst. Die Spezialvorschrift des § 6c BDSG ist leider nur anwendbar auf RFID-Chips mit integriertem Prozessorchip. Für andere RFID-Arten, auf denen Daten ohne Personenbezug hinterlegt werden, mangelt es an speziellen Vorgaben. So muss z. B. der Handel seine Kunden bisher erst dann darüber informieren, dass Chips in Waren integriert sind, wenn persönliche Daten damit verknüpft werden, etwa bei Verwendung der Kundenkarte. Dritte, die den Chip eventuell auch auslesen können, sind von dieser Regelung ohnehin nicht betroffen.

Aus meiner Sicht muss die Kennzeichnung für Produkte mit Chip sichergestellt werden. Außerdem brauchen wir ein Recht für den Betroffenen, die darin gespeicherten Informationen einzusehen und den Transponder nach dem Kauf permanent deaktivieren zu können. Das kann über eine Gesetzesänderung gehen. Für denkbar halte ich aber auch eine verbindliche Selbstverpflichtung von Handel und Industrie.

Das Bundesdatenschutzgesetz soll in absehbarer Zeit noch weiterentwickelt und modernisiert werden. Welche Änderungen im BDSG erachten Sie für notwendig?

Peter Schaar: Aufgrund der rasanten technologischen Entwicklung und der immer noch zunehmenden Nutzung entsprechender Verfahren und Produkte in praktisch allen Bereichen ist eine Anpassung der rechtlichen Bestimmungen überfällig. Für besonders wichtig halte ich auch eine Vereinfachung und Zusammenfassung des geltenden Datenschutzrechts. Hier sollte das Bundesdatenschutzgesetz eine möglichst einheitliche Grundlage werden, in der das Wesentliche für alle Bereiche geregelt ist. Ausnahmen und spezielle Vorschriften in anderen Gesetzen sollte es nur noch in dem Umfang geben, wie es unbedingt erforderlich ist.

Daneben sollten die Möglichkeiten für den Einzelnen verbessert werden, selbst für seinen Datenschutz zu sorgen, etwa durch präzisere Regelungen zur Einwilligung. Zudem ist die Möglichkeit für branchen- bzw. konzernspezifische Selbstregulierung und Selbstkontrolle zu erweitern. Auch der Datenschutz durch Technik ist noch verbesserungsfähig.

Europäische Einigung und Datenschutz gehören zusammen. Wie entwickelt sich angesichts gemeinsamer europäischer Aufgaben die Harmonisierung des Datenschutzes auf europäischer Ebene? Welches sind hier die „Hauptaufgaben“ in den nächsten Jahren?

Peter Schaar: Die europäische Datenschutzrichtlinie 95/46/EG aus dem Jahre 1995 stellt in ihrer staatenübergreifenden Verbindlichkeit weltweit das einzige Instrument seiner Art dar. Sie gilt auch in den Ländern des Europäischen Wirtschaftsraums (EWR).

Damit sind die Vorgaben der Richtlinie in nunmehr 28 europäischen Staaten verbindlich.

Mit seiner Harmonisierung im europäischen Binnenmarkt – dem Bereich der sog. Ersten Säule – hat der europäische Datenschutz eine neue Qualität erhalten. Wesentliche nationale Entscheidungen sind ohne Berücksichtigung der europäischen Dimension jetzt nicht mehr möglich, auch wenn dies durch die Öffentlichkeit nicht immer wahrgenommen wird. So wird die notwendige Anpassung des Datenschutzes an die sich dynamisch weiterentwickelnde Informationstechnik künftig wesentlich durch Entwicklungen auf europäischer Ebene bestimmt werden. Die praktische Bedeutung der EG-Datenschutzrichtlinie wurde noch dadurch erweitert, dass der Europäische Gerichtshof sie auch unabhängig von einem Bezug zum Binnenmarkt für anwendbar erklärt hat.

Das wichtigste Forum zur Harmonisierung der Datenschutzpraxis in den Mitgliedstaaten der EU ist nach wie vor die Gruppe nach Art. 29 der Datenschutzrichtlinie, einem Gremium, bestehend aus den Vertretern der nationalen Datenschutzkontrollbehörden. In den beiden zurückliegenden Jahren hat sich die Gruppe zu einer Vielzahl von Themen geäußert: Verabschiedet wurden Papiere, wie die jährlichen Berichte über die Entwicklungen der Gemeinschaft, der Mitgliedstaaten und Drittstaaten. Ausgearbeitet wurden ferner Positionspapiere zu einzelnen Rechtsfragen, etwa zum adäquaten Schutzniveau in Drittstaaten, zu Mustervertragsklauseln für Drittlandsübermittlungen oder zur Videoüberwachung. Weiter ging es um Positionen zum Arbeitnehmerdatenschutz, zur Direktwerbung und zur Speicherung von Verkehrsdaten bis hin zu den aktuellen internationalen Problemen in Folge des 11. September 2001.

Vor diesem Hintergrund habe ich wenige Wochen nach meinem Amtsantritt als Bundesdatenschutzbeauftragter den Vorsitz der Art.-29-Gruppe für zwei Jahre übernommen, auch wenn dies mit erheblichen Zusatzbelastungen verbunden ist. Als Vorsitzender muss ich nicht nur die teilweise unterschiedlichen Vorstellungen der jetzt 25 Mitgliedstaaten zusammenführen, sondern versuche auch, programmatisch-strategische Akzente zu setzen. Arbeitsschwerpunkte der Art.-29-Gruppe für dieses Jahr bilden zum einen Anwendungs- und Auslegungsfragen der Datenschutzrichtlinie. Zum anderen stehen sektorale Probleme wie der Arbeitnehmerdatenschutz, der Umgang mit Patientendaten oder biometrische Verfahren in Reisedokumenten sowie technische Herausforderungen (z. B. RFID, PETs, Genetische Daten) auf der Agenda.

Die im EU-Vertrag vorgesehene Schaffung eines „Raums der Freiheit, der Sicherheit und des Rechts“ ist in der Politik der EU an die vorderste Stelle getreten. Eines der wichtigsten Ziele besteht darin, einen ungehinderten Datenaustausch im Bereich der sog. Dritten Säule, also zwischen den nationalen Polizeibehörden und Organen der Strafverfolgung, zu gewährleisten. Ein harmonisierter europäischer Datenschutz auch für dieses Gebiet ist von der gleichen grundsätzlichen Bedeutung, wie es die EG-Datenschutzrichtlinie in den neunziger Jahren für den Bereich der Ersten Säule war. Dabei müssen einheitliche Rechtsgrundsätze, eine effektive Kontrolle der europäischen Informationssysteme und die Gewährleistung der Einbeziehung der unabhängigen Datenschutzbehörden in die Vorbereitung von Rechtsakten durch den europäischen Gesetzgeber gewährleistet werden.

Die 28. Datenschutzfachtagung (DAFTA) im November 2004 hatte das Leitthema „Orwells 1984 – 20 Jahre danach“. Eine kritische Reflexion scheint also angebracht, denn Orwell war ja bekanntlich ein glühender Verfechter der Freiheit des Individuums. Welchen Preis verlangt der heutige gesellschaftliche Fortschritt dem Individuum ab?

Peter Schaar: Der technologische Fortschritt, vor allem das weltumspannende Internet, hat sicherlich dazu beigetragen, dass eine unübersehbare Flut von personenbezogenen Daten anfällt, gespeichert, übermittelt und genutzt wird. Der nationale Gesetzgeber ist oft gar nicht mehr in der Lage, hier wirksam regelnd und kontrollierend einzugreifen. Die mit dem Fortschritt einhergehenden Probleme und Gefahren muss der Einzelne sicher bis zu einem gewissen Grad hinnehmen. Schutzlos darf er aber nicht werden. Wer das wirklich will, kann auch heute noch seine personenbezogenen Daten weitgehend vor Missbrauch schützen.

Voraussetzung dafür ist aber, dass der Einzelne seine Freiheitsrechte wahrnimmt, dass er informiert wird und sich informiert. Schließlich sollte er sorgfältig mit seinen Daten umgehen und sich überlegen, wie er sich datenschutzgerecht verhalten kann, damit sich seine Datenspuren in Grenzen halten. Wünschenswert ist auch, dass er technische Schutzmechanismen nutzt und sich gegebenenfalls gegen Missbrauch zur Wehr setzt, auch wenn das Zeit und Mühe kostet. Die „Bürde“ der Eigeninitiative kann ihm auch der Datenschutzbeauftragte nicht abnehmen. Andererseits müssen die öffentlichen und privaten Stellen, die Datenverarbeitung betreiben, ihren Verpflichtungen nachkommen. Dies bedeutet, dass auch hier verantwortliches Tun angesagt ist, das bei jeder Maßnahme die Auswirkungen auf die Bürgerrechte berücksichtigt.

Das Interview führte Jürgen Klocke