Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
16(4)176 B

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Peter Schaar
Bundesbeauftragter für den Datenschutz
und die Informationsfreiheit

Schriftliche Stellungnahme für die Öffentliche Anhörung zur Thematik

„Modernisierung des Datenschutzes“

1. Modernisierung des Datenschutzes

I.

In einem Artikel eines Informationsdienstes für Unternehmer, Manager und Marketingleiter hieß es im August 2005: „Bald wissen wir alles über die Kunden. Was Kunden kaufen, wann sie es kaufen und wo, was sie in ihrer Freizeit tun, wie sie leben – all das wird in wenigen Jahren offen liegen. Die Technologien dafür sind da, in den nächsten Jahren werden sie gebündelt und damit einen Strom von unbekannter Breite erzeugen: Rechnen Sie mit einer exponentiellen Vermehrung des Wissens über Ihre Kunden – und machen Sie sich das zunutze, bevor es Ihre Wettbewerber tun.“

Nicht nur der Staat, sondern vor allem die Wirtschaft hat – wie das Zitat anschaulich zeigt - schon seit langem das Potential von personenbezogenen Daten erkannt. Anders als im öffentlichen Bereich haben wir im privaten Sektor ein relativ freizügiges Datenschutzrecht, was etwa das Sammeln und Nutzen von Daten zu Werbezwecken, zur Bonitätsbewertung oder zur Bildung von Kundenprofilen betrifft. Dabei entwickelt sich gerade in diesem Bereich nicht nur die Quantität, sondern auch die Qualität der Datenerhebung und –verarbeitung immer schneller fort.

Erst 1991 wurde der Begriff vom „Ubiquitous Computing“ - übersetzt etwa mit allgegenwärtige Datenverarbeitung - in die Welt gesetzt. Heute ist diese beiläufige und umfassende Informationsverarbeitung in Teilen bereits Wirklichkeit. RFID-Chips, sogn. Funkchips, die die Ortung der mit ihnen versehenen Gegenstände ermöglichen, werden zwar noch vor allem im Transport und der Logistik eingesetzt - ein Bezug zum einzelnen Menschen ist aber längst nicht mehr nur Theorie. Im Rahmen eines von der EU mitfinanzierten Projekts wird derzeit am kleinen ungarischen Flughafen Debrecen mit einer Kombination von hochauflösenden Videokameras, hochempfindlichen Ortungsantennen und aktiven RFID-Chips, die fortlaufend ihre Position senden, jeder Passagier mittels einer ID-Nummer auf seiner Bordkarte geortet. Die ID-Nummer und Position wird an ein Videoüberwachungssystem übergeben. Bei Bedarf lassen sich sowohl im Videobild als auch im Lageplan alle Flugdaten des Passagiers über die ID-Nummer abrufen.

Dieses Beispiel ist leicht ausbaubar. Die Technik für eine solche Überwachung ist längst vorhanden. Zudem können heute immer mehr Daten immer länger gespeichert werden. Die In-

dustrie wetteifert ständig um die besten und leistungsfähigsten Systeme. Die Digitalisierung der Telekommunikation, der Ausbau des Mobilfunks verbunden mit immer neuen Anwendungen für das Handy, das stetige Wachsen des Internets und seiner Dienste lassen fast beiläufig ständig neue Nutzer- und Nutzungsdaten entstehen. Ortungstechniken, ob nun GSM, GPS oder künftig das noch präzisere Galileo-System, erlauben genaue Standortbestimmungen und Bewegungsprofile, auch ohne Wissen der Betroffenen oder sogar gegen ihren Willen.

Jeder von uns trägt bereits heute eine solche potentielle Identifizierungs- und Überwachungsmöglichkeit mit sich herum: seien es die Vielzahl unterschiedlicher Kunden- und Kreditkarten oder zukünftig die Gesundheitskarte und die Jobcard oder auch der neue elektronische Personalausweis. Sie alle können mit Funkchips ausgestattet werden. Dies wird dann geschehen, wenn eine solche Ausstattung als wirtschaftlich oder – bezogen auf den elektronischen Personalausweis – als politisch sinnvoll angesehen wird. Was aber könnte für die Wirtschaft interessanter sein, als Profile, die das Verhalten und die Interessen der betroffenen Menschen immer genauer abbilden?

Wenn einmal Daten gesammelt und gespeichert sind, wachsen schnell die Begehrlichkeiten, diese für eine Vielzahl von Zwecken einzusetzen. Dabei sind die Übergänge zwischen der staatlichen – und mit Sanktionen erzwingbaren – Datenerhebung und den privatwirtschaftlichen Datensammlungen längst fließend geworden: Wer kann denn ausschließen, dass Profile, die ursprünglich für Zwecke der Werbung, Risikobewertungen oder für Servicezwecke erstellt wurden, später in der Strafverfolgung, bei der Kriminalitätsprävention oder bei der Fahndung nach Schwarzarbeitern oder Steuerhinterziehern verwendet werden. So werden Genom-Analysen immer einfacher und genauer und könnten nicht nur bei der Kriminalitätsbekämpfung zum Einsatz kommen, sondern etwa auch im Versicherungsrecht oder im Arbeitsleben. An den Daten, die für die geplante Volkszählung 2010 gesammelt werden sollen, hat die Wirtschaft bereits heute ein lebhaftes Interesse und erhofft sich neue, aktuelle Datenbestände für eine noch genauere Profilbildung.

II.

Das Bundesdatenschutzgesetz gibt auf diese Herausforderungen keine zeitgemäßen Antworten. Es hinkt seit Jahren der gesellschaftlichen und technologischen Entwicklung hinterher. Die erste Phase der Novellierung des BDSG im Jahr 2001 hat nur Flickarbeit geleistet, aber kaum wegweisende Richtmarken für die Zukunft in der Informationsgesellschaft gesetzt. Die Mängel und Unzulänglichkeiten betreffen dabei viele Bereiche der datenschutzrechtlichen Arbeit.

Bereits der erste Zugriff auf das Datenschutzrecht macht es dem Leser und Anwender nicht leicht: Es ist in viele Einzelgesetze zersplittert, es gibt eine Flut von Spezialnormen, die nur schwer miteinander in Einklang zu bringen sind. Das Bundesdatenschutzgesetz ist zudem schwer lesbar und handhabbar, dies wiederum erschwert letztlich seine Akzeptanz.

In weiten Teilen des Wirtschaftslebens wird die Befolgung datenschutzrechtlicher Vorgaben heute durch vom Verbraucher bei Vertragsschluss unterzeichnete - häufig pauschal gehaltene - Einwilligungen praktisch ausgehebelt. Eine solche Einwilligung suggeriert Freiwilligkeit und Eigenverantwortung, bedeutet aber häufig nichts anderes als faktischer Zwang. Wer die

SCHUFA-Klausel unter seinem Vertrag nicht unterzeichnen will, erhält eben die Versicherung, das Handy oder auch die Wohnung nicht.

Nicht länger hinnehmbar ist das täglich wachsende Vollzugsdefizit. Zwar werden immer mehr Aufgaben an die Aufsichtsbehörden übertragen, dies geht aber nicht mit einer entsprechenden, insbesondere personellen, Aufstockung einher. Durch die komplizierte Aufsichtsstruktur werdend dabei auch die Verbraucher in die Irre geführt: für diese bleibt es häufig unklar, wer für den Schutz ihrer Daten zuständig ist. Unzureichend sind die Sanktionsmechanismen: Anzeige- und Unterrichtungsbefugnisse sind meist fruchtlos, nur in seltenen Fällen können Bußgelder verhängt werden. Anordnungen und Untersagungen kommen grundsätzlich nur bei technischen Mängeln in Betracht. Die Aufsichtsbehörden entpuppen sich gegenüber der Privatwirtschaft allzu oft als zahnlose Tiger.

Statt lenkend in den eingangs beschriebenen Datenstrom einzugreifen, müssen sich Datenschützer in einem juristischen Kleinkrieg immer wieder mit der Frage auseinandersetzen, ob überhaupt personenbezogene Daten vorliegen und sie eine Befugnis zur Prüfung und Kontrolle haben. Dies betrifft dabei keinesfalls Randbereiche, sondern gerade die Brennpunkte der Fortentwicklung der Informationsgesellschaft: so wird immer wieder vorgetragen, dass durch Funkchips eben keine Personen, sondern nur Gegenstände verfolgt werden, das Scoring beurteile keine individuellen Personen, sondern nur statistische Wahrscheinlichkeiten, mit der Georeferenzierung würden nur völlig harmlose geographische Daten erhoben. Allen diesen Daten ist aber gerade gemein, dass sie auf Menschen bezogen werden sollen, dass mit ihnen eine Aussage zu konkreten Personen verbunden werden soll. Doch statt sich Gedanken darüber machen zu können, wie hier eine verhältnismäßige Nutzung unter Wahrung der Verbraucherinteressen ermöglicht werden kann, werden Datenschützer allzu oft ganz aus der Diskussion verdrängt.

III.

Dieser Entwicklung möchte ich einen modernes Verständnis von Datenschutz und dem, was Datenschutzrecht leisten kann und soll, entgegensetzen. Wir müssen an dieser Stelle zu einer Ethik der Informationsgesellschaft kommen, die die Richtung zu einem verantwortungsvollen Umgang mit den technischen Möglichkeiten vorgibt. Dies bedeutet aber auch, dass das Datenschutzrecht nicht mehr nur statisch bloß den gegenwärtigen Stand der Technik reflektieren darf. Es kann nicht darum gehen, das Datenschutzrecht einmalig zu modernisieren und dann wieder zu vergessen, es muss vielmehr kontinuierlich an den neuesten gesellschaftlichen und technologischen Entwicklungen gemessen werden.

Den technologischen Fortschritt, die Entwicklung der Informationsgesellschaft will ich dabei keinesfalls aufhalten. Im Gegenteil: das Datenschutzrecht soll sich in diese dynamische Entwicklung einpassen, sie mitprägen und sich vor allem mit ihr weiterentwickeln. Es geht nicht darum, die Informationsgesellschaft aufzuhalten, aber sie darf nicht zu einer Überwachungsgesellschaft werden, der Mensch ist Subjekt, nicht Objekt der Information. Hier aber beginnt der politische Gestaltungsauftrag, die Pflicht, Grenzen zu definieren und eine Antwort auf die Frage zu geben, welchen Stellenwert der Mensch und sein Recht auf informationelle Selbstbestimmung in der Informationsgesellschaft hat.

Für die Datensammler bedeutet dies eine Pflicht zur Selbstbegrenzung verbunden mit einer klaren Verantwortung für die Verarbeitung der Daten. Ich sehe aber auch den einzelnen Bürger vor der Herausforderung, sich eigenverantwortlich um den Umgang mit seinen persönlichen Daten zu kümmern.

Dafür aber muss der Gesetzgeber die Position des Bürgers stärken und das derzeit bestehende Informationsungleichgewicht beheben. Nur der informierte Bürger kann seine Recht auch eigenverantwortlich und selbstbestimmt wahrnehmen. Hier gilt es die Informationspflichten entscheidend zu verbessern. Der Bürger muss verständlich informiert und über Datenströme über ihn benachrichtigt werden. In den Vereinigten Staaten ist es etwa möglich und machbar, dass jedem Bürger einmal im Jahr kostenlos mitgeteilt wird, welche Daten etwa Auskunfteien über ihn gespeichert haben. Der Auskunftsanspruch darf dabei auch nicht hinter einem vermeintlichen Geschäfts- oder Betriebsgeheimnis zurückstehen: d.h. Scoring-Komponenten, deren Berechnung und Gewichtung sind zu beauskunften, die Auskunftserteilung muss auch nicht gespeicherte, aber zusammengeführte Daten umfassen. Dabei dürfen Bürger nicht durch Kosten von der Nutzung dieser Rechte abgeschreckt werden.

Das moderne Datenschutzrecht muss sich auf ein allgemeines Gesetz gründen, das nur in erforderlichem Umfang durch bereichsspezifische Regelungen ergänzt wird. Es soll grundsätzliche und präzise Vorschriften zur Verarbeitung personenbezogener Daten enthalten und möglichst offene Abwägungsklauseln vermeiden.

Spezialgesetzliche Regelungen sollten auf das unabdingbar Notwendige beschränkt werden und nur noch die Ausnahme von den allgemeinen Regelungen enthalten und nur für bestimmte riskante Datenverarbeitungen die Anforderungen verschärfen oder bei unterdurchschnittlich riskanten Datenverarbeitungen Erleichterungen bieten.

Ein modernes Datenschutzrecht lebt dabei weniger von Verbot und Kontrolle als von der Einbeziehung des Datenschutzes in Planung und Entwicklung. Datenschutz muss zur Gestaltungsmaxime und Managementaufgabe öffentlicher und nicht-öffentlicher Stellen werden. Ich will hier nur zwei dafür wichtige Bereiche ansprechen: die Mechanismen der Selbstregulierung und den technologischen Datenschutz.

Mit Regeln zur Selbstregulierung sollen Anreize geschaffen werden, auf die Vereinheitlichung interner Verhaltensregeln in Unternehmen hinzuwirken. Hier muss ein gesetzlicher Rahmen geschaffen werden, der die Anforderungen und Rechtsfolgen von Selbstregulierungsmechanismen definiert und zugleich Mindestanforderungen zum Schutz der Betroffenen festlegt.

Im technologischen Datenschutz müssen Hard- und Software so gestaltet werden, dass in ihnen von vornherein der Datenschutz integriert ist. Datenschutzrechtliche Anforderungen müssen bereits bei deren Entwicklung berücksichtigt werden, Datenschutz muss systemintegrierter Bestandteil der Technik werden. Die technischen Möglichkeiten des Selbstschutzes müssen so einfach zu handhaben und so leicht zugänglich sein, dass sie auch jedermann ohne tiefgehende technische Vorkenntnisse nutzen kann.

Schließlich brauchen wir neue Mechanismen, um künftig Datenschutz zu gewährleisten. Dazu gehört eine Stärkung der Einwirkungsmöglichkeiten der Aufsichtsbehörden. Es muss einen

durch effektive und umsetzbare Sanktionsmöglichkeiten gestützten Schutz gerade für besonders sensible Daten und für gravierende Missbrauchsrisiken geben. Der Datenschutz darf nicht mehr nur auf dem Papier bestehen und sein Fehlen lediglich in den Tätigkeitsberichten beklagt werden.

2. Datenschutz-Audit

I.

Umfragen unter Internetnutzern, Versandhandels- oder Versicherungskunden darüber, wie groß das Vertrauen in eine sorgfältige Verarbeitung ihrer Daten bei diesen oder anderen Unternehmen ist, offenbaren regelmäßig ein großes Akzeptanzproblem. Wir alle – ob gewollt oder widerstrebend - ermöglichen heute täglich Dritten Zugang zu unseren persönlichen Daten, nicht immer jedoch fühlen wir uns dabei gut aufgehoben, sondern nehmen dies oftmals mit einem mulmigen Gefühl als notwendiges Übel hin. Akzeptanz aber hängt direkt mit dem Kaufverhalten zusammen, wenn ich mir Sorgen um den Umgang mit meinen Daten mache, schrecke ich eher davor zurück, im Internet zu bestellen. Vertrauen in die Datensicherheit der Technik ist daher eine wesentliche Voraussetzung für die Weiterentwicklung der Informationsgesellschaft.

Derzeit gibt es aber für Verbraucher und interessierte Unternehmen keine Möglichkeit, diesem Missstand zu begegnen. Zwar wird durch § 9a BDSG ein Datenschutzaudit als Gütesiegel angeboten. Danach können Anbieter von Datenverarbeitungssystemen und –programmen und datenverarbeitende Stellen zur Verbesserung des Datenschutzes und der Datensicherheit ihre Verfahren und Produkte bis hin zu ihrem Datenschutzkonzept durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Seit beinahe sechs Jahren läuft diese Bestimmung aber leer, da das für die Durchführung notwendige Ausführungsgesetz nicht beschlossen worden ist.

II.

Ich bin mir bewusst, dass der Ausarbeitung eines solchen Gesetzes vor allem die Befürchtung im Wege steht, durch das Datenschutzaudit fände eine weitere Bürokratisierung des Datenschutzrechtes zu Lasten der Wirtschaft statt, ohne dass diese ein solches Audit wollte oder aus ihm Nutzen ziehen könnte. Auch wird argumentiert, das Datenschutzaudit sei kostenträchtig. Außerdem werde die Stellung des betrieblichen Datenschutzbeauftragten entwertet. Neben die Selbstkontrolle durch den betrieblichen Datenschutzbeauftragten und die Fremdkontrolle durch die Aufsichtsbehörde trete nunmehr noch eine dritte Kontrolle durch das Datenschutzaudit.

Diese Kritik ist meines Erachtens nicht berechtigt. Im Gegenteil: das Audit ist gerade ein Schritt auf dem Weg zu einem verbraucherfreundlichen und nachfrageorientierten Datenschutz, in dem die Betroffenen nicht nur bloße Normadressaten sind, sondern den Datenschutz aktiv mitgestalten und fortentwickeln können.

Keinesfalls sollte das Datenschutzaudit als zusätzliche Kontrollinstanz verstanden oder gar konstruiert werden. Es sollte vielmehr als ein Angebot an die Privatwirtschaft ausgestaltet werden, Datenschutz nicht mehr gleichsam als lästige Pflichtübung anzusehen, sondern gezielt zum Teil einer Unternehmensphilosophie, einer Unternehmenskultur auszubauen. Daher ist das Datenschutzaudit keine verbindliche Verpflichtung für die Wirtschaft - im Gegenteil: dort, wo datenverabreitende Stellen zu der Überzeugung gelangen, dass ein Audit eine Verbesserung des Datenschutzes und der Datensicherheit bringen würde, können diese Stellen eine solche Zertifizierung erlangen, sie müssen es aber nicht.

Dieses Verständnis des Audit ist bereits in seiner grundlegenden Gestaltung angelegt: Durch das Audit wird nicht der Umgang mit personenbezogenen Daten in laufenden Betrieben kontrolliert, sondern es werden Datenverarbeitungssysteme und –programme sowie Datenschutzkonzepte zertifiziert, d.h. es wird von einem hierfür zugelassenen unabhängigen Gutachter geprüft und bestätigt, dass Systeme, Programme und Schutzkonzepte das leisten können, was von ihnen behauptet wird, und dass sie den gesetzlichen und technischen Vorgaben entsprechen. Dies schafft bei den Herstellern und Anwendern Investitionssicherheit und bei den Verbrauchern Vertrauen.

Auch die Freiwilligkeit des Audit ist daher keine Leerformel, sondern dessen grundlegendes Gestaltungsmerkmal. Freiwilligkeit meint dabei, dass jede Branche und jedes Unternehmen für sich anhand der Gegebenheiten in seinem Markt selbst entscheiden kann, ob ein Audit, etwa für ein neu einzuführendes Produkt oder ein anzuwendendes Verfahren, sinnvoll ist, und ob ein Werben mit einem geprüften Datenschutzsystem in den Augen der Kunden einen Wettbewerbsvorteil darstellt. So soll etwa ein Unternehmen sein Bestellverfahren im Internet damit bewerben dürfen, dass dieses Verfahren zertifiziert und seine Datenschutzzuverlässigkeit überprüft und festgestellt worden ist.

Auditverfahren haben sich dabei in vielen Bereichen des modernen Wirtschaftslebens etabliert, um allgemeine Probleme und Verbesserungsmöglichkeiten aufzuzeigen. Da regelmäßig auch die Wettbewerber ihre Prozessabläufe einer Analyse und Bewertung unterziehen, entwickelt sich innerhalb einer Branche der – beabsichtigte – Effekt einer ständigen Optimierung. Ein Audit führt so zu einer kontinuierlichen, praxisnahen Verbesserung der Arbeitsabläufe, nicht weil immer neue Anforderungen, etwa als gesetzlich verbindliche Regelungen aufgestellt werden, sondern weil im Wettbewerb der konkurrierenden Anbieter derjenige mit dem aktuellsten Systemen einen Wettbewerbsvorteil hat.

Interessant ist in diesem Zusammenhang eine Initiative von Microsoft in den USA. Bereits zum Jahreswechsel 2005/2006 hatte Microsoft Vorschläge für ein einheitliches und effektives US-Datenschutzrecht vorgestellt. Begründet wurde dieser Vorstoß damit, dass der Datenschutz ein Kundenbindungsinstrument darstelle, mit dem man durch Offenheit und Transparenz das Vertrauen der Kunden gewinnen und dauerhaft behalten könne. Darüber hinaus sei Datenschutz in zunehmendem Maße ein Wettbewerbsfaktor bei der Abgrenzung gegenüber anderen Marktteilnehmern.

Hierin zeigt sich ein marktwirtschaftlicher Datenschutzansatz, der bewusst darauf setzt, die Verwirklichung des Datenschutzes mit Anreizen des Marktes zu unterstützen. Dort, wo von den Verbrauchern ein Datenschutzsiegel als Vertrauensbonus gewertet wird, werden sich Unternehmen um ein solches bemühen. Ein datenschutzrechtlich vorbildliches Verhalten soll sich als Marketingargument nutzen lassen und durchaus in höheren Umsätzen auszahlen können. Umgekehrt führt eine Missachtung der Regeln zu einem Verlust.

Da in der sich herausbildenden Informationsgesellschaft die gesetzlich eingerichteten Kontrollstellen nicht überall auf den Plan treten können, führt eine derartige Einbindung der Verantwortlichen für die Datenverarbeitung zu einer deutlichen Entlastung der Aufsichtsbehörden. Wenn die Datenverarbeiter von Anfang an selbst mit „ins Boot“ genommen werden, ist der Gewinn für einen sich als präventiv verstehenden Datenschutz unübersehbar.

Gleichzeitig wird dadurch die bewährte Arbeitsteilung zwischen interner Datenschutzkontrolle durch betriebliche Datenschutzbeauftragte und externer Behördenaufsicht fortgeschrieben und der betriebliche Datenschutzbeauftragte gestärkt. An der Entwicklung entsprechender Datenschutzeinrichtungen und –konzepte wirken neben den Herstellern von Hard- und Software die betrieblichen Datenschutzbeauftragten mit, die nach einer Zertifizierung auch völlig eigenverantwortlich für die weitere datenschutzrechtliche Begleitung bei der Umsetzung der Konzepte zuständig bleiben.

Damit verbunden werden könnte eine partielle Freistellung von der externen Kontrolle seitens der Aufsichtsbehörden. Diese bräuchten nur noch anlassbezogen tätig zu werden, wenn konkrete Anhaltspunkte für einen Verstoß vorliegen; diejenigen hingegen, die sich nicht auf ein Gütesiegel verpflichtet haben, würden weiterhin der Daueraufsicht unterliegen.

Auch die Verbraucher würden von einem verbesserten Datenschutz profitieren. Das herkömmliche Aufsichts- und Kontrollverfahren des deutschen Datenschutzrechts leidet an einer letztlich zu geringen Kontrolldichte und daraus resultierenden spürbaren Vollzugsdefiziten. Konkret bedeutet dies nichts anderes als schlichte Folgenlosigkeit für viele Fälle unzureichender Datenschutzpraxis.

III.

Damit das Datenschutzaudit diese Erwartungen erfüllen kann, sind verbindliche Rahmenbedingungen für Datenschutz-Gütesiegel notwendig, um den Unternehmen, die sich einer Auditierung unterziehen wollen und auch den Verbrauchern eine Gewähr dafür zu bieten, dass das vergebene Prädikat auch wirklich die Einhaltung bestimmter Datenschutzstandards gewährleistet. Ohne verbindliche Kriterien und Verfahren kann dieses Instrument seine positive Wirkung nicht entfalten. Wirtschaft und Verwaltung sind seit Jahren im Ungewissen, ob und wann ein Ausführungsgesetz erlassen wird. Es droht so die Verschwendung finanzieller und personeller Ressourcen.

§ 9a BDSG ist Ausdruck für einen neuen, modernen Ansatz im Datenschutzrecht. Datenschutz ist hier nicht restriktiv als Behinderung zu begreifen, sondern positiv einzusetzen als Mittel des wirtschaftlichen Wettbewerbs, als verkaufsförderndes Plus, das die Sorgen der Anwender und Konsumenten aufgreift und ihnen abhilft.

Ich glaube, dass wir ohne einen funktionierenden Datenschutzaudit eine wichtige Weiterentwicklungsmöglichkeit des Datenschutzrechtes verpassen.

3. Scoring und Unternehmensinformationspflicht bei Datenschutzpannen

I.

Das Thema Scoring und die Pflicht von Unternehmen, Informationen über Datenschutzpannen zu veröffentlichen, berühren eine der zentralen Fragen des Datenschutzrechtes: wie kann ich als mündiger und datenschutzrechtlich sensibilisierter Bürger den Umgang mit meinen Daten kontrollieren?

Seit Jahren fordern wir Datenschützer die Bürger dazu auf, sich den Umgang mit ihren Daten bewusst zu machen und genauer hinzuschauen, wer welche Daten über sie speichert und zu welchem Zweck dies geschieht. Ich halte dies nach wie vor für berechtigt. Jeder Bürger sollte sein bester Datenschützer sein, doch kann dies unter den gegenwärtigen Umständen eigentlich redlich von den Bürgern verlangt werden? Sowohl beim Scoring als auch bei Datenschutzpannen in Unternehmen stößt der Betroffene nämlich schnell an die Grenzen dessen, was er überhaupt zu seinem eigenen Schutz leisten kann.

II.

Zur Transparenz gehört notwendigerweise die Forderung, die Betroffenen darüber zu informieren, wenn ihre Daten verloren gegangen sind oder gestohlen wurden.

Daten sind heute zu einem wertvollen und interessanten Gut geworden. Interessant aber etwa auch für Hacker, die sich online unbefugten Zugriff verschaffen, eigene Angestellte der datenverarbeitenden Stelle, die Daten missbräuchlich verwenden, oder Dieben, die gleich mit dem Brecheisen einsteigen und den gesamten PC oder Laptop mit samt der Daten stehlen. Diese Beispiele sind keine Erfindungen, sondern leidvolle Erfahrungen, die vor allem in den USA gemacht werden. Einige der größten Diebstähle von persönlichen Informationen ereignete sich Mitte letzten Jahres, als Sicherungsbänder eines weltweiten Finanzinstituts auf dem Transit vom Laster des Kurierunternehmens fielen. Die Bänder enthielten Sozialversicherungsnummern von fast vier Millionen Kunden. Daten werden aber auch durch Nachlässigkeit gefährdet: etwa wenn sie versehentlich auf Internetseite publik gemacht worden sind.

Millionen Nutzer von Kreditkarten fürchteten im Frühjahr letzten Jahres um ihr Geld. Hacker hatten in den USA über ein Sicherheitsleck bei einer Abrechnungsfirma die Daten von 40 Millionen Karteninhabern gestohlen, teilten die beiden größten US-Kreditkartenunternehmen Mastercard und Visa mit. Allein bei Mastercard sollen knapp 14 Millionen Kunden betroffen sein, für 68.000 davon besteht nach neuesten Informationen ein "erhöhtes Risiko". Auch unter deutschen Kreditkartenbesitzern war die Verunsicherung groß. Dies war der bisher größte bekannte Fall von Datendiebstahl in der Kreditkarten-Branche.

Der Staat Kalifornien hat diese Erfahrungen 2003 zum Anlass für ein neues Gesetz genommen, das inzwischen von 33 weiteren US-Bundesstaaten und New York übernommen wurde: das Security Breach Information Act. Derzeit wird darüber nachgedacht, ob ein einheitliches föderales Gesetz die Rechtslage vereinheitlichen soll. Auch Kanada erwägt inzwischen darüber, ein solches Gesetz einzuführen.

Das Security Breach Information Act verpflichtet Unternehmen, die Betroffenen davon zu unterrichten, wenn auf die sie betreffenden Daten unrechtmäßig zugegriffen wurde oder die Daten gesetz- bzw. vertragswidrig genutzt wurden. Damit werden die Betroffenen in die Lage versetzt, Vorkehrungen zu treffen, um das Risiko von Folgeschäden zu vermindern. Die Kenntnis von der Tatsache eines Datenmissbrauchs ist jedoch auch eine Voraussetzung dafür, dass die Betroffenen zivilrechtlich gegen die Verantwortlichen vorgehen und ggf. Schadensersatz geltend machen können. Schließlich – und dies halte ich für den bedeutsamsten Effekt – bestraft der Markt die Unternehmen, die mit den Daten nicht sorgfältig umgehen.

In den USA war nach Einführung des Gesetzes zu beobachten, dass sich Unternehmen verstärkt Gedanken über Datensicherheit machen und eigene Strategien für einen verbesserten Datenschutz entwickelt haben. Letztlich kann auch nur eine schnelle Information der Betroffenen dabei helfen, die Schäden so gering wie möglich zu halten: wenn zum Teil tausende von Daten gestohlen oder missbraucht werden, ist anders eine schelle Reaktion der Betroffenen kaum möglich. Nur so haben sie die Chance, Gegenmaßnahmen zu ergreifen, um weitere negative Folgewirkungen zu begrenzen oder zu verhindern. Ein entsprechendes Gesetz sollte auch bei uns ein Umdenken der Unternehmen bewirken: Ich denke, dass wir in Europa diesen Anstoß aufnehmen sollten. Warum sollen die europäischen Verbraucherinnen und Verbraucher in dieser Hinsicht schlechter gestellt sein als die Bewohner von inzwischen mehr als dreißig US-Bundesstaaten? Ich finde, dies ist ein neuer interessanter Aspekt in der Debatte über ein angemessenes Datenschutzniveau.

III.

Beim Scoring-Verfahren werden Verbraucher durch spezielle Unternehmen auf ihre Kreditwürdigkeit hin beurteilt. Das Ergebnis soll dem potentiellen Vertragspartner helfen zu entscheiden, ob etwa ein Kauf auf Rechnung angeboten werden kann, ob ein Kredit gewährt werden soll und – wenn ja – zu welchen Konditionen. Es handelt sich dabei um Verfahren, die auf mathematisch statistischer Grundlage Risikoklassen bilden, denen dann Kreditsuchende, Kaufinteressenten etc. zugeordnet werden und die dann je nach Branche anhand hunderter Kriterien angeblich ein Bild von deren Bonität zeichnen. Mit den Verfahren soll die Kreditwürdigkeit weitgehend unabhängig vom tatsächlichen Verhalten des Betroffenen beurteilt werden, selbst dann, wenn keinerlei negative Informationen über das Zahlungsverhalten einer Person aus der Vergangenheit vorliegen.

Ohne diese Informationen, so die Begründung der Wirtschaft, wäre eine Kreditvergabe nicht mehr oder nur zu erheblich schlechtern Konditionen möglich. Mit dieser Argumentation gewinnen Scoring-Verfahren einen immer größeren Einfluss auf wirtschaftliche Entscheidungsprozesse und längst ist dieses Argument nicht mehr auf die Vergabe von Krediten beschränkt. Es gibt heute kaum noch wirtschaftliche Entscheidungen, die ohne Hinzuziehung solcher Verfahren getroffen werden.

So wird inzwischen auch beim Abschluss von Versicherungsverträgen, dem Kauf im Internet und beim Versandhandel, beim Anmieten einer Wohnung oder vor dem Abschluss eines Handyvertrages mittels eines Score festgestellt, wie hoch das Risiko bei einem bisher unbescholtenen Kunden ist, seinen Vertragspflichten nicht nachzukommen. Dieses Aussieben nach Arm und Reich ist zu einem wichtigen Instrument im Produktmarketing geworden. Bestellt man eine Ware per Internet, läuft in der Regel bereits während des Erhebungsvorgangs der Ad-

ressdaten ein Scoring-Verfahren ab, von dessen Ergebnis es der Händler abhängig macht, ob er nur Lieferung per Nachnahme oder auch Zahlung gegen Rechnung anbietet. Dies geschieht mit dem Argument, dass bereits der Kauf auf offene Rechnung ein existentiell bedrohendes Risiko für ein Unternehmen darstelle: Ohne vorheriges Scoring könne daher kein Verbraucher mehr einen solchen Kauf auf Rechnung tätigen.

Prinzip und Konsequenzen dieser Verfahren sind immer gleich: Kunden mit schlechtem Score bekommen schlechtere Konditionen. Sie zahlen höhere Zinsen für Kredite, können Waren nur per Vorkasse bestellen oder werden als Kunden erst gar nicht akzeptiert. Dies ist nichts anderes als eine neue Form der Diskriminierung, die Menschen zum Opfer einer erhöhten statistischen Wahrscheinlichkeit macht.

Die Zunahme der Scoring-Verfahren ist daher nicht nur datenschutzrechtlich, sondern vor allem auch gesellschaftspolitisch bedenklich. Scoring-Verfahren nehmen dem Einzelnen die Möglichkeit, selbst über sein Erscheinungsbild in der Öffentlichkeit zu entscheiden oder dieses durch eigenes rechtstreues Verhalten auch nur beeinflussen zu können. Mehr noch: dem Einzelnen wird auch das Wissen darüber vorenthalten, wie sich sein „Wert“ für die Gesellschaft bestimmt, wie konkret sein Score-Wert berechnet wurde und weshalb bei ihm etwa ein besonders hohes Risiko dafür besteht, dass er einen Kredit nicht zurückzahlen kann. Völlig unklar ist, wie sich der Score errechnet und welche Merkmale mit welcher Wertigkeit berücksichtigt werden: Hier verbergen sich aber erhebliche Risiken: Falschmeldungen an die Auskunfteien, unbefugte Weitergabe von Daten, Verwendung dieser Daten für Score-Berechnung, was etwa zum Verlust der Kreditwürdigkeit führen kann. Der Betroffene wird durch die Berechnung eines Score nicht nur argumentativ in die Defensive gedrängt: er hat auch keine Möglichkeit, die Berechnung zu überprüfen und Gegenargumente vorzutragen.

Die Daten stammen nur zum Teil von den Konsumenten selber - durch Teilnahme an Bonusprogrammen, Kundenkarten etc. Ein Teil der Daten, die beim Scoring verwendet werden, sind zudem aus dem Verhalten der Betroffenen gewonnen worden: Ist er häufig umgezogen? Hat er kürzlich ein Konto eröffnet oder einen Kredit beantragt? Zu einem großen Teil sind es zudem scheinbar harmlose statistische und soziodemografische Daten über die Bewohner von Straßenabschnitten oder Stadtbezirken. Mithilfe intelligenter Software werden daraus aber individuelle Konsumentenprofile. Da statistische Daten und soziodemografische Daten separat gesehen keine personenbezogenen Daten sind, bewegt sich das Scoring in einer juristischen Grauzone. Intelligent verknüpft und einzelnen Personen zugeordnet, werden aus all diesen zunächst „harmlosen“ Daten personenbezogene Daten.

Wer aber weiß schon, was etwa Wirtschaftsauskunfteien über einen selbst gespeichert haben. Die wenigsten Bürger nehmen die Möglichkeit einer Selbstauskunft wahr. Um umfassend informiert zu sein, müsste man jedoch auch bei allen in Deutschland tätigen Auskunfteien nachfragen, ob und ggf. welche Daten über einen gespeichert sind. Trotz der grundsätzlich im Datenschutzgesetz verankerten Kostenfreiheit muss der Bürger für jede erteilte Auskunft bezahlen – und dies bei jeder Auskunftei. Wenn er dann noch seinen Score erfahren möchte, zahlt er wieder extra.

Zwar erklärte sich eine Auskunftei inzwischen bereit, Betroffenen auf Nachfrage deren tagesaktuellen Score-Wert mitzuteilen, nicht jedoch den tatsächlich dem jeweiligen Vertragspartner übermittelten Score-Wert. Im Sinne einer verbesserten Transparenz halte ich es für not-

wendig, dass der Betroffene auch diesen Wert erfährt, der ggf. zu ihn betreffenden Entscheidungen – etwa zur Ablehnung eines Kreditantrags – beigetragen hat. Eine Begrenzung des datenschutzrechtlichen Auskunftsanspruchs des Betroffenen unter Berufung auf „Betriebs- und Geschäftsgeheimnisse“ des Unternehmens halte ich nicht für hinnehmbar. Hier ist der Gesetzgeber gefordert.

Deshalb sind klare rechtliche Rahmenbedingungen notwendig, auch um eine solide und bonitätsrelevante Datengrundlage zu gewährleisten. Hier sind branchenspezifische Regelungen erforderlich und insbesondere eine Beschränkung auf relevante individuelle Informationen zu Zahlungsverhalten, Einkommens- und Vermögensverhältnissen, denn aus der Sicht eines Kreditunternehmens sind andere Daten bonitätsrelevant als für einen Wohnungsvermieter oder Handyanbieter. Branchenübergreifende Auskunfteisysteme sind dagegen zu begrenzen.