Berliner Beauftragter für
Datenschutz und Informationsfreiheit

Berlin

Berlin sagt Nein
zu Fremdenfeindlichkeit
und Gewalt

741.619.5

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
16(4)176 D

26. Februar 2007

Stellungnahme bei der öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages zum Thema „Modernisierung des Datenschutzes“ am 5. März 2007

I. Modernisierung des Datenschutzes

Die Modernisierung des Datenschutzes ist zwingend geboten, weil die derzeitige Gesetzeslage keinen hinreichenden Schutz des Rechts auf informationelle Selbstbestimmung gewährleistet.

Hierzu sind bereits mehrere Studien verfasst worden, welche grundlegenden Defizite des derzeit geltenden Datenschutzrechts ausführlich analysieren (vgl. z.B. Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts, Studie im Auftrag des Bundesministeriums des Innern, 2001; Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Erhöhung des Datenschutzniveaus zugunsten der Verbraucher, Studie im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft, 2006). Ich beschränke mich deshalb darauf, einige aus meiner Sicht besonders relevante Aspekte anzusprechen.

1. Herausforderungen an das Datenschutzrecht

In besonderer Weise muss das Datenschutzrecht der **rasanten technologischen Entwicklung** angepasst werden. Die Informationstechnologie ermöglicht eine Massendatenverarbeitung auf immer kleineren Datenträgern und Verarbeitungsmedien. Technologische Grenzen verlieren dabei an Stellenwert. Diese technologische Entwicklung führt dazu, dass die Verarbeitung personenbezogener Daten in ihrer Gesamtheit nicht nur im Bereich der öffentlichen Stellen (Gefahrenabwehr und Strafverfolgung), sondern auch und gerade im Bereich der Privatwirtschaft immer näher an den absolut zu schützenden Kern privater Lebensgestaltung der Betroffenen heranrückt.

Zugleich ist die Tendenz zu beobachten, dass im Rahmen der automatisierten Verarbeitung von Daten die **Grenzen zwischen Personenbezug und Nichtpersonenbezug verschwimmen**. Zwei Beispiele dazu: Unternehmen werten georeferenzierte Daten aus, um anhand des Wohnorts den „Wert“ von potentiellen Kunden abschätzen zu können. Die 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung vom 27. Oktober 2006 bereits darauf aufmerksam gemacht, dass der Einsatz von RFID-Tags (Radio Frequency Identification) unaufhaltsam Einzug in den Alltag hält. Schon jetzt werden sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich viele Gegenstände mit diesen miniaturisierten IT-Systemen gekennzeichnet. Es ist zu erwarten, dass neben bereits jetzt mit RFID-Technik gekennzeichneten Lebensmitteln künftig auch Personalausweise, Geldscheine,

Kleidungsstücke und Medikamentenpackungen mit RFID-Tags versehen werden. Mit Hilfe der **Nanotechnologie** wird die Miniaturisierung möglicherweise so weit voranschreiten, dass die RFID-Etiketten auf Staubkorngröße reduziert werden (**smart dust**). In wenigen Jahren könnten praktisch alle Gegenstände des täglichen Lebens weltweit eindeutig gekennzeichnet sein. Die flächendeckende Einführung derart gekennzeichneter Gegenstände birgt erhebliche Risiken für das Recht auf informationelle Selbstbestimmung in sich. Die RFID-Kennungen verschiedenster Gegenstände können sowohl miteinander als auch mit weiteren personenbezogenen Daten der Nutzenden - in der Regel ohne deren Wissen und Wollen - zusammengeführt werden. Auf diese Weise werden detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile von Betroffenen ermöglicht.

Hinzuweisen ist auch auf die zunehmende **Internationalisierung der Datenflüsse**. Die internationale Verflechtung von Unternehmen bringt es mit sich, dass Daten im großen Umfang weltweit kursieren. Die Weitergabe von Flugdaten und von Bankdaten (SWIFT) an US-amerikanische Sicherheitsbehörden sind ein Beispiel dafür, dass es nicht bei einem Datentransfer unter nichtöffentlichen Stellen bleibt.

Mit der technologischen Entwicklung und der Internationalisierung von Datenflüssen geht das Problem der **abnehmenden Transparenz** von Datenverarbeitung und Datenbeständen, von Technik und Wirtschaftsverflechtung usw. für Nichtfachleute einher. Gleichzeitig ist das Phänomen zu beachten, dass in der Bevölkerung das Bewusstsein für den Schutz von Privatsphäre sehr unterschiedlich ausgeprägt ist. Häufig geben Personen freiwillig oder unachtsam Informationen über sich preis, entweder weil sie die Tragweite ihrer Entscheidungen nicht überschauen oder weil es ihnen solange gleichgültig ist, bis sie die negativen Auswirkungen der Datenverwendungen konkret spüren. In diesem Moment ist es jedoch häufig zu spät, um die Folgen einer Datenverarbeitung für die Betroffenen noch abzuwenden.

Das **Rechtsinstitut der Einwilligung**, das seinem Grundgedanken dazu dient, dem Einwilligenden die individuelle Steuerung von Datenverarbeitungsflüssen zu ermöglichen, wird in **Massengeschäften** durch faktischen Zwang zur Erklärungsabgabe und Standardisierung **entwertet**.

2. Lösungsansätze

Grundsätzlich empfehle ich, einen am **Gedanken der Risikoadäquanz orientierten, abgestuften Datenschutz** zu entwickeln. Um Missverständnissen vorzubeugen: Der Gesetzgeber hat für unterschiedliche Regelungsbereiche zahlreiche bereichsspezifische Normen geschaffen, die sich aber inhaltlich kaum voneinander unterscheiden. Dies meine ich nicht, wenn ich von einem abgestuften Datenschutzregelungskonzept spreche.

Vielmehr sollte der Gesetzgeber die allgemeinen Regeln, die bereits im BDSG enthalten sind, durch teilweise sehr konkret zu fassende Regelungen ergänzen, wenn dies erforderlich erscheint. Sind Datenverarbeitungsprozesse besonders gefahrengeneigt, haben sie erfahrungsgemäß eine besondere Nähe der Daten zum Persönlichkeitskern der Betroffenen? Dann ist der Gesetzgeber aufgrund seiner verfassungsrechtlichen Schutzpflichten gehalten, konkrete Schutzregeln zu schaffen, die Verarbeitungsinteressen klare Grenzen setzen. Insbesondere genügt es nicht, wie in den §§ 28, 29 BDSG eine abstrakte Interessenabwägungsklausel vorzusehen, die den verantwortlichen Stellen eine Einschätzungsprärogative über die Zulässigkeit der Datenverarbeitung einräumt.

Um die Problematik anhand eines Beispiels aufzuzeigen: Das Datenverarbeitungsverhalten des Auskunfteiwesens zeigt, dass § 29 BDSG mit seinen allgemein gehaltenen Abwägungsklauseln nicht genügt, um die Risiken für die Betroffenen angemessen zu begrenzen. Nach dieser Vorschrift sollen die verantwortlichen Stellen die Rechtmäßigkeit der Verarbeitung personenbezogener Daten beurteilen, die selbst an der Sammlung und Veräußerung möglichst vieler Daten wirtschaftlich interessiert sind. Das Ergebnis solcher Abwägungsvorgänge steht von vorneherein fest. Aufgrund der zu allgemein gehaltenen gesetzlichen Vorgaben können die Aufsichtsbehörden dem auch nicht effektiv entgegenwirken. Erforderlich sind insoweit klare und konkrete Regelungen.

Liegen keine solchen gefahrenträchtigen Datenverarbeitungsvorgänge vor, kann das allgemeine Datenschutzrecht gelten. Man kann dabei durchaus Ansätze zur Selbstregulierung fördern. Datenschutz bereits bei der Technologieentwicklung kann dabei durch Standardisierungen und die Schaffung von Anforderungsprofilen gestärkt werden.

Ich hatte bereits das Problem aufgezeigt, dass es Datenverarbeitungsvorgänge gibt, die sich im „**Vorfeld des Personenbezugs**“ bewegen. Sie bergen für die Betroffenen häufig ebenso große Risiken wie die Verarbeitung personenbezogener Daten. Deshalb sollten sie normenklar in den Anwendungsbereich des Datenschutzrechts einbezogen werden.

Transparenz- und Verarbeitungsregeln sollten zugunsten der Betroffenen gestärkt werden. Sie sollten so ausgestaltet werden, dass die Betroffenen nicht den Eindruck haben, dass die Geltendmachung ihrer Rechte ohnehin sinnlose Mühe darstellt. Um eine Formulierung des Bundesverfassungsgerichts aufzugreifen: Der Gesetzgeber ist gehalten, den Betroffenen die **Mittel zum „informationellen Selbstschutz“** an die Hand zu geben (Beschluss von 23. Oktober 2006 – 1 BvR 2027/02 -).

Ich möchte dies anhand der derzeitigen Gesetzeslage veranschaulichen, die für die Verwendung personenbezogener Daten zu Zwecken der Werbung, zu Markt- und Meinungsforschung gilt. Sie ist zu Lasten der Verbraucher sehr wirtschaftsfreundlich ausgestaltet. Dies beeinträchtigt die Verbraucher erheblich in ihren Persönlichkeitsrechten.

So entspricht es dem Alltag in der Werbewirtschaft, dass Unternehmen Adressdaten ihrer Kunden an so genannte Adresshändler verkaufen. Diese übermitteln die Daten an andere Unternehmen, welche die Betroffenen zu Werbezwecken anschreiben. Wie sich aus § 28 Abs. 3 Nr. 3 BDSG ergibt, ist ein solcher Vorgang derzeit in aller Regel legal, es sei denn, der Betroffene widerspricht der Übermittlung seiner Daten.

Das bedeutet praktisch: Will ein Bürger keine direkten Werbezuschriften mehr erhalten, muss er sich *an jedes* Unternehmen wenden, das seine Daten zu Werbezwecken nutzt. Es liegt auf der Hand, dass ein solches Bemühen von normalen Bürgern gar nicht geleistet werden kann.

Der Deutsche Direktmarketing Verband unterhält zwar eine so genannte „Robinsonliste“, in die man sich eintragen lassen kann. Die dem DDV angeschlossenen Unternehmen erhalten dann die Nachricht, dass der Betroffene keine Werbezuschriften wünscht. Angeblich soll ein Eintrag in diese Liste zu einer gewissen Reduzierung der Werbezuschriften führen. Eine verbindliche Pflicht der angeschlossenen Unternehmen, den Eintrag zu respektieren, gibt es aber nicht. Überdies gilt der Eintrag lediglich für fünf Jahre und muss dann erneuert werden.

Auch hat sich herausgestellt, dass die bisherigen datenschutz- und wettbewerbsrechtlichen Regelungen nicht ausreichen, um die Probleme mit **cold calls, SPAM und Werbefaxen** in den Griff zu bekommen. Ich begrüße Bestrebungen der Bundesregierung, die im Zusammenhang mit Änderungen von wettbewerbsrechtlichen Regelungen Verbesserungen schaffen will. Gleichzeitig rege ich an, dass das Verhältnis dieser Vorschriften zum BDSG klar geregelt wird.

Ich mache auch darauf aufmerksam, dass die **Stellung des betrieblichen Datenschutzbeauftragten** in § 4 f BDSG nicht angemessen geregelt ist. Die Erfahrung zeigt, dass die funktionelle Weisungsfreiheit des betrieblichen Datenschutzbeauftragten unzureichend ist. Eine wirkliche Weisungsfreiheit setzte einen deutlich verbesserten Kündigungsschutz voraus. Der betriebliche Datenschutzbeauftragte sollte analog dem Betriebsratsmitglied Kündigungsschutz genießen, selbst dann, wenn ein Datenschutzbeauftragter nicht seine ganze Arbeitszeit für die Funktion aufwenden muss.

Schließlich rege ich an, die **Bußgeldvorschriften** des § 43 BDSG zu harmonisieren. So sollte in § 43 Abs. 2 Nr. 1 BDSG nicht nur die rechtswidrige Erhebung und Verarbeitung, sondern auch die rechtswidrige *Nutzung* personenbezogener Daten als Ordnungswidrigkeit ausgestaltet sein. Derzeit ist es eine Ordnungswidrigkeit, wenn ein Unternehmen einen Betroffenen zu Werbezwecken anschreibt und ihn nicht darauf hinweist, dass er ein Recht hat, der Nutzung zu widersprechen. Macht der Betroffene jedoch von diesem Recht Gebrauch, kann das Unternehmen diesen Widerspruch gegen die Nutzung zu Werbezwecken völlig ignorieren, ohne dass dies Folgen hat. Hier tun sich erhebliche Wertungswidersprüche auf.

Auch die Verwendung allgemein zugänglicher Daten sollte dann als Ordnungswidrigkeit verfolgt werden können, wenn ihr offensichtlich schutzwürdige Interessen Betroffener entgegen stehen. Dafür besteht deshalb eine praktische Notwendigkeit, weil eine verstärkte Tendenz zur Anprangerung Betroffener im Internet unter Verwendung bereits veröffentlichten Materials zu beobachten ist. So bedrohen etwa rechtsradikale Gruppen und Personen zunehmend Personen im Internet, die sich zuvor öffentlich gegen Aktivitäten von Neo-Nazis engagiert haben, wie z. B. im Fall des vereitelten Grundstücksverkaufs in Delmenhorst. Straf- und zivilrechtliche Sanktionen greifen in derartigen Fällen oft nicht.

II. Datenschutzaudit (BT-Drs. 16/1169; BT-Drs. 16/1499)

Ich halte es für einen überfälligen Schritt für eine Modernisierung des Datenschutzes, dass die Bundesregierung den Entwurf eines Ausführungsgesetzes zu § 9a BDSG vorlegt. Diese Vorschrift bekundet unmissverständlich den Willen des Gesetzgebers, für Datenverarbeitungssysteme und –programme, Datenschutzkonzepte verantwortlicher Stellen und technische Einrichtungen ein Datenschutzaudit zu ermöglichen. Das Bundesverfassungsgericht hat in seinem Beschluss vom 23. Oktober 2006 (- 1 BvR 2027/02 -) die **Bedeutung des Wettbewerbs um den besseren Datenschutz** hervorgehoben. Gerade dieser Wettbewerb würde durch ein Datenschutzaudit gefördert.

Die Vorteile des Datenschutzaudits sind in den Anträgen der FDP-Fraktion und der Fraktion BÜNDNIS90/DIE GRÜNEN hinreichend beschrieben. Um wenige Stichworte zu wiederholen: Datenschutzaudits tragen zur Transparenz von Datenverarbeitungsprozessen bei, sie fördern Datenschutz und Datensicherheit und vor allem ermöglichen sie einen präventiven Datenschutz. Dem stehen aus meiner Sicht keine wesentliche Nachteile gegenüber.

Die Erfahrungen des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein zeigen überdies, dass es einen nicht unerheblichen Bedarf in Wirtschaft und Verwaltung für die Durchführung von Datenschutzaudits gibt. Entsprechendes gilt für die Zertifizierungen durch die Datenschutz Nord GmbH, die als Landesgesellschaft der Freien Hansestadt Bremen Online-Dienstleistungen datenschutzrechtlich bewertet.

Im Grundsatz unterstütze ich daher die Vorschläge Nr.1-5 der Fraktion BÜNDNIS90/DIE GRÜNEN in BT-Drs. 16/1499, S.2 sowie den Vorschlag Nr. 1 der FDP-Fraktion in BT-Drs. 16/1169, S.2.

Bei der Schaffung einer Rechtsgrundlage für das Datenschutzaudit sollte dafür Sorge getragen werden, dass die **Einbindung der Datenschutzbehörden in Auditverfahren** nicht zu einer Beeinträchtigung ihrer verfassungsrechtlich und europarechtlich gebotenen Unabhängigkeit führen kann. Dabei sollte der Sachverstand der Datenschutzbehörden für die Schaffung und Fortschreibung von einheitlichen Kriterien durchaus genutzt werden. Ihre unmittelbare Beteiligung an der Überprüfung der datenschutzkonformen Ausgestaltung eines Produkts, eines Verfahrens oder einer Datenschutzorganisation halte ich demgegenüber für bedenklich. Für mich ist es

schwer vorstellbar, dass eine Datenschutzbehörde in der Lage ist, auf die Eingabe eines Betroffenen hin unvoreingenommen die Rechtmäßigkeit einer Datenverarbeitung zu kontrollieren, wenn sie zuvor für das entsprechende Verfahren ein Gütesiegel vergeben hat.

Soweit Vorschlag Nr. 3 des genannten Antrags der Fraktion BÜNDNIS90/DIE GRÜNEN besagt, dass das Datenschutzaudit auf freiwilliger Grundlage zu erfolgen hat, um den Unternehmen selbst die Möglichkeit zu belassen, über die Teilnahme an einer Auditierung zu entscheiden, unterstütze ich diesen Vorschlag.

Ich sehe diese Freiwilligkeit als nicht unangemessen beeinträchtigt an, wenn die öffentliche Hand für die Durchführung von Datenschutzaudits **wirtschaftliche Anreize** setzt. Ein solcher Anreiz kann insbesondere darin bestehen, dass die öffentliche Hand bei der Auftragsvergabe vorrangig Produkte oder Dienstleistungen berücksichtigt, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde. Auf diese Weise werden Unternehmen motiviert, datenschutzfreundliche Produkte herzustellen bzw. Dienstleistungen anzubieten. Für die öffentliche Hand hat dies den Vorteil, dass der datenschutzkonforme Einsatz von Informationstechnologie erleichtert wird.

Ich verkenne dabei nicht, dass eine solche **bevorzugte Auftragsvergabe** zu einer gewissen Beeinflussung des Wettbewerbs führen kann und soll. Insoweit wurde in der Vergangenheit eingewandt, dies führe zu einer Benachteiligung kleinerer oder mittlerer Unternehmen, die sich die Durchführung von kostenträchtigen Audits wirtschaftlich nicht leisten könnten.

Die Erfahrungen der bisherigen Audits stützen diese Befürchtungen jedoch nicht. Im Gegenteil: Ausweislich der vom Unabhängigen Landeszentrum für Datenschutz und der Datenschutz Nord GmbH veröffentlichten Listen zertifizierter Produkte und Online-Dienstleistungen scheinen gerade kleinere und mittlere Unternehmen die Möglichkeit zu nutzen, sich in bestimmten Marktsegmenten als datenschutzfreundliche Hersteller bzw. Dienstleister zu profilieren. Eine unangemessene Benachteiligung kleinerer Unternehmen durch eine datenschutzorientierte Vergabepolitik kann ich daher nicht erkennen. Eine entsprechende gesetzliche Regelung würde auch nicht mit nationalem und europäischem Vergabe- und Wettbewerbsrecht kollidieren.

III. a) Mehr Datenschutz beim so genannten Scoring (BT-Drs. 16/683)

Der genannte Antrag der Fraktion BÜNDNIS90/DIE GRÜNEN enthält nicht nur Forderungen zu einer Neuregelung von Scoringverfahren (vgl. Vorschläge Nr. 2-3), sondern auch zu einer spezifischen **Regelung des Auskunfteiwesens** (vgl. Vorschläge Nr. 1 und Nr. 4). Beide Regelungsvorschläge unterstütze ich inhaltlich.

1. Regelungsbedürftigkeit von Scoringverfahren

Abstrakt gesprochen dienen Scoringverfahren im datenschutzrechtlichen Sinne dazu, Prognosen über ein bestimmtes Verhalten der „gescorten Person“ zu ermitteln. Traditionell werden dabei bestimmte Kriterien mit statistischen Erfahrungen abgeglichen. Beispielsweise kann es sein, dass ein verheirateter Bankkunde statistisch gesehen ein anderes Zahlungsverhalten zeigt als Nichtverheiratete, Verwitwete, Lebenspartner usw. In einem Scoringverfahren werden verschiedene solcher statistischen Zusammenhänge automatisiert ausgewertet. Die Gesamtheit der Kriterien nennt man Scorekarte und das Ergebnis des Verfahrens Scorewert.

Für das Kreditgewerbe hat der Gesetzgeber in § 10 KWG Regeln für das „Rating-Verfahren“ aufgestellt, deren Rechtsgedanken wohl auch auf Scoring-Verfahren anwendbar sind. Zunehmend findet Scoring jedoch auch in anderen Wirtschaftszweigen Anwendung, sodass nicht nur mehr die Kreditwürdigkeit, sondern die **„Vertragswürdigkeit“ des Betroffenen** generell anhand von Scoringverfahren bewertet wird.

Ich bestreite nicht den praktischen Nutzen von Scoringverfahren insbesondere für die Kreditwirtschaft. Die derzeitige Handhabung durch die Privatwirtschaft führt jedoch immer wieder zu massiven Eingriffen in die Rechte der betroffenen Personen.

Das Scoringverfahren hat zur Konsequenz, dass Betroffene in der Tendenz wegen ihrer Zugehörigkeit zu bestimmten Personengruppen **informationell diskriminiert** werden. Häufig geschieht dies, ohne dass dieser Umstand offengelegt wird. Aus meiner aufsichtsbehördlichen Erfahrung weiß ich, dass Kriterien wie beispielsweise das Alter, der Familienstand, die Ethnie und teilweise auch der Wohnort zu typischen Kriterien von Scorekarten zählen. Diese Kriterien mögen eine statistische Relation zur Bonität der Betroffenen haben. Aus Sicht der Betroffenen besteht jedoch **regelmäßig kein unmittelbarer Zusammenhang mit einer Vertragserfüllung**.

Um das eingangs gebildete Beispiel aufzugreifen: Es ist verfassungsrechtlich äußerst problematisch und rechtspolitisch völlig unakzeptabel, wenn ein Mensch wegen einer persönlichen Lebensentscheidung für einen anderen Menschen, sei es durch Eheschließung, Eingehung einer Lebenspartnerschaft oder den Verzicht einer solchen Bindung unter statistisch-wirtschaftlichen Gesichtspunkten pauschal informationell schlechter gestellt wird als andere. Der Einzelne darf nicht wegen rein statistischer Zusammenhänge diskriminiert werden.

Die Regelung des § 10 Abs. 1 Satz 3 KWG schützt das Persönlichkeitsrecht der Betroffenen im Bereich des Kredit-Scoring nur unzureichend, weil der Kreis der auszuschließenden Daten nicht weit genug gefasst ist. Es besteht also ein **dringender Regelungsbedarf**. Diesen Regelungsbedarf hat der Bundesgesetzgeber bereits erkannt und mit **§ 6a BDSG** eine Regelung geschaffen, die auch Scoringverfahren umfassen soll (vgl. dazu BT-Drs.14/5793, Beschlussempfehlung des Innenausschusses zum Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze, S.65, rechte Spalte).

Diese Regelung verfolgt ein legitimes Ziel, hat sich jedoch nach den aufsichtsbehördlichen Erfahrungen als **praxisuntauglich** erwiesen.

Sie soll verhindern, dass Entscheidungen „ausschließlich aufgrund von automatisiert erstellten Persönlichkeitsprofilen getroffen werden, ohne dass eine Person Sachverhalt neu überprüft“ (vgl. BT-Drs. 14/4329, Regierungsentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze, S. 30).

Allerdings ist die Regelung nicht geeignet, ihr Ziel zu erreichen. Seit der Einführung dieser Vorschrift habe ich keinen einzigen Fall erlebt, bei dem § 6a BDSG angewendet wurde. Die Ursachen hierfür sind leicht zu erklären: Häufig orientieren sich Unternehmen bei ihren Entscheidungen an einem bestimmten Scorewert. Es kann dabei sogar durchaus vorkommen, dass es hausinterne Anweisungen gibt, die den Mitarbeitern vorgibt, ab einem bestimmten Scorewert keine positive Vertragsentscheidung zu treffen. Informell habe ich immer wieder solche Rückmeldungen von Mitarbeitern insbesondere von Kreditinstituten erhalten. Eine derartige Anweisung ist jedoch bislang nie nachweisbar gewesen. Nutzer von Scoringverfahren behaupten vielmehr offiziell stets, dass sie einen Scorewert lediglich als eine von mehreren „Entscheidungshilfen“ ansehen.

Insbesondere Vertreter der SCHUFA meinen, dass Scorewerte keine personenbezogenen Daten darstellen. Sie werden dabei von einigen Klientelpublikationen unterstützt. Die dabei vorgebrachten Argumente sind allerdings nicht überzeugend. Sehen wir hierbei einmal von juristischen Spitzfindigkeiten ab: Ziel des Einsatzes von Scorewerten ist es, einem Unternehmen eine Entscheidungshilfe an die Hand zu geben, ob sie mit einer Person einen Vertrag abschließen soll oder nicht. Natürlich muss dann der Scorewert der Bewertung des Betroffenen dienen. Doch selbst wenn man einen Personenbezug verneinen sollte, ändert dies nichts daran, dass Scoringverfahren **ein erhebliches Risiko für das Persönlichkeitsrecht** der Betroffenen bedeuten. Sie sollten deshalb unmissverständlich in den Anwendungsbereich des BDSG einbezogen werden.

Teilweise wird auch behauptet, dass das Scoringverfahren sogar besonders datenschutzfreundlich sei, weil es die Grundsätze der Datenvermeidung und Datensparsamkeit unterstütze. Es würde die Erhebung anderer Daten vermeiden. Auch diese Auffassung kann ich nicht nachvollziehen. Zunächst glaube ich aufgrund meiner aufsichtsbehördlichen Erfahrungen nicht, dass der Umfang der erhobenen Daten durch den Einsatz von Scoringverfahren gegenüber der Vergangenheit verringert worden ist. Im Übrigen realisiert das Scoringverfahren in besonders ausgeprägter Weise die Risiken, die das Bundesverfassungsgericht bereits im Volkszählungsurteil festgestellt hat: Die automatisierte Datenverarbeitung führt dazu, dass Daten „vor allem beim Aufbau integrierter Informationssysteme – mit anderen Datensammlungen zu einem teilweise oder weitgehend **vollständigen Persönlichkeitsbild** zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann“ (vgl. BVerfGE 65, 1, 42).

Diese Gefahr für den Betroffenen wird insbesondere nicht allein dadurch gebannt, dass man ihm den Scorewert mitteilt. Was hilft es denn, wenn der Betroffene erfährt, dass er ein für ihn notwendiges Darlehen nicht erhält, weil sein Scorewert zu schlecht sei? Für ihn ist es notwendig, dass er **Kenntnis über die Informationen** erhält, **die zur Bildung des** für ihn **ungünstigen Scorewertes geführt haben**. Denn nur so kann er die Möglichkeit erhalten, die „Richtigkeit“ der Bewertung in Frage zu stellen und individuelle Besonderheiten seiner Situation aufzudecken.

Selbst wenn – was durchaus zweifelhaft ist – das Verfahren zur Bildung des Scorewerts ganz oder teilweise als Betriebs- und Geschäftsgeheimnis zu qualifizieren wäre, hat der Schutz des

informationellen Selbstbestimmungsrechts der automatisiert bewerteten Betroffenen grundsätzlich Vorrang vor den Geheimhaltungsinteressen der verantwortlichen Stellen.

Aus diesen Gründen unterstütze ich die Vorschläge Nr. 2 und 3 des Antrags der Fraktion BÜNDNIS90/DIE GRÜNEN in BT-Drs. 16/683 vorbehaltlos.

Es ist weiterhin zu empfehlen, dass der Gesetzgeber klarstellt, dass Scoringverfahren, wenn sie im Zusammenhang mit natürlichen Personen eingesetzt werden, als eine risikoträchtige Verwendung personenbezogener Daten anzusehen ist, die nur unter bestimmten, näher zu regelnden Voraussetzungen zulässig ist. Es ist zu empfehlen, dass für Scoringverfahren nur solche Kriterien verwendet werden dürfen, die bei vernünftiger Betrachtungsweise einen **Bezug zur Vertragserfüllung** aufweisen. Ich habe in den zahlreichen Diskussionen zum Scoring-Verfahren die Erfahrung gemacht, dass die Frage, welche Daten in ein Scoring-Verfahren eingebracht werden dürfen, zu einer Glaubensfrage geworden ist. Dies ist für mich ein untrügliches Zeichen dafür, dass eine gesetzgeberische Hilfe hier sinnvoll wäre.

Ergänzend füge ich hinzu, dass auch dafür Sorge getragen werden sollte, dass die verantwortliche Stelle die Scorekarte kennen muss. Insbesondere wenn Unternehmen als Kunden von Auskunfteien sich deren Scorewerte übermitteln lassen, wissen sie üblicherweise nicht, aufgrund welcher Kriterien ein Scorewert günstig oder ungünstig ausfällt. Dies verträgt sich nicht mit dem Grundsatz, dass sie mit der Nutzung des Scorewerts gleichzeitig die Verantwortlichkeit dafür tragen, dass der genutzte Wert datenschutzkonform zustande gekommen ist.

2. Regelung der Datenverarbeitung durch Auskunftssysteme

Ich würde es begrüßen, wenn der Bundesgesetzgeber auch den Umgang mit personenbezogenen Daten und mit Daten im Vorfeld des Personenbezugs durch Auskunftssysteme neu regeln würde. Meiner Einschätzung nach werden § 4, § 4a und § 29 BDSG den Schutzanforderungen des Persönlichkeitsrechts für das Auskunfteigewerbe nicht annähernd gerecht.

Dies gilt zunächst für die **datenschutzrechtlichen Einwilligungen bei Massengeschäften**. Das Bundesdatenschutzgesetz sieht zwar in § 4a vor, dass Einwilligungen „auf der freien

Entscheidung“ des Betroffenen beruhen müssen. Die grundrechtlich begründete Idee der Einwilligung besteht darin, dem Betroffenen die Möglichkeit zu eröffnen, Datenverarbeitungsvorgänge individuell steuern zu können.
Diese Zielsetzung wird in Massengeschäften jedoch durch einen faktischen Zwang zur Erklärungsabgabe und Standardisierung entwertet. Weder beim Abschluss einer Versicherung noch bei der Eröffnung eines Girokontos hat der Kunde letztendlich die Möglichkeit, eventuelle Datenflüsse zu den Hinweissystemen der Versicherung bzw. zur SCHUFA durch Nichteinwilligung zu verhindern und trotzdem den gewünschten Vertrag abschließen zu können. **Die Freiwilligkeit der Einwilligung ist insoweit reine Fiktion** (vgl. auch hierzu den Beschluss des BVerfG vom 23.10.2006 – 1 BvR 2027/02 -). Ich schlage deshalb vor, in diesen beiden Bereichen klare gesetzliche Regelungen zu schaffen, die zu einer gerechten Abwägung der wirtschaftlichen Interessen der Banken, Versicherungen und Auskunfteien mit dem informationellen Selbstbestimmungsrecht der Betroffenen führen.

Durch Auslegung des § 29 BDSG nicht zu klären ist auch die Frage, **welche Grenzen Auskunftssystemen** gesetzt werden sollen. Beispielsweise hat sich die SCHUFA in den letzten Jahren von einer Kreditschutzorganisation zu einer Auskunftei gewandelt, die fast alle wirtschaftlichen Aktivitäten erfasst und die ihren Kunden nicht nur Kreditschutz gewährt, sondern auch vor allen sonstigen möglichen Risiken bewahren will.

Das Gesetz sollte hierzu möglichst klare Grenzen ziehen. Das betrifft zunächst die Frage, welchen Datenumfang eine Auskunft haben soll. Hat es wirklich eine Bank oder einen Vermieter zu interessieren, dass der Betroffene eine Mobilfunkrechnung in Höhe von 200 € nur zum Teil beglichen hat? Soll § 29 BDSG Unternehmen wirklich auch davor schützen, unnötige Versandkosten zu tragen oder die Versicherungen davor, dass der Versicherungsfall tatsächlich eintritt? So wird dies von einigen Auskunfteien gesehen, ohne dass die Aufsichtsbehörden aufgrund der abstrakten Interessenabwägungsklausel des § 29 BDSG dem nachhaltig entgegenwirken können. Stets ist auch sehr umstritten, ab wann Daten „hart“ genug für eine Einmeldung in ein Warnsystem sind. Hier wäre eine gesetzgeberische Hilfe von Vorteil.

Ich befürworte dabei auch den Vorschlag, dass der Gesetzgeber die Frage klärt, inwieweit branchenübergreifende Auskunftssysteme zulässig sind.

Einen weiteren Regelungsbedarf sehe ich hinsichtlich der **Speicherdauer** von sogenannten „**Negativmerkmalen**“. Hierunter versteht man Daten, die unmittelbar ein vertragswidriges Verhalten eines Betroffenen kennzeichnen. Nach § 35 Abs. 2 Satz 2 Nr. 4 BDSG sollen solche Daten selbst dann bis zu vier Jahre gespeichert bleiben, wenn der Betroffene kurz nach der Einmeldung durch seinen Vertragspartner seine Schuld beglichen hat. Das halte ich für unverhältnismäßig. Es kann immer wieder Situationen geben, bei denen eine legitime Auseinandersetzung über eine Forderung geführt wird, selbst wenn sie im Grundsatz nicht bestritten wird. Es benachteiligt den Betroffenen unangemessen, wenn er eine Schuld sogleich begleicht und gleichwohl ein Negativmerkmal bis zu vier Jahren gespeichert werden darf. Deshalb halte ich es für sinnvoll, dass die Frist in dieser Norm verkürzt wird. Personen, die ihre Schuld sofort begleichen, sollten bevorzugt werden.

Ein weiterer wesentlicher Punkt betrifft die Frage der **Entgeltlichkeit von Selbstauskünften**. Verlangt ein Betroffener eine solche Auskunft, so ist diese grundsätzlich schriftlich und unentgeltlich zu erteilen. Unternehmen, die Daten „geschäftsmäßig zum Zwecke der Übermittlung“ speichern, also insbesondere Auskunfteien, Adresshandelsunternehmen, Markt- und Meinungsforschungsunternehmen sowie teilweise Unternehmen der Werbebranche, können sich jedoch auf eine Ausnahmevorschrift berufen. Nach § 34 Abs. 5 S. 2 BDSG kann dann ein Entgelt verlangt werden, „wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann.“ Diese Bedingung ist aber theoretisch stets erfüllt. Die Vorschrift wird jedenfalls insbesondere von einigen Auskunfteien so gehandhabt. So verlangt die SCHUFA für die Erteilung einer SCHUFA-Selbstauskunft stets eine Gebühr von 7,60 Euro zuzüglich Versandkosten selbst dann, wenn das Auskunftsbegehren des Betroffenen eindeutig nicht wirtschaftlich motiviert ist.

Es ist im Hinblick auf das Recht auf informationelle Selbstbestimmung nicht hinnehmbar, dass ein Betroffener nur deshalb Geld für die Erteilung einer Selbstauskunft bezahlen soll, weil ein Unternehmen mit diesen, „seinen“ Daten Handel treibt. Das Bundesverfassungsgericht hat klar festgestellt, dass mit dem Recht auf informationelle Selbstbestimmung eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar wäre, „in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“ (vgl. BVerfGE 65, 1, 43). Es dürfte unstreitig sein, dass für breite Bevölkerungsschichten bereits der von der SCHUFA verlangte Betrag von 7,60 zuzüglich Versandkosten eine erhebliche, oft prohibative Hürde für das Stellen eines Auskunftsbegehrens darstellt. Dabei ist zu berücksichtigen, dass der Betroffene sich

nicht nur der SCHUFA, sondern einer Vielzahl von Auskunfteien gegenübersieht, die nach dem Gesetzeswortlaut sämtlich Gebühren erheben könnten.

Ich schlage daher vor, § 34 Abs. 5 S. 2 bis 4 BDSG ersatzlos zu streichen.

III b) Informationspflicht für Unternehmen bei Datenschutzpannen einführen (BT-Drs. 16/1887)

Ich unterstütze den Regelungsantrag uneingeschränkt und füge lediglich ergänzend hinzu, dass es in anderen Zusammenhängen vergleichbare Unterrichtungspflichten bereits gibt. Insoweit ist die Verpflichtung zur Informationspflicht Ausdruck des Prinzips der Schadensminderungspflicht.

Die Erfahrungen in den USA haben gezeigt, dass die Meldepflicht bei Datenschutzpannen und Sicherheitslecks Unternehmen, bei denen solche Vorfälle auftraten, unter einen heilsamen öffentlichen Druck gesetzt hat. Die Transparenz von Datenschutzmängeln trägt nicht nur dazu bei, dass solche Mängel beschleunigt behoben werden, sondern auch zu verstärkten präventiven Maßnahmen der verantwortlichen Stellen.

Die Gruppe nach Art. 29 der Europäischen Datenschutzrichtlinie hat darüber hinaus in ihrer Stellungnahme 8/2006 zur Überprüfung des Rechtsrahmens für elektronische Kommunikationsnetze und –dienste mit Schwerpunkt auf der Datenschutzrichtlinie für elektronische Kommunikation vom 26. September 2006 eine Erstreckung der Informationspflicht auf „Datenmakler“, Banken und Anbieter von Online-Diensten vorgeschlagen. Diesem Vorschlag sollte auch der Deutsche Bundestag folgen.

Dr. Alexander Dix