

# **„Mehr Schutz für den Bürger? Neue Entwicklungen und Tendenzen im Datenschutz“**

**Vortrag im Rahmen der Fachtagung der dbb akademie am 10.  
Dezember 2008 im Marriott Hotel in Köln von  
Ministerialdirigent Michael Scheuring**

*Es gilt das gesprochene Wort*

Meine sehr verehrten Damen,  
sehr geehrte Herren,  
sehr geehrte Frau Weigend,  
sehr geehrter Herr Russ,

vielen Dank, dass Sie mir als Vertreter der Bundesregierung die Gelegenheit geben, hier zu „Neuen Entwicklungen und Tendenzen im Datenschutz“ referieren zu können. Ich glaube, man kann bereits jetzt sagen, dass Sie bei der Auswahl des Veranstaltungsthemas und des Zeitpunktes dieser Veranstaltung eine glückliche Hand hatten! Sie haben sprichwörtlich „ins Schwarze getroffen“! Denn das Jahr 2008 ist zweifellos ein Jahr des Datenschutzes!

Zunächst feiert im Jahr 2008, genau gesagt in fünf Tagen, das Recht auf informationelle Selbstbestimmung seinen 25. Geburtstag. Am 27. Februar 2008 hat das Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht ein „neues“ Datenschutzrecht, das Recht auf Gewährleistung der Vertraulichkeit und der Integrität informationstechnischer Systeme, abgeleitet. Die Bundesregierung hat Ende Juli den Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes beschlossen und sie befasst sich gerade heute, ich gehe darauf später im einzelnen noch näher ein, erneut mit dem Datenschutz. Dies alleine zeigt schon, dass sich der Datenschutz keineswegs im Jahr 2008 vor dem Untergang befindet, wie es noch gestern in einer großen deutschen Tageszeitung behauptet wurde!

Leider hat das Jahr 2008 auch Anlass zur Sorge um den Datenschutz im nicht-öffentlichen Bereich gegeben: Im Ende Mai – Herr Russ erwähnte dies bereits – wurden Datensicherheitslücken bei einem Groß-Unternehmen der Telekommunikationsbranche bekannt. Bereits 2006 sollen 17 Millionen

Stammdatensätze des Mobilfunkanbieters - darunter auch solche von prominenten und gefährdeten Personen - entwendet worden sein. Ein Missbrauch der Datensätze wurde bisher zum Glück nicht bekannt - aber allein die Tatsache, dass es möglich war, sich dieser Daten zu bemächtigen, hat berechtigterweise zu großer Beunruhigung geführt.

Im Sommer dieses Jahres hat eine breite Diskussion zur Effektivität des Schutzes personenbezogener Daten in Wirtschaft und Unternehmen begonnen. Dem Verbraucherzentrale-Bundesverband waren auf dem Schwarzmarkt 6 Millionen Datensätze – 4 Millionen davon enthielten nicht nur Namen und Adresse, sondern auch Kontodaten - angeboten worden. Mit den Daten sollen Call-Center und Unternehmen im Rahmen unerlaubter Telefonwerbung bundesweit tausende Verbraucher angerufen und Waren oder Dienstleistungen, insbesondere Glücksspielangebote, vermarktet haben. In mehreren Fällen wurden anschließend ohne Einzugsermächtigung und, obwohl die Verbraucher der Leistung ausdrücklich widersprochen hatten, Beträge von 30 bis 70 Euro von ihren Konten abgebucht. Die 6 Millionen Datensätze sollen auf dem Schwarzmarkt ganze 850 Euro gekostet haben. Und schließlich mussten wir am vergangenen Wochenende Meldungen zur Kenntnis nehmen, Händler hätten einer Fachzeitschrift die Daten von 21 Millionen Deutschen für zwölf Millionen Euro angeboten.

Diese Vorfälle haben den Blick der Öffentlichkeit zu Recht auf Fragen zum Datenschutz gelenkt: Die Frage etwa, auf welche Weise die Daten der Bürger in Wirtschaft und Unternehmen gesichert werden und ob gegebenenfalls das Datenschutz- und Datensicherheitsniveau in unserem durch Technologie und Vervielfältigungsmöglichkeiten geprägten Zeitalter angehoben werden sollte; die Frage, wie Bürger mehr Einfluss auf die Weitergabe ihrer persönlichen Daten gewinnen können; oder etwa die Frage, welchen Stellenwert das Recht auf informationelle Selbstbestimmung gegenüber gewerblichen Interessen der Wirtschaft hat.

Meine Damen und Herren,  
die Koordinaten für den Datenschutz haben sich in den letzten Jahrzehnten stark verändert. Während seit den 80er Jahren des vergangenen Jahrhunderts das Datenschutzrecht vor allem als Schutz des Bürgers vor dem informationshungrigen Staat verstanden wurde, werden zunehmend Gefahrenpotenziale deutlich, die sich aus dem raschen Anwachsen von Datenmengen in der Hand privater Unternehmen ergeben. Das Bundesdatenschutzgesetz entstand vor 25 Jahren vor dem

Hintergrund von Großrechner-Technik als Abwehrrecht des Bürgers gegenüber dem Staat.

Die technologischen Rahmenbedingungen sind heute grundlegend anders. Während der räumlich fixierte Großrechner für Datenschutzbeauftragte ein zwar komplexes aber eingrenzbares Kontrollobjekt war, haben wir es heute - im Internetzeitalter - mit vielschichtig vernetzten, grenzüberschreitenden Systemen zu tun. Zudem werden - vor allem im Zuge des zunehmenden elektronischen Handels - immer mehr personenbezogene Daten im privaten Geschäftsverhältnis über das Internet übermittelt. Datenschutz im modernen Sinne befasst sich deshalb nicht allein mit dem Verhältnis Bürger-Staat sondern vor allen mit dem Schutz der Privatsphäre des einzelnen Menschen im Rahmen wirtschaftlicher Betätigungsfelder, dem elektronischen Geschäftsverkehr und einer Vielzahl vertraglicher Gestaltungserfordernisse. Schon im Jahr 2001 betrafen alle wesentlichen Diskussionspunkte im Rahmen der damaligen Novelle des Bundesdatenschutzgesetzes dementsprechend Regelungen mit Relevanz für die gewerbliche Wirtschaft. Dieser Trend setzt sich fort. Im Fokus geplanter bzw. bereits laufender Neuregelungen, die ich Ihnen im Folgenden näher vorstellen möchte, stehen Wirtschaft und Unternehmen. In meinen Ausführungen werde ich mich dabei auf die Änderungen beschränken, die das allgemeine Datenschutzrecht betreffen. Auf Gesetze, die den Sicherheitsbereich oder andere bereichsspezifische Datenschutzregelungen, etwa den Arbeitnehmerdatenschutz, betreffen, kann ich hier schon aus Zeitgründen nicht im einzelnen eingehen !

Meine Damen und Herren,

zur Zeit gibt es zwei, eigentlich drei Gesetzesvorhaben der Bundesregierung im Bereich des allgemeinen Datenschutzrechtes, für die das Bundesinnenministerium federführend zuständig ist, nämlich

- das Gesetz zur Änderung datenschutzrechtlicher Vorschriften (Hintergrund ist der Adresshandel),
- das Gesetz zur Regelung des Datenschutzaudits, beide sind zusammengefasst , sowie
- das Gesetz zur Änderung des Bundesdatenschutzgesetzes, die sog. Scoring-Novelle.

Das erste Gesetz, das Gesetz zur Änderung datenschutzrechtlicher Vorschriften ist Folge des Gespräches, zu dem Bundesinnenminister Dr. Wolfgang Schäuble für den 4. September dieses Jahres im Hinblick auf bekannt gewordene Vorkommnisse

beim geschäftsmäßigen Handel mit personenbezogenen Daten eingeladen hatte. Die für den Datenschutz zuständigen Institutionen aus Bund und Ländern hatten damals mit großer Übereinstimmung Eckpunkte zur Änderung der gesetzlichen Grundlagen zum Datenschutz vereinbart. Zentraler Punkt des Gesetzentwurfs ist die Neugestaltung des so genannten „Listenprivilegs“.

Nach derzeit noch bestehender Rechtslage erlaubt das Listenprivileg – vereinfacht gesagt - die Verwendung bestimmter personenbezogener Daten zu Zwecken der Werbung, Markt- und Meinungsforschung. Es handelt sich um im Gesetz abschließend aufgezählte Daten wie Berufsbezeichnung, Namen, Anschrift und Geburtsjahr - Daten, die man früher leicht aus Telefonbüchern oder Adressverzeichnissen hat entnehmen können - keinesfalls aber um Bankverbindungsdaten, Kreditkartennummern oder gar sonstige sensible Daten. Unzulässig ist die Verwendung dieser privilegierten Daten aber, wenn der Betroffene der Verwendung ausdrücklich widerspricht. Da nun aber eher selten Widersprüche eingelegt werden, verwundert es kaum – und das ist sicher schon allen hier im Saal Anwesenden passiert - warum wir plötzlich einen persönlich adressierten Werbeprospekt von einem Unternehmen bekommen, von dem wir noch nie gehört hatten, und warum dieser Prospekt Waren bewirbt, die tatsächlich unsere Interessen treffen - z.B. Gartengeräte, bestimmte Bücher oder Musik-CDs. Und wahrscheinlich sind auch Sie schon durch Anrufe von Meinungsforschungsunternehmen auf ihrem privaten Telefonanschluss überrascht worden.

Der Gesetzentwurf, den das Bundeskabinett voraussichtlich gerade heute beschließt, - Sie bekommen hier wirklich aktuellste Informationen aus erster Hand - sieht vor, dass die Verwendung personenbezogener Daten zu Zwecken der Werbung, Markt- und Meinungsforschung in Zukunft grundsätzlich nur noch mit ausdrücklicher Einwilligung der Betroffenen (also nicht nur bei unterbliebenem Widerspruch) zulässig sein soll. Dadurch werden die Einflussmöglichkeiten der Bürgerinnen und Bürger auf die Verwendung ihrer personenbezogenen Daten - und damit auch generell ihr Recht auf informationelle Selbstbestimmung - gestärkt. Der Gesetzentwurf hat zum Ziel, mehr Transparenz im Adresshandel zu schaffen. Bürgerinnen und Bürger sollen erkennen können, wer Daten über sie zu Werbezwecken nutzt. Klares Ziel dieser Neuregelung ist, gerade auch die Möglichkeiten zur missbräuchlichen Verwendung von Adressen zu verringern. Denn durch die Dokumentation der Einwilligung und damit des Datenursprungs wird bei gehandelten Daten in der Regel sofort erkennbar, ob es sich Daten handelt, zu deren Nutzung eine Einwilligung der Betroffenen gegeben wurde – oder eben nicht !

Es liegt auf der Hand, dass die Neuregelungen in einem Spannungsverhältnis zu den Interessen der Wirtschaft stehen. Die gezielte Werbeansprache ist für viele Unternehmen ein wichtiges Mittel der Kundengewinnung und Kundenbindung. Deshalb wird die Neugestaltung des Listenprivilegs für die betroffenen Wirtschaftskreise teilweise zu Einschnitten und zu Umstellungsprozessen führen. Um diese Auswirkungen abzumildern, sieht der Gesetzentwurf für bestimmte Bereiche Ausnahmen vom Erfordernis einer ausdrücklichen Einwilligung vor. So soll das Einwilligungserfordernis nicht gelten für die Eigenwerbung mit eigenen Kundendaten, für die steuerbegünstigte Spendenwerbung vor allem gemeinnütziger und kirchlicher Organisationen, für die Geschäftswerbung (z.B. die Werbung eines Großhändlers für Friseurbedarf gegenüber Friseurbetrieben) sowie für die so genannte Beipackwerbung (z.B. wenn ein Lebensversicherungsunternehmen eines Konzerns die Kfz-Sparte bewirbt.). Daneben gibt es ein großes Umschichtungspotenzial zu anderen, weiterhin zulässigen Arten der Werbung, so z.B. zu teildressierter Werbung bzw. Streu- oder Briefkastenwerbung. Der Entwurf räumt den betroffenen Wirtschaftszweigen eine Übergangsfrist von drei Jahren ein.

Neben dem so genannten „Listenprivileg“ sind auch noch andere Regelungen des Bundesdatenschutzgesetzes überarbeitet worden. Der Gesetzentwurf sieht ein so genanntes „Kopplungsverbot“ für marktbeherrschende Unternehmen vor. Dies bedeutet, dass Unternehmen den Abschluss eines Vertrages nicht von einer Einwilligung der Betroffenen in die Nutzung ihrer personenbezogenen Daten zu Werbezwecken abhängig machen dürfen, wenn den Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne Einwilligung nicht oder nicht in zumutbarer Weise möglich ist.

Des Weiteren werden mit dem Entwurf die Bußgeldtatbestände für Verstöße gegen das Datenschutzrecht erweitert, die Höhe der maximal verhängbaren Bußgelder auf 50.000 Euro bei formalen Verstößen und auf 300.000 Euro bei materiellen Datenschutzverstößen angehoben, Möglichkeiten zur Abschöpfung unrechtmäßiger Gewinne aus illegaler Datenverwendung geschaffen – das ist wichtig, wenn im am Wochenende bekannt gewordenen Fall tatsächlich 12 Millionen Euro erzielt worden sein sollten –, eine Informationspflicht gegenüber den Betroffenen bei Datenschutzpannen eingeführt und die Stellung der betrieblichen Datenschutzbeauftragten gestärkt.

Bestandteil dieses Gesetzentwurfes – offiziell heißt er: Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften – Bestandteil ist auch – wie der Titel schon aussagt - ein Vorschlag zur

Schaffung eines freiwilligen und unbürokratischen Datenschutzauditverfahrens. Dieses Auditverfahren soll marktorientierte Anreize zur Verbesserung des Datenschutzes in Unternehmen setzen; es wird schon seit einigen Jahren von verschiedenen Seiten gefordert und ist Bestandteil des in § 9 a Bundesdatenschutzgesetz an den Gesetzgeber gerichteten Auftrages. Im Rahmen des geplanten Verfahrens können Unternehmen ein Datenschutzauditsiegel erwerben, wenn sie sich einem regelmäßigen datenschutzrechtlichen Kontrollverfahren anschließen und bestimmte Branchen-spezifische Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit und zwar über die allgemein gültigen gesetzlichen Datenschutzvorgaben hinausgehend erfüllen. Wir nennen das „Datenschutz-Plus“! Die Richtlinien sollen von einem mit Experten aus Wirtschaft und Verwaltung besetzten Ausschuss erarbeitet werden. Erwerb und werbewirksamer Einsatz des Datenschutzsiegels eröffnen den Unternehmen die Möglichkeit, Vorteile gegenüber Wettbewerbern zu erzielen. Bei den Bürgerinnen und Bürgern wird das Bewusstsein für die Datenschutzrelevanz eines Produktes oder einer Dienstleistung geschaffen und gefördert. Sie können gekennzeichnete Datenschutzkonzepte oder technische Einrichtungen an dem Datenschutzauditsiegel erkennen und bei der Entscheidung zwischen mehreren Anbietern berücksichtigen. Das Datenschutzaudit ist daher ein weiteres sinnvolles Instrument, um Transparenz zu schaffen und das Vertrauen der Bürgerinnen und Bürger in den wirkungsvollen Schutz ihrer personenbezogenen Daten zu stärken. Es ist zugleich insoweit eine Folge aus den Datenschutzproblemen in der Telekommunikationsbranche, als so ein bestmöglicher Datenschutzlevel in der Branche als solcher erreicht werden soll. Dies deshalb, weil wir von dem betroffenen Unternehmen wissen, dass es inzwischen eine ganze Reihe von kurz-, mittel- und langfristig wirkenden Maßnahmen für einen besseren Datenschutz ergriffen hat. Diese Maßnahmen könnten – was im Einzelnen noch geprüft wird – Vorbild-Charakter für die gesamte Telekommunikationsbranche im Sinne von „best-practice“ haben. Künftig könnten das die Audit-Gutachterausschüsse im Rahmen ihrer branchenspezifischen Richtlinien aufgreifen!

Ich komme nun zum dritten Gesetzgebungsverfahren, der sog. Scoring-Novelle, die das Bundeskabinett bereits am 30. Juli dieses Jahres beschlossen hat. Dieser Gesetzentwurf passt die Regelungen des Bundesdatenschutzgesetzes zu so genannten Auskunfteien den veränderten Bedingungen unserer Geschäftswelt an. Auskunfteien sind privatwirtschaftlich geführte Unternehmen, die wirtschaftsrelevante Daten über Privatpersonen und Unternehmen sammeln. Diese Daten werden an Firmen weitergeleitet, die diese im Rahmen von Bonitätsprüfungen nutzen. Die Tätigkeit von Auskunfteien hat durch die Entwicklung neuer Formen von Konsumentenkrediten und des elektronischen Handels stark an Bedeutung

gewonnen. In der Praxis hat sich gezeigt, dass die Betroffenen die von einer Auskunftgeberin ihnen oder ihren potentiellen Vertragspartnern erteilte Auskunft oftmals nicht nachvollziehen können. Ihnen erschließt es sich nicht ohne weiteres, warum sie zum Beispiel im Elektromarkt nicht die Waschmaschine „auf Pump“ oder den Bankkredit nur zu wesentlich schlechteren als den bunt beworbenen Konditionen erhalten haben. Die Novelle sieht deshalb die Erweiterung der Informations- und Auskunftsrechte der Bürgerinnen und Bürger gegenüber Auskunftgebern und deren Geschäftspartnern vor. Bürgerinnen und Bürger sollen auf Wunsch die Informationen zur Verfügung gestellt werden, aus denen sie ersehen können, mit Hilfe welcher Daten eine sie betreffende Entscheidung zustande gekommen ist. Weiterhin soll durch die Schaffung spezieller Erlaubnistatbestände (z.B. für die Durchführung von Scoringverfahren) die Rechtssicherheit für Bürgerinnen und Bürger sowie für Unternehmen erhöht werden. Zugleich wird dadurch die Tätigkeit von Auskunftgebern transparenter gemacht. Den Bürgerinnen und Bürgern wird es erleichtert oder teilweise sogar erst ermöglicht, fehlerhafte Daten zu korrigieren, Missverständnisse aufzuklären und ihre Interessen sachgerecht gegenüber dem Geschäftspartner zu vertreten. Aber auch die Wirtschaft wird von den geplanten Neuregelungen profitieren. Gegenwärtig führen nämlich die mitunter sehr weiten Auslegungs- und Wertungsspielräume im Bundesdatenschutzgesetz zu sehr unterschiedlichen Rechtsauffassungen hinsichtlich der Zulässigkeit von bestimmten Datenverarbeitungen durch Auskunftgeberin und deren Geschäftspartnern. Die Novelle wird zur Zeit im Deutschen Bundestag beraten und wir gehen davon aus, dass sie bald in Kraft treten kann.

Eine sehr spannende Frage wird jetzt sein: was werden die drei Gesetze in der Praxis an Verbesserungen bewirken? Wir erhoffen uns einen starken Präventiveffekt für den Datenschutz. Klar ist aber: die Gesetze können nur so gut sein, wie ihre Einhaltung beachtet wird, insbesondere wie ihre Einhaltung von den Aufsichtsbehörden im nicht-öffentlichen Bereich kontrolliert sowie Verstöße sanktioniert werden !

Zu den neuen Entwicklungen und Tendenzen im Datenschutz gehören natürlich auch solche, die nicht, jedenfalls noch nicht die Änderung der gesetzlichen Grundlagen zum Ziel haben. Hier möchte ich beispielhaft zwei weitere aktuelle datenschutzrelevante Verfahren ansprechen, die so genannte RFID-Technologie und die Kundenkarten.

RFID, die sog. Funk-Chip-Technik, ist ein Verfahren zur kontaktlosen Identifizierung

von Objekten per Funk, bestehend aus zwei Komponenten: einem elektronischen Mikrochip mit Antenne und einem Lesegerät, das die auf dem Chip gespeicherten Daten erfasst und in eine Datenbank überträgt. Die RFID-Technologie bietet großes Potential für Wirtschaft und Verbraucher. Auf Seiten der Unternehmen verspricht sie vor allem Effizienzsteigerungen im Bereich logistischer Prozesse. Die Verbraucher profitieren durch vereinfachte Zahlungsvorgänge und höhere Produktsicherheit. Deutsche Unternehmen sind derzeit als Hersteller und Verwender von RFID-Technologie führend in Europa. In Logistik und Prozesskontrolle hat RFID bereits signifikante Verbreitung gefunden. Im Endkundenbereich beschränkt sich die Anwendung von RFID-Systemen dagegen noch weitestgehend auf Pilotprojekte. Ein flächendeckender Einsatz ist hier aufgrund der hohen Investitionskosten auch mittelfristig nicht zu erwarten. Datenschutzrechtliche Risiken können entstehen, wenn RFID-Technologie zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten eingesetzt wird. Dies ist der Fall, wenn die Chipdaten entweder selbst persönlicher Natur sind oder in der Hintergrunddatenbank des Systems mit personenbezogenen Angaben von Verbrauchern verknüpft werden. Werden personenbezogene Daten verarbeitet, gelten zwar grundsätzlich die umfassenden Datenschutzrechte des Betroffenen nach dem Bundesdatenschutzgesetz. Die praktische Gewährleistung dieser datenschutzrechtlichen Vorgaben wird jedoch durch die besondere Funktionsweise von RFID erschwert. Denn aufgrund der automatischen und sichtkontaktlosen Art der Datenübertragung vom Chip zum Lesegerät ist oftmals nicht ohne weiteres erkennbar, wann, wo und in welchem Umfang ein Personenbezug entsteht und ob etwa personenbezogene Profile über das Kauf- und Konsumverhalten erstellt werden. Daher muss das informationelle Selbstbestimmungsrecht bei RFID-gestützter Datenverarbeitung durch präventive Schutzmaßnahmen abgesichert werden. Diese Schutzmaßnahmen sollten Transparenz, Datensicherheit, den Verzicht auf heimliche Profilbildung und Datensparsamkeit gewährleisten. Vor einem möglichen gesetzgeberischen Tätigwerden ist aus der Sicht der Bundesregierung jedoch zunächst abzuwarten, ob die genannten Anforderungen des Datenschutzes auch durch eine Selbstregulierung des Marktes in Form effektiver Selbstverpflichtungen der betroffenen Wirtschaftskreise zu realisieren sind und diese gegebenenfalls durch Sensibilisierung der Öffentlichkeit und durch die Förderung datenschutzfreundlicher Technologien unterstützt werden können.

Anders als bei den RFID-Anwendungen im Endkundenbereich ist der Einsatz von Kundenkarten bereits weitflächig verbreitet. Kundenkartenprogramme haben in Deutschland seit der Jahrtausendwende stark zugenommen. Bereits heute besitzt jeder Bundesbürger im Schnitt vier Kundenkarten und die Tendenz ist weiter

steigend. Kundenkartenprogramme zählen zu den so genannten „personalisierten Kundenbindungssystemen“, mit denen Unternehmen ihren Kunden Rabatte auf Waren oder Dienstleistungen anbieten. Die Teilnahme an einem solchen Programm setzt voraus, dass die Kunden sich mit Namen, Anschrift, Geburtsdatum und - je nach System - weiteren personenbezogenen Daten beim Systembetreiber anmelden, der die erworbenen Rabatte für sie verwaltet und bei Erreichen einer bestimmten Summe in Einkaufsgutscheine, Sachprämien oder andere Rabattleistungen umwandelt. Sicherlich besitzen auch die meisten von Ihnen Kundenkarten und nehmen die damit verbundenen Preisnachlässe gerne wahr. Manch einer kauft vielleicht sogar bevorzugt bei den Partnerunternehmen eines bestimmten Kundenkartenprogramms ein, um sich regelmäßig Rabatte zu sichern. Den Unternehmen dienen solche Programme jedoch nicht nur zur Kundenbindung sondern vor allem zur Sammlung kundenbezogener Informationen, mithilfe derer sie ihr Angebotssortiment optimieren und die einzelnen Karteninhaber gezielt bewerben können. Insbesondere die großen branchenübergreifenden Systembetreiber vereinen inzwischen Anbieter aus fast allen Lebensbereichen und verfügen damit über umfangreiche personenbezogene Datenbestände, die sie vorrangig zu Zwecken der zielgruppenbezogenen Werbung und Marktforschung nutzen, aus denen sich jedoch auch detaillierte Erkenntnisse über die Konsumgewohnheiten und Lebensumstände der einzelnen Karteninhaber gewinnen lassen. Den Betroffenen ist zumeist nicht hinreichend bewusst, in welchem Ausmaß, zu welchen Zwecken und mit welchen Folgen sie den Systembetreibern Einblick in ihre persönlichen Verhältnisse gewähren. Kundenkartenprogramme sind daher von Daten- und Verbraucherschützern wiederholt kritisiert und in jüngster Zeit auch in den Medien kontrovers diskutiert worden.

Vor diesem Hintergrund untersucht die Bundesregierung derzeit die datenschutzrechtlichen Aspekte von Kundenkartenprogrammen und prüft insbesondere, ob die gegenwärtigen gesetzlichen Instrumentarien ausreichen, um die Verbraucher wirksam vor Datenschutzverstößen - vor allem einer ungewollten Verwendung ihrer personenbezogenen Daten zu Zwecken der Werbung und Marktforschung - zu schützen. Vorrangiges Ziel ist es daher auch hier, Transparenz zu schaffen und den Verbrauchern eine frei bestimmte Entscheidung zu ermöglichen.

Meine Damen und Herren,

einen weiteren wichtigen Bereich habe ich noch nicht angesprochen, den der Datensicherheit! Datenschutz ist nicht nur das „Datenschutzrecht“, Datenschutz ist heutzutage - „im Internet-Zeitalter“ - vor allem auch eine Frage der „Datensicherheit

und Datensicherung“, also eine Frage der technischen Vorkehrungen. Der Begriff der Datensicherheit ist dabei weiter als der des Datenschutzes, denn er umfasst auch Informationen, die nicht unter die gesetzlichen Regelungen zum Datenschutz fallen. Plakativ lässt sich sagen: Datensicherung schützt die Daten, Datenschutz schützt die Person. Die Bürger müssen darauf vertrauen können, dass ihre Daten in ausreichendem Maße vor Verlust, Manipulationen, unberechtigter Einsichtnahme durch unbefugte Dritte geschützt werden. Denn Vertrauen stellt die Basis der Informationsgesellschaft dar. Dies gilt für den öffentlichen Bereich genauso wie für den nicht-öffentlichen Bereich.

Während man früher unter Computersicherheit die Sicherstellung der korrekten Funktionalität von Hardware verstand, gehört es heutzutage zum Sicherheitsgedanken neben der reinen Sicherstellung der Funktionalität auch, die Daten zu sichern. Insbesondere verlangt es die Datensicherheit, technische und organisatorische Maßnahmen zu treffen, um Daten vor dem Zugriff Unbefugter zu schützen. Die Lage der Datensicherheit muss weltweit als bedrohlich bezeichnet werden. Mit Sorge betrachten wir die stetige Zunahme der Anzahl von Schadprogrammen. So stieg die Zahl neuer Schadprogramme im Jahr 2007 um mehr als 300 % auf 130.000. Zum Vergleich: Im Jahr 2006 betrug die Zunahme rund 40.000. Gleichsam im Sekundentakt werden neue Schadprogramme ins Internet eingespeist. Den größten Anteil haben dabei so genannte Trojanische Pferde, die vom Nutzer unbemerkt Daten ausspähen. Dies zeigt, dass die technologischen Errungenschaften nicht nur neue Chancen eröffnen, sondern dass auch neue Risiken entstehen. Erst heute Morgen habe ich gelesen, dass Cyber-Kriminelle sich die gegenwärtige Wirtschaftskrise für ihre Zwecke zu Nutze machen.

Eines der größten Risiken ist der Identitätsdiebstahl, der in der digitalen Welt um einiges bequemer ist, als es bisher in der realen Welt der Fall war. Als Identitätsdiebstahl bezeichnet man die missbräuchliche Nutzung personenbezogener Daten, also der Identität einer natürlichen Person durch Dritte. Meist wollen „Identitätsdiebe“ einen betrügerischen Vermögensvorteil erzielen oder den rechtmäßigen Inhaber der Identitätsdaten in Verruf bringen. Der Identitätsdiebstahl ist ein reales Problem mit realen Opfern in der virtuellen Welt. Bei einem Identitätsdiebstahl werden persönliche Daten wie beispielsweise Geburtsdatum, Sozialversicherungsnummern, Daten von Bankkonten oder Kreditkartenummern unrechtmäßig verwendet. Die missbräuchliche Verwendung von Kreditkartendaten zum betrügerischen Einkauf hat dabei den größten Anteil. Identitätsdiebstahl kann sich zu einem enormen Problem in der ganzen Welt entwickeln. Es ist unerlässlich, hier für einen wirksamen Schutz der Daten Sorge zu tragen.

Daten, die nicht in die Hände Dritter geraten sollen, müssen durch geeignete Maßnahmen gesichert, insbesondere verschlüsselt werden. Dies betrifft nicht nur Daten, die zwischen zwei bestimmten Rechnern ausgetauscht werden sondern auch Daten, die auf Rechnern gespeichert werden. Ganz besonders gilt das beim Übertragen sensibler Daten. Wer seine persönlichen Daten nicht schützt, macht es anderen einfach, diese bei der Übertragung mitzulesen, zu verändern, zu löschen oder sogar zu missbrauchen. Wichtig ist deshalb, dass die technischen Möglichkeiten zum Datenschutz genutzt und stetig weiterentwickelt werden.

In erster Linie ist das natürlich eine Sache der Unternehmen bzw. eines jeden Einzelnen! Aber auch der Staat ist gefordert, die Entwicklung neuer Technologien aufmerksam zu beobachten und seinerseits zur Sicherheit informationstechnischer Systeme beizutragen. Und der Staat sieht sich gefordert.

Eine zentrale Rolle für die Erfüllung dieser Aufgabe spielt das Bundesamt für Sicherheit in der Informationstechnik, kurz das BSI. Es untersucht als Geschäftsbereichsbehörde des Bundesinnenministeriums des Innern Sicherheitsrisiken bei der Anwendung der Informationstechnik in Deutschland und entwickelt Sicherheitsvorkehrungen. Die so genannten „IT-Grundschutz-Kataloge“, die unentgeltlich auf der Homepage des BSI abgerufen werden können, unterstützen IT-Sicherheitsverantwortliche in Behörden und Unternehmen dabei, angemessene Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Das BSI wendet sich mit seinen Angeboten aber auch an die Bürgerinnen und Bürger. Unter dem Einstiegsportal [[www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)] finden sich allgemeine Informationen zur IT-Sicherheit. Dazu zählen - auch für technische Laien verständliche - Ratschläge und Hinweise zum Schutz vor Viren genauso wie Empfehlungen für Eltern, wie sie ihre Kinder vor Gefahren aus dem Internet schützen können.

Auch bei den staatlichen internetbasierten Informations- und Dienstleistungsangeboten für Bürger und Wirtschaft – dem so genannten E-Government - ist der Staat in der Pflicht, für ein größtmögliches Sicherheitsniveau zu sorgen. Bürgerfreundlichkeit und Sicherheit sollen beim E-Government Hand in Hand gehen. Ein umfangreiches und für die Entwicklung des E-Government in Deutschland wegweisendes Projekt ist das Projekt „Bürgerportale“, das die Bundesregierung im Rahmen ihrer High-Tech-Strategie und ihres E-Government-Programms 2.0 im Jahre 2006 angestoßen hat. Zentrales Ziel des Projektes ist es, einen staatlichen Rahmen zu schaffen, der es Bürgerinnen und Bürgern sowie Organisationen erlaubt, im Internet so sicher, verbindlich und vertraulich zu kommunizieren, wie das heute im Bereich der Papierpost der Fall ist. Dazu soll ein Verbund von Internet-

Dienst Providern aufgebaut werden, die im Rahmen eines staatlichen Zertifizierungsverfahrens nachweisen, dass sie die folgenden Leistungen sicher und mit hoher Vertraulichkeit anbieten können. Dabei geht es um folgende Leistungen:

#### 1. Postfach- und Versanddienste

Bürgerportale sollen Bürgerinnen, Bürgern und juristischen Personen ihnen eindeutig zugeordnete elektronische Postfächer zur Verfügung stellen. Mit diesen soll – vergleichbar zur klassischen Post – das sichere und verbindliche Versenden elektronischer Post unter klar definierten Bedingungen ermöglicht werden.

#### 2. Authentisierungsdienst

Bürgerportale sollen natürlichen und juristischen Personen die Möglichkeit bieten, sich im Internet gegenüber dem jeweiligen Kommunikationspartner sicher zu identifizieren, z.B. beim Einkauf in einem E-Shop oder bei der Nutzung einer E-Government-Dienstleistung.

#### 3. Dokumentenablage

Bürgerportale sollen einen Dokumenten- bzw. Datensafe anbieten, der eine sichere und langfristige Speicherung elektronischen Schriftguts ermöglicht.

Ich möchte jetzt noch keine kurze Bemerkung zum elektronischen Personalausweis machen, auch weil Herr Russ dieses Thema im Rahmen seiner Eröffnungsrede angerissen hat: Auch der elektronische Personalausweis, der ab November 2010 den bisherigen Personalausweis ablösen wird, ist ein Beispiel für mehr Datensicherheit. In manchen Kreisen als „Datenschutzrisiko“ geschmäht, ist er in Wahrheit eine Chance für verbesserten Datenschutz. Die Daten, die heute optisch vom Dokument ablesbar sind, sollen zukünftig in einem Ausweis-Chip gespeichert werden. Damit wird es möglich sein, sich im Internet elektronisch auszuweisen – sowohl gegenüber Behörden im E-Government als auch gegenüber privatwirtschaftlichen Dienstleistungsanbietern im Internet, beispielsweise beim Online-Shopping, Online-Banking oder Online-Auktionen. Gleichzeitig kann der Ausweisinhaber sicher sein, dass diejenige Stelle, die seine Daten abfragt, tatsächlich dazu berechtigt ist. Der elektronische Personalausweis bietet damit die Möglichkeit, bestehende Sicherheitslücken im elektronischen Geschäftsverkehr zu schließen und insbesondere dem zunehmenden Identitätsdiebstahl vorzubeugen.

Meine Damen und Herren,

die besten rechtlichen Regelungen und technischen Schutzvorkehrungen nutzen natürlich nichts, wenn die Bürgerinnen und Bürger selbst, insbesondere bei der Nutzung des Internet, nicht auf ihre privaten Daten Acht geben. Es ist allgemein bekannt, dass sich heute Portale wie „MySpace“, „Facebook“, „Xing“ und „StudiVZ“ größter Beliebtheit erfreuen. In diesen virtuellen Beziehungsnetzen stellen gerade

junge Menschen häufig höchstpersönliche Informationen ein. Dabei wird allzu oft übersehen, dass das Internet nichts vergisst und leichtsinnige Einträge noch Jahre später - etwa bei der Suche nach einem Arbeitsplatz - negative Folgen haben können. Aber bei der Nutzung anderer Internetdienste wie E-Mail und Online-Verkaufsangeboten sind die Bürgerinnen und Bürger sich der Schutzwürdigkeit ihrer persönlichen Daten nicht immer bewusst. Hier gilt es, Aufklärungsarbeit zu leisten, das Bewusstsein der Menschen für die Sensibilität ihrer Daten zu stärken und z.B. Internetnutzer aufzurufen, ihre Kommunikationsgewohnheiten zu überprüfen.

Vielleicht noch ein paar Worte zum Internationalen Datenschutz: die internationale Zusammenarbeit im Bereich des Datenschutzes heute wichtiger denn je! Denn elektronische Datenströme machen bekanntermaßen nicht an Staatsgrenzen halt. Zunehmender Handel, staatliche Kooperationsvorhaben und größere persönliche Mobilität tragen ebenfalls dazu bei, dass immer mehr personenbezogene Daten international übermittelt werden. Ein wirksamer Schutz der Privatsphäre kann in einer digitalen Welt ohne Grenzen nicht durch einzelstaatliche Maßnahmen allein gewährleistet werden. Erforderlich ist eine intensive grenzüberschreitende Zusammenarbeit aller verantwortlichen Stellen im nationalen und internationalen Bereich, um zu verhindern, dass der unbegrenzte Informationsaustausch zu einem unbeschränkten wird. Die Internationale Datenschutzkonferenz, die im Oktober ihr 30-jähriges Bestehen feiern konnte, hat hierzu in der Vergangenheit wichtige Beiträge geleistet. Auch die Europäische Datenschutzrichtlinie von 1995 hat Maßstäbe gesetzt, die inzwischen in vielen Teilen der Welt akzeptiert werden. Wichtig ist es, dass wir diese Bemühungen fortführen.

Meine sehr verehrten Damen und Herren,  
ich komme zum Schluß! Ich denke, die von mir aufgezeigten aktuellen Entwicklungen und Tendenzen im Datenschutz haben gezeigt, dass in der heutigen Zeit ein wirksamer Datenschutz nur durch ein großes Bündel unterschiedlicher nicht-staatlicher und staatlicher Maßnahmen gewährleistet werden kann. Zwar spielen gesetzliche Regelwerke und staatliche Aufsicht auch weiterhin eine große Rolle für ein hohes Datenschutzniveau in Deutschland. Entscheidend aber bleibt, dass die Verantwortlichen in Behörden und Unternehmen „Datenschutz“ als besonders wichtige Daueraufgabe verstehen. Die Gewährleistung von Datenschutz und Datensicherheit ist insofern eine gesamtgesellschaftliche Aufgabe, zu der wir alle, Sie als Träger der „Datenschutz-Verantwortung“ in Ihrem Bereich, aber natürlich auch jede Einzelne und jeder Einzelne maßgeblich beitragen können. Nur so wird es

tatsächlich mehr Schutz, mehr Datenschutz für die Bürger und mehr Datenschutz für alle Bürger geben!

Vielen Dank für Ihre Aufmerksamkeit !