

1. Vorwort

Es ist jedes Jahr wieder spannend, wie der Jahresbericht wohl tatsächlich ausfallen wird. Allein die Auflistung der in der Betreff-Zeile genannten Themen, die jedes Jahr mit der Post in die Dienststelle schwemmen, würden aneinandergereiht wohl leicht fünfzehn bis zwanzig engbedruckte Seiten füllen. Hinzu käme im Jahr ein fast gleichgroßer Anteil an neuen Themen, die per E-Mail bei der Dienststelle eingehen, gefolgt von dem nicht unwesentlichen Anteil an telefonischen Anfragen und Eingaben. Am Jahresende wird dann von den Referaten die Auswahl getroffen: Welche Themen stellen einen Schwerpunkt der Arbeit dar, von welchen Themen können auch andere Stellen lernen, welche Entwicklungen werden uns auch die kommenden Jahre noch beschäftigen und bei welchen Themen sollte eine öffentliche Diskussion stattfinden. Diese Themenauswahl schreiben wir dann in eine Liste, die i. d. R. immer noch viel zu lang ist. Jetzt beginnt die interne vergleichende Diskussion über die Relevanz von einzelnen Themen. Ist die Auswahl getroffen, werden die Beiträge erstellt. Dabei müssen die von den Referaten gefertigten Artikel regelmäßig in einem zweiten Arbeitsschritt gekürzt werden, um möglichst das selbst gesteckte Ziel zu erreichen, den Bericht in seinem Umfang unter einhundert Seiten zu halten. Am Ende dieses Prozesses steht dann das, was der Leser jetzt in den Händen hält oder in einem Download-Verzeichnis auf seinem PC hat. Im Inhaltsverzeichnis zum Jahresbericht findet er die so ausgewählten Bereiche im Überblick wieder. In diesem Jahr sind es mehr als 150 verschiedene Themen, die der Bericht enthält. Ein Beweis für die außergewöhnliche Leistungsfähigkeit und die hohe Motivation der in der Dienststelle Beschäftigten.

Auch wenn der Schwerpunkt des Augenmerks im Land Bremen liegt, ist doch immer auch der Blick nach Europa und den anderen führenden Industrienationen notwendig, insbesondere, um die technologischen und gesellschaftlichen Entwicklungen zu erkennen und datenschutzrechtlich und -technisch einordnen zu können. Die Vorbemerkungen zu meinem Bericht sind daher in besonderem Maße geeignet, schlaglichtartig auf besondere Entwicklungen einzugehen und die mit den Entwicklungen einhergehenden Gefahren für das informationelle Selbstbestimmungsrecht darzustellen, was in den folgenden 25 Punkten zum Teil deutlich werden dürfte. Die Zusammenarbeit unter den Datenschutzbeauftragten und den Datenschutzaufsichtsbehörden auf nationaler wie auch auf europäischer und internationaler Ebene ist dabei mittlerweile so gut ausgebaut, dass man von einem funktionierenden Frühwarnsystem sprechen kann.

1.1 25 Jahre Datenschutz im Land Bremen

In 2003 gab es "25 Jahre Datenschutz in der Freien Hansestadt Bremen" zu feiern. Ich habe dieses Jubiläum zum Anlass genommen, eine Festausgabe auf einer multimedialen CD herauszugeben. Die CD spiegelt die wechselvollen Themen und Entwicklungen der Vergangenheit wider, enthält aktuelle Sammlungen und Übersichten und wirft interessante Blicke in die Zukunft. Auszugsweise zu nennen sind: Die Bürger werden über ihre aktuellen Datenschutzrechte aufgeklärt, ein chronologischer Überblick und eine Zeitleiste zur Datenschutzgesetzgebung im Land, verbunden mit den Plenarprotokollen aus der Bremischen Bürgerschaft zur Datenschutzgesetzgebung, wie auch eine umfassende Sammlung des Landesrechts zum Datenschutz sind auf der CD zu finden. Die Landesbeauftragten für den Datenschutz in Bremen, die Senatskommissare sowie die acht Vorsitzenden des Datenschutzausschusses in den einzelnen Legislaturperioden kommen zu Wort. Alle 25 Jahresberichte liegen auf der CD komplett in elektronischer Form vor, was mich darüber hinaus erstmalig in den Stand versetzt, Bestellungen alter Jahresberichte nachzukommen. Wer einmal versucht hat, ein Werk mit einer Vielzahl von Autoren herauszubringen, wird erahnen können, wie viel Mühe es bereitet hat, alle Beiträge zusammenzustellen. Gleichwohl hat sich der Aufwand gelohnt, die Beschäftigung mit der Vergangenheit hat auch Freude bereitet und das vielseitige Lob für die CD waren Dank genug. Gleichzeitig wurde mit ihr ein Grundstock gelegt, der sich jederzeit aktualisieren lässt, denn die Navigationsinstrumente auf der CD lassen sich auch bei Erweiterungen nutzen. Die erste Auflage von 1.000 CDs war schnell vergriffen, lediglich einige wenige Stücke wurden für besondere Anlässe zurückgehalten.

1.2 Zwanzig Jahre Volkszählungsurteil

Ein weiteres Jubiläum war 2003 zu feiern: Vor zwanzig Jahren, am 15. Dezember 1983, hatte das Bundesverfassungsgericht mit dem Volkszählungsurteil das Grundrecht auf informationelle Selbstbestimmung anerkannt und damit eine grundlegende Änderung des gesamten Datenschutzes in Gesetzgebung, Rechtsprechung und Praxis bewirkt. Das Bundesverfassungsgericht hat in den Leitsätzen zum Volkszählungsurteil festgehalten: "Das Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig."

Das in dem Urteil zum Ausdruck kommende Grundrechtsverständnis, das die Selbstbestimmung des Bürgers als Regelfall und ihre Einschränkung als Ausnahme feststellt, ist bis heute keineswegs durchgängig akzeptiert. Statt Verfahren ohne personenbezogene Daten einzusetzen, zeichnet sich ab, dass verstärkt Identifikationsnummern und solche Systeme eingeführt werden, die das Verhalten des Einzelnen kontrollierbar machen. Beispiele dafür sind die elektronische Kontrolle mit den neuen Ortungstechniken, Videoüberwachung und die geplante Vorratsspeicherung von Kommunikationsdaten durch Telefonanbieter sowie der Einsatz von RFID-Mikrochips. Diese und andere Entwicklungen gefährden das Recht auf informationelle Selbstbestimmung in immer stärkerem Maße. Das Bundesverfassungsgericht hat im Volkszählungsurteil ausdrücklich vor den Gefahren der unbegrenzten Erhebung und Verwendung persönlicher Daten durch den flächendeckenden Einsatz von Informations- und Kommunikationstechnik gewarnt.

Insbesondere wird die weitere Aussage des Bundesverfassungsgerichts häufig übergangen, dass die Einschränkungen zu Lasten des Bürgers nicht weitergehen dürfen, „als es zum Schutze öffentlicher Interessen unerlässlich ist“. Gerade in jüngster Zeit sind wieder Tendenzen festzustellen, dieses Verhältnis umzudrehen, was zum Beispiel in dem Schlagwort zum Ausdruck kommt, der rechtstreue Bürger brauche sich vor staatlicher Datenverarbeitung nicht zu fürchten. Dabei wird vergessen, dass nicht der Bürger sich dafür rechtfertigen muss, dass er einen Eingriff in sein informationelles Selbstbestimmungsrecht nicht hinnehmen will, vielmehr ist der Staat dafür beweispflichtig, dass die geplante Datenverarbeitung mit personenbezogenen Daten zwingend erforderlich ist.

Auf der anderen Seite hat das Urteil des Bundesverfassungsgerichts eine Reihe positiver Datenschutzregelungen in Gesetzen und Verordnungen des Bundes und des Landes hervorgerufen. Die Änderung der bremischen Landesverfassung in Art. 12 wäre ohne das Volkszählungsurteil nicht zu denken. Exemplarisch sei hier weiter an die Datenschutzordnung der Bremischen Bürgerschaft, das Bremische Krankenhausdatenschutzgesetz oder das Bremische Schuldatenschutzgesetz, auch wenn dieses demnächst novelliert werden soll, erinnert.

1.3 Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz

Immer mehr Beschäftigte in Wirtschaft und Verwaltung erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner sowie bei der technischen Abwicklung sind bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Beschäftigten neben der beruflichen auch eine private Nutzung des Internets am Arbeitsplatz gestattet wird.

In dem Maße aber, in dem der Einsatz moderner Telekommunikationstechnik im Arbeitsumfeld zunimmt, wachsen auch die Gefahren für die informationelle Selbstbestimmung der Beschäftigten. Das Surfen im Internet oder das Versenden von E-Mails hinterlässt Datenspuren auf dem Arbeitsplatzrechner, auf dem Internetserver und in den Netzen. In wachsendem Maße sind die Beschäftigten auf die Nutzung von E-Mail und Internet bei ihrer Arbeit angewiesen. Es wird für Vorgesetzte und Arbeitgeber daher leichter, durch die Auswertung und die Kenntnisnahme von protokollierten Verbindungs-, Nutzungs- oder sogar Inhaltsdaten, umfassend die Leistung und das Verhalten ihrer Mitarbeiter zu kontrollieren. Datenschutz- und Arbeitsrecht müssen daher für einen Ausgleich zwischen den Direktions- und Kontrollrechten der Arbeitgeber auf der einen Seite und dem Schutz der informationellen Selbstbestimmung der Beschäftigten auf der anderen Seite sorgen.

Bei der beruflichen Nutzung ist eine Kontrolle bei konkretem Missbrauchsverdacht im Einzelfall zulässig, auch hat der Arbeitgeber grundsätzlich das Recht, stichprobenartig zu prüfen, ob das Surfen oder das Versenden von E-Mails dienstlicher Natur ist. Eine umfassende automatisierte Vollprotokollierung aller Aktivitäten hingegen ist untersagt. Wird eine private Nutzung erlaubt, so ist es grundsätzlich möglich, diese Erlaubnis an einschränkende Voraussetzungen zu knüpfen. Beschäftigte, die jedoch solche Voraussetzungen nicht erfüllen wollen, müssen ihre Einwilligung ohne berufliche Nachteile verweigern können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits in einer Entschließung der 63. Konferenz (vgl. 25. JB, Ziff. 15.3) wesentliche dabei zu beachtende Grundsätze formuliert.

Im vergangenen Jahr bin ich häufig mit Fragen aus diesem Bereich konfrontiert worden (vgl. z. B. Ziff. 16.3.1 dieses Berichts), wobei mich sowohl Beschäftigte wie auch betriebliche Datenschutzbeauftragte um Rat gebeten haben. In einem Fall hatte der Arbeitgeber sämtliche private E-Mails einer Beschäftigten während ihres Urlaubs gelesen und darauf gestützt, eine Kündigung ausgesprochen. Auch das Tul-Referat des Senators für Finanzen hat mich bei der Entwicklung einer Internetnutzungsrichtlinie intensiv beteiligt; es konnte auch die Abstimmung mit dem Gesamtpersonalrat noch im letzten Jahr erreicht werden, so dass einer Umsetzung in 2004 nichts mehr im Wege steht (vgl. Ziff. 5.4 dieses Berichts). Zu begrüßen ist insbesondere, dass durch die Verwendung des so genannten P-Switch eine klare Trennung zwischen dienstlicher und privater Nutzung möglich wird, so dass auch bei einer Kontrolle durch den Arbeitgeber keine Vermischung dieser beiden Sphären auftreten kann.

1.4 Behördliche Datenschutzbeauftragte

Durch die Novelle des Bremischen Datenschutzgesetzes (BremDSG) sind dem behördlichen Datenschutzbeauftragten wichtige Aufgaben zugewachsen. Der mit der Modernisierung der Verwaltung einhergehende verstärkte Einsatz automatisierter Verfahren und fachspezifischer eGovernment-Anwendungen stellt erhöhte Anforderungen an die Kompetenz und Sachkunde der behördlichen Datenschutzbeauftragten, sowohl im Bereich des Datenschutzrechts wie auch im Bereich des technischen Datenschutzes. Darüber hinaus haben die behördlichen Datenschutzbeauftragten nunmehr bereits im Vorfeld neue Aufgaben, wenn wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien besondere Risiken damit verbunden sind. Mit der Novellierung hat der Landesgesetzgeber sich dazu entschlossen, den öffentlichen Stellen beim Einsatz automatisierter Verfahren für die Verarbeitung personenbezogener Daten verbindlich die Bestellung eines Beauftragten für den Datenschutz vorzuschreiben, § 7a BremDSG. Damit folgt er dem auch im Bundesdatenschutzgesetz für öffentliche und private Stellen verankerten Gedanken, zur Gewährleistung des Datenschutzes die Selbstkontrolle in den öffentlichen Stellen der Fremdkontrolle durch den Landesbeauftragten vorzuschalten.

Die Bestellung eines behördlichen Datenschutzbeauftragten ist mir anzuzeigen. Im Laufe des Jahres sind eine ganze Reihe von Meldungen bei mir eingegangen, allerdings muss ich ein Jahr nach Inkraft-Treten dieser Bestimmung noch davon ausgehen, dass viele öffentliche Stellen ihrer gesetzlichen Verpflichtung zur Bestellung eines behördlichen Datenschutzbeauftragten immer noch nicht nachgekommen sind. Ich habe mich daher entschlossen, in 2004 noch einmal alle Stellen auf die gesetzliche Regelung hinzuweisen. Auf meiner Internetseite habe ich ausführlich die Aufgaben der behördlichen Datenschutzbeauftragten und die Verfahren zur Bestellung beschrieben. Im Intranet der öffentlichen Verwaltung in Bremen habe ich in den öffentlichen Ordnern auf dem Formularserver Bestellungsvordrucke zum Abruf bereitgestellt. Darüber hinaus biete ich für behördliche Datenschutzbeauftragte Schulungen an.

1.5 Tod in der Neustadt

Im Sommer des Berichtsjahres wurde in der Stadtgemeinde Bremen eine psychisch kranke Frau beschuldigt, eine Nachbarin getötet zu haben. Bei mir schrillten deshalb die Alarmglocken, weil in einem Pressebericht am 18. Juli 2003 behauptet wurde, der Datenschutz sei an einer nicht ausreichenden Information der beteiligten Stellen schuld. Ich habe daher umgehend den Vorgang bei den beteiligten Stellen prüfen lassen, denn hätte eine Vorschrift bestanden, die eine hinreichende Information der beteiligten Stellen verhindert hätte, so hätte diese umgehend geändert werden müssen. Die datenschutzrechtlichen Nachforschungen haben aber ergeben, dass ein umfassender Datenaustausch zwischen der Psychiatrie, dem Stadtamt, der Polizei und dem Vormundschaftsgericht in solchen Fällen möglich ist. Bereits wenige Tage später titelte die Presse dann auch mit: „Die 41-jährige Täterin ... war der Polizei einschlägig bekannt - doch angeblich ist diese Information nicht weitergereicht worden.“

Der Datenschutz Mitschuld an einem Tötungsdelikt? Indirekt verbunden sah ich damit wieder einmal den platten Vorwurf, der Datenschutz sei Täterschutz. Ich habe nicht mehr aufklären können, wie diese Pressemeldung zu Stande gekommen ist, aber manche interessierte Kreise können den Versuch nicht lassen, den Datenschutz an den Pranger zu stellen. Unabhängig von meinem Prüfergebnis in der Sache kommt auch die vom Senat eingesetzte interne Untersuchungsgruppe in ihrem Prüfbericht zu dem Ergebnis, dass nicht der Datenschutz eine Mitschuld trägt, sondern ausschlaggebend waren andere Umstände, die dazu führten, dass die Tat nicht verhindert wurde. Damit wird der Datenschutz auch von neutraler Seite von dem Vorwurf, er trage eine Mitschuld an dem Tod der Frau, entlastet (vgl. Ziff. 8.2.5 dieses Berichts).

1.6 Zum Ausgang der Rasterfahndung

Zu den datenschutzrechtlich umstrittensten Themen der letzten beiden Jahre gehört die Rasterfahndung. Viele Fragen sind dabei offen geblieben, eine Evaluation dieses Instruments erscheint nach wie vor erforderlich. Ich habe die damit im Zusammenhang stehende Datenverarbeitung in Bremen bis zum Abschluss der Rasterfahndung verfolgt und in einer Stichprobe die rund 20 Personendatensätze einer letzten Prüfung unterzogen, die dem Staatsschutz bei der Polizei Bremen zur weiteren Abklärung übergeben wurden (vgl. Ziff. 6.1.3 dieses Berichts). Hervorheben möchte ich an dieser Stelle, dass das Bundeskriminalamt (BKA) bestätigt hat, dass aus Bremen stammende Datensätze, die beim BKA in die bundesweite Rasterfahndung mit einbezogen wurden, nicht an Nachrichtendienste und auch nicht an ausländische Polizeidienststellen weitergegeben wurden. Die an das BKA übermittelten Daten der Rasterfahndung durch die Polizei Bremen wurden im April 2003 dort gelöscht. In Bremen wurden die Daten der Rasterfahndung im September 2003 gelöscht und die zugehörige Arbeitsdatei aufgelöst.

1.7 Datenabgleich

Öffentliche Kritik gab es in 2003 sowohl in Bremen wie in Bremerhaven an der Durchführung eines Datenabgleichs von Sozialhilfeempfängern mit der Kfz-Zulassungsstelle. Dieser Abgleich ist aber im Bundessozialhilfegesetz geregelt (§ 117 BSHG). Ich hatte daher nur die rechtmäßige Verarbeitung der Daten zu kontrollieren.

Auch die Bremer Entsorgungsbetriebe (BEB) wollten im vergangenen Jahr einen Datenabgleich vorbereiten, um zu überprüfen, ob die Bremer Haushalte entsprechend der Anzahl der Bewohner eines Grundstücks auch genügend Müllgebühren bezahlen. Hierzu war ein Onlinezugriff auf das Melderegister geplant. Die Vertragspartner der BEB sind die Hauseigentümer, nicht etwa die Mieter. Es hätte daher für die Fragestellung der BEB ausgereicht, wenn die Anzahl der Haushalte und Bewohner bekannt gegeben worden wäre. Ein Zugriff auf die Namen der Bewohner war dafür nicht erforderlich. Am Ende hat das Bauressort die Planungen zum Datenabgleich abgebrochen, laut Presseberichten, "weil sich der Aufwand nicht lohne und es Probleme mit dem Datenschutz gebe". Auch wenn das Ziel des Datenabgleichs ohne die Verarbeitung personenbezogener Daten hätte erreicht werden können, freut es mich, wenn so viel Rücksicht auf den Datenschutz genommen wird.

1.8 Vom Big Brother am Straßenrand und anderen Überwachungstechniken

Nach dem Motto "steter Tropfen höhlt den Stein" werden immer neue Ansprüche zur Verwendung von Video- und anderen Überwachungstechniken formuliert. Hierzu zähle ich die Vorschläge aus einem benachbarten Land, nachdem dort ein Schüler gequält worden ist, die Schulhöfe videoüberwachen zu lassen, ebenso wie den Vorschlag, an belebten Straßen Videokameras zu installieren, die die Nummernschilder vorbeifahrender Fahrzeuge registrieren sollen, um diese Daten dann mit in polizeilichen Systemen gespeicherten Daten abzugleichen. Schließlich wurden nicht umsonst die neuen Nummernschilder mit maschinenlesbaren Kennzeichen eingeführt. Die Datenschutzbeauftragten müssen sich daher auch mit diesen Vorhaben datenschutzrechtlich beschäftigen. Mit der polizeilichen Videoüberwachung auf dem Bahnhofsvorplatz in Bremen, wie auch in Firmen und Betrieben, habe ich mich im letzten Jahresbericht hinreichend auseinandergesetzt. Im Berichtsjahr konnte ich vermehrt Eingaben zum Einsatz von Videokameras vermerken, die zum Objektschutz montiert waren, aber zugleich den öffentlichen Raum überwachten (vgl. Ziff. 16.4.1 dieses Berichts). Seit Einführung der Überwachungskameras in öffentlichen Verkehrsmitteln in Bremen reißt der Strom der Beschwerden nicht ab, dabei ist bisher nur ein Teil der Fahrzeuge mit Videotechnik ausgestattet (vgl. Ziff. 16.4.2 dieses Berichts). Auch die sog. Webcams, die Bildsequenzen ins Internet stellen, können zur Beobachtung menschlichen Verhaltens genutzt werden. Wegen grundsätzlicher Fragestellungen zum Einsatz solcher Kameras habe ich den Düsseldorfer Kreis mit dieser Thematik befasst (vgl. Ziff. 16.4.3 dieses Berichts). Durch die geplante Einführung des Maut-Systems hätten sich weitere Überwachungsmöglichkeiten geboten, zumal bei der Durchfahrt an den Maut-Kontrollbrücken alle Fahrzeuge, LKW wie PKW, erfasst werden sollten. Bei der automatischen Einbuchung durch die sogenannte On-Board-Unit (OBU) sollte jede Autobahnbenutzung eines LKW per Satellitennavigation mit Positions- und Fahrzeugdaten registriert und über GSM-Mobilfunk an die Betreibergesellschaft übermittelt werden. Die Begehrlichkeiten anderer Stellen an diesen Daten sind abzusehen, ebenso wie beim Handy, das zunächst ausschließlich zum Telefonieren konzipiert, mehr und mehr zum Überwachungsinstrument umfunktioniert wird (vgl. Ziff. 1.21 dieses Berichts).

1.9 eGovernment

Durch die Einführung von eGovernment begibt sich die Verwaltung auf lange Sicht in zunehmendem Maße in die Abhängigkeit von elektronischen Datenverarbeitungssystemen. Damit entstehen neue Gefahren für das informationelle Selbstbestimmungsrecht. Netzsicherheit, Nutzungsprofile, die Verantwortlichkeit für elektronisch getroffene Entscheidungen oder Fragen zur Sicherstellung der eindeutigen Identität der Nutzer sind in diesem Zusammenhang zu nennen. Die Datenschutzbeauftragten des Bundes und der Länder haben Empfehlungen zum Datenschutz einer serviceorientierten Verwaltung erarbeitet. Sie wurden dabei durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Professoren Lenk und Rossnagel unterstützt. Auch ich habe an dieser Arbeitsgruppe mitgewirkt, die Arbeiten konnten im Frühjahr 2003 abgeschlossen werden. Produkt ist eine auch bei mir erhältliche Broschüre, in der neben der Darstellung rechtlicher Rahmenbedingungen viele praktische Handlungsempfehlungen enthalten sind. Umfangreich und interessant ist auch die Sammlung ausgewählter eGovernment-Anwendungen (vgl. Ziff. 3.2 dieses Berichts). Adressaten dieser Veröffentlichung sind in erster Linie Verwaltungschefs, Organisatoren, Verfahrensentwickler, IT-Verantwortliche, behördliche Datenschutzbeauftragte und Personalräte, eben alle, die Anwendungen von eGovernment vorzubereiten oder umzusetzen haben. Daneben kommen aber auch die privaten Anwender und Bürger, die eGovernment nutzen wollen, nicht zu kurz. Für sie finden sich Hinweise und Empfehlungen zum Selbstschutz, denn ein wesentlicher Teil der Verantwortung für Sicherheit und Vertraulichkeit ihrer Daten verbleibt bei ihnen selbst.

1.10 Lauschangriff

Zur Reihe der grausamen Angriffe wider den Datenschutz zählt auch der Vorschlag, für den sich die Justizminister und -ministerinnen der Bundesländer im Sommer 2003 mehrheitlich ausgesprochen haben sollen. Ihr Vorschlag war laut Presseberichten, eine gesetzliche Grundlage dafür zu schaffen, dass Hausverwalter, Schlüsseldienste, Angestellte der Stadtwerke oder Schornsteinfeger künftig aushelfen sollen, wenn Kriminalpolizei oder Verfassungsschutz "Wanzen" in Wohnungen oder Geschäftsräumen platzieren wollen. Der Nachbar als Schnüffler und verlängerter Arm der Staatsmacht?

In 2003 habe ich zusammen mit anderen Datenschutzbeauftragten der Länder eine Stellungnahme gegenüber dem Bundesverfassungsgericht (BVerfG) in der Verfassungsbeschwerde zu Art. 13 Abs. 3 bis 6 GG (BvR 2378/98 u. BvR 1084/99) im Verfahren gegen den sog. "Großen Lauschangriff" abgegeben und darin meine verfassungsrechtlichen Bedenken zum Ausdruck gebracht. Die mit Spannung erwartete Verkündung einer Entscheidung in dieser Sache ist vom Gericht für das Frühjahr 2004 terminiert. Ich hoffe, dass das Gericht die Gelegenheit nutzt, auch zu der genannten, von den Justizministern und -ministerinnen mehrheitlich getragenen Initiative, deutliche Worte zu finden.

Für das Land nachzutragen bleibt: Ergebnis der Parlamentarischen Kontrollkommission ist, dass im Land Bremen im Jahr 2002 keine Maßnahme nach § 100c Abs. 1 Nr. 3 der Strafprozessordnung durchgeführt wurde, die von einem bremischen Gericht angeordnet wurde (Bremische Bürgerschaft Drs. 16/20).

1.11 Beratung neuer Datenschutzvorschriften im Land

Im April 2003 traten Änderungen des Bremischen Verwaltungsverfahrensgesetzes in Kraft (Brem.GBl. 2003, S. 147 ff.). Mit den Änderungen soll die elektronische Kommunikation im Verwaltungsverfahren ermöglicht werden. Ebenfalls im Frühjahr beriet ich einen Arbeitsentwurf des Senators für Inneres, Kultur und Sport zur Änderung des bremischen Verfassungsschutzgesetzes. Die Formulierungen waren schon sehr weit gediehen, einige wenige Punkte waren aus datenschutzrechtlicher Sicht noch kontrovers und hätten der politischen Meinungsbildung zugeführt werden können. Wohl auch wegen der bevorstehenden Bürgerschaftswahl wurde das Gesetz nicht mehr in die Bremische Bürgerschaft eingebracht.

Die Beratungen zur Änderung des Bremischen Krankenhausdatenschutzgesetzes (Brem.GBl. 2003, S. 47) hingegen wurden noch zum Ende der Legislaturperiode abgeschlossen. Wesentliches Anliegen dieser Gesetzesnovelle war, die Datenschutzbestimmungen den veränderten technischen Bedingungen und praktischen Behandlungsbedürfnissen in den Krankenhäusern anzupassen, ohne das im Bremischen Krankenhausdatenschutzgesetz verankerte Datenschutzniveau zu verschlechtern (vgl. Ziff. 8.1.1 dieses Berichts).

Seit Ende 2002 befasst sich eine Arbeitsgruppe mit der Überarbeitung der Aktenordnung für die Behörden der Freien Hansestadt Bremen und der Stadtgemeinde Bremen. Die jetzt noch gültige Fassung stammt aus dem Jahr 1958 und ist dringend überarbeitungsbedürftig. Sie genügt weder den Anforderungen des Datenschutzes noch berücksichtigt sie die neuen technischen Anforderungen, die sich aus einer modernen Bürokommunikation ergeben. Die neue Aktenordnung soll die Rahmenvorgaben für den Umgang mit und die Organisation von Schriftgut geben, dessen nähere Ausgestaltung den senatorischen Bereichen überlassen werden soll. Ich habe in der Arbeitsgruppe mitgewirkt, die Arbeiten stehen kurz vor dem Abschluss.

Durch die Mithilfe des Rechtsausschusses konnte darüber hinaus im vergangenen Jahr erreicht werden, das Einvernehmen über den Inhalt einer Internet-Nutzungsrichtlinie zwischen den beteiligten Stellen herzustellen. Der Senator für Finanzen hat die I.8 Richtlinie für die Bereitstellung und Nutzung von Internet/Intranet Zugängen in Kraft gesetzt und Anfang 2004 im Amtsblatt (Brem.ABl. 2004, S. 77 ff.) veröffentlicht. Auch die Arbeiten an einer Verordnung zum Datenschutzaudit von öffentlichen Stellen (vgl. Ziff. 3.4 dieses Berichts) sind weitestgehend abgeschlossen, ich rechne mit einer baldigen Veröffentlichung. Die Richtlinien für die E-Mail-Nutzung in der Seestadt Bremerhaven, die für den Magistrat und die Vollzugspolizei unterschiedlich ausfallen werden, stehen kurz vor dem in Kraft setzen.

In Kraft getreten ist zwischenzeitlich auch die Änderung der bremischen Meldedatenübermittlungsverordnung (§ 5 Abs. 18 MeldDÜV), die die Einrichtung von Online-Zugriffen auf das Einwohnermelderegister durch die Amtsgerichte Bremen, Bremen-Blumenthal und Bremerhaven sowie das Landgericht Bremen ermöglicht (Brem.GBl. 2004, S. 37).

1.12 Internetauftritt: www.datenschutz.bremen.de

Der im Jahr 2001 begonnene Internetauftritt des Landesbeauftragten für den Datenschutz hat sich mittlerweile etabliert. Allerdings muss immer wieder Arbeit hineingesteckt werden, um die vorhandenen Seiten à jour zu halten. Der Aktualisierungsaufwand wird vom Besucher nicht gesehen, aktuelle Seiten werden einfach erwartet, eine nicht aktuelle Homepage wird binnen kurzer Zeit mit Nichtbeachtung gestraft. Der flüchtige Besucher ist häufig nur an Neuem interessiert. Ich habe daher auch im vergangenen Jahr das Angebot weiterentwickelt, wenn auch in 2003 ein Schwerpunkt in der Erstellung der CD "25 Jahre Datenschutz in der Freien Hansestadt Bremen" lag.

Natürlich kann ich mich mit dem umfassenden Angebot des Virtuellen Datenschutzbüros unter www.datenschutz.de nicht messen, sehe aber das Angebot auch nicht als Konkurrenz. Auf meiner Homepage liegen in erster Linie Seiten, die die Bürger im Land erreichen sollen; soweit darüber hinaus ein gutes bundesweit interessierendes Angebot auf meiner Internetseite besteht, wird dieses mit dem Virtuellen Datenschutzbüro verlinkt.

Eine projektbezogene Arbeitsgemeinschaft der Deutschen Hochschule für Verwaltungswissenschaften Speyer hat im Rahmen des Themas eGovernment „Datenschutz im Internet – Internet im Datenschutz“ die Internetauftritte der Datenschutzbeauftragten des Bundes und der Länder auf den Prüfstand gestellt. Wesentliche Kriterien waren hierbei der Inhalt und die Aufbereitung der Informationen, Benutzerfreundlichkeit, angebotene Kommunikation und Transaktion.

Dabei hat der Bremer Internetauftritt die bestmögliche Bewertung „außerordentlich erfreulich“ erhalten.

In dem Speyerer Arbeitsheft 2003, Nr. 153, werden die Homepages der Datenschutzbeauftragten in Bund und Ländern auf 60 Seiten genauestens untersucht. Für die Homepage des LfD Bremen wird besonders hervorgehoben, dass das Datenschuttscheckheft des Landesbeauftragten für den Datenschutz „eine sehr gute Übersicht von Downloadmöglichkeiten standardisierter Formulare zur Wahrung von Auskunftsrechten enthält“.

Die Anzahl der Aufrufe meiner Homepage ist auch immer ein Gradmesser für das Interesse der Internetgemeinde am Datenschutz. Ende 2002 landete ich mit dem Thema "Selbstverteidigung im Internet" einen Volltreffer, die Zugriffe auf die Homepage nahmen im Dezember rapide zu. Dies hielt auch noch im Januar 2003 an, danach gingen die Zugriffe um rund 20 Prozent zurück, stabilisierten sich aber auf einem höheren Niveau gegenüber dem Vorjahr. Besonders berichtenswert erscheint mir aber die Zahl der Downloads des letzten Jahresberichts. Der 25. Jahresbericht, der zum 31. März 2003 eingestellt wurde, ist bis Ende Dezember, also im letzten dreiviertel Jahr, 927 mal abgerufen worden, d. h., pro Monat werden über 100 Jahresberichte aus Bremen über das Internet nachgefragt. Allein die Gesamtzahl der Abrufe des Jahresberichts in elektronischer Form bis Dezember ist doppelt so hoch wie die Anzahl der für die Bürger in Papierform vorgehaltenen Jahresberichte. Drucklegung und Versandporto eingerechnet, rechtfertigt allein dieser eingesparte Posten die Kosten für meinen Internetauftritt.

1.13 Öffentlichkeitsarbeit und Presseresonanz

Auch im vergangenen Jahr habe ich wieder zu aktuellen Themen der Informationsverarbeitung Stellung genommen und in Pressemitteilungen und Interviews auf neue Entwicklungen im Datenschutz aufmerksam gemacht. Meine Pressemitteilungen sind jeweils aktuell auf meiner Homepage www.datenschutz.bremen.de abrufbar. Dass Datenschutzthemen auch im vergangenen Jahr einen breiten Raum in der Presseberichterstattung eingenommen haben, ist dem im Anhang beigefügten Pressespiegel (vgl. Ziff. 20.1 dieses Berichts) zu entnehmen.

1.14 Fortbildung durch den LfD

Im Berichtszeitraum haben Mitarbeiter des Landesbeauftragten für den Datenschutz verschiedene Fortbildungsveranstaltungen abgehalten oder mitgestaltet. Dies waren z. B. Veranstaltungen beim Aus- und Fortbildungszentrum der Bremischen Verwaltung (AFZ), an der Wirtschafts- und Sozialakademie der Arbeitnehmerkammer, bei Radio Bremen sowie Fortbildungen für Personalräte und für betriebliche Datenschutzbeauftragte zu speziellen, insbesondere technischen Themen. Weiter habe ich mich an der Schulung von Administratoren und Webmastern zur Internetnutzung in Schulen beteiligt. Eine gleiche Schulungsveranstaltung habe ich im Ökumenischen Gymnasium in der Stadt Bremen durchgeführt.

Auf Bitten der Dienstleistungsgewerkschaft „ver.di“ habe ich im Rahmen des Projektes Call-Center in Niedersachsen/Bremen auf einem Seminar und auf dem 21. Treffen des Netzwerkes von Call-Center-Beschäftigten auf einer Abendveranstaltung zum Thema „Arbeitnehmerdatenschutz in Call-Centern“ über die besonderen Datenschutzprobleme beim Arbeiten in Call-Centern referiert.

Im nächsten Jahr sehe ich insbesondere Fortbildungsbedarf für neu bestellte behördliche Datenschutzbeauftragte nach § 7a des BremDSG. Es ist beabsichtigt, für diesen Personenkreis in Zusammenarbeit mit dem AFZ und der datenschutz nord GmbH Fortbildungsveranstaltungen anzubieten.

1.15 Zur Situation der Dienststelle

Personelle Abgänge konnten durch personelle Neuzugänge aufgefangen werden, auch wenn dies nicht lückenlos gelang. Dabei gilt ein besonderer Dank dem Senator für Finanzen, der für ein Jahr einen Juristen aus seinem Einstellungspool an meine Dienststelle abgeordnet hat. Ohne diese Hilfe hätte ich meinen gesetzlichen Aufgaben nicht im erforderlichen Umfang nachkommen können. Die Lage wird im nächsten Jahr erneut prekär werden, weil durch den Abgang eines erfahrenen und bewährten Kollegen ohne erneute fremde Hilfe aus personalwirtschaftlichen Gründen kein Ersatz zur Verfügung stehen wird. Diese Situation wird sich in den nächsten Jahren noch erheblich verschärfen, wenn weitere Beschäftigte vorzeitig ausscheiden werden. Ich bin um Lösungen bemüht und benötige für die Überbrückung dieser Zeit gegebenenfalls auch politische Unterstützung.

Eine weitere Entwicklung ist berichtenswert: Im vergangenen Jahr ist es endlich gelungen, ein elektronisches Dokumentenmanagementsystem nach dem DOMEA-Prinzip in meiner Dienststelle einzuführen. Dazu mussten von allen Beschäftigten in der Dienststelle erhebliche Vorarbeiten geleistet werden, denn das System musste auf die Struktur und die Bedingungen der Dienststelle voreingestellt werden. In Schulungen waren dann vor Einführung alle Beschäftigten der Dienststelle mit den Funktionen und dem Aufbau des Systems vertraut zu machen, denn ab dem Zeitpunkt der Einführung musste jeder die Anwendung beherrschen. So muss jetzt jeder selbst seine E-Mails und andere elektronische Dokumente den entsprechenden Vorgängen zuordnen oder auch durch Recherche elektronisch abgespeicherte Dokumente im System auffinden. Auch die Ausgangsschreiben werden mit Hilfe des Systems erstellt.

Nicht leistbar wäre es gewesen, auch den gesamten alten Aktenbestand in das neue System zu integrieren. Ich habe mich dazu entschlossen, die alten Akten über einen Zeitraum von fünf Jahren auszusondern. Nur soweit nach dem Stichtag der Einführung des Systems Themen aus dem alten Aktenbestand aufgegriffen werden, werden diese in das neue System überführt. Dies wird dann im alten Aktenplan vermerkt. Auch das Scannen der gesamten eingehenden Post ist personell nicht leistbar, so dass es weiterhin neben der elektronischen Akte eine papierene Akte geben kann. In der elektronischen Akte ist aber erkennbar, welche weiteren Dokumente außerhalb des Aktenverwaltungssystems zu dem jeweiligen Vorgang bestehen. Eine über 25 Jahre eingefahrene Aktenverwaltung auf einen Stichtag hin umzustellen, ist kein leichtes Unterfangen und bedurfte der Anstrengung aller. Durch ihre Beteiligung bei der Auswahl und der Umsetzung des Systems ist eine hohe Akzeptanz in der Dienststelle erreicht worden. Auch wenn die Umstellung mit erheblichen Strapazen verbunden war und noch ist, zeichnet sich doch schon jetzt ab, dass sich der Schritt gelohnt hat und in vielen Bereichen zu erheblichen Arbeitserleichterungen führt. Selbstverständlich wurden für die Einführung des Systems Regelungen zur Aktenverwaltung getroffen und ein Datenschutzkonzept in Kraft gesetzt.

1.16 Kooperationen

Das Datenschutzgesetz verpflichtet zur Zusammenarbeit mit allen Stellen, die mit Kontrollaufgaben des Datenschutzes betraut sind (§ 27 Abs. 5 BremDSG). In der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die im vergangenen Jahr unter dem Vorsitz des Sächsischen Datenschutzbeauftragten tagte, wurden erneut eine Reihe von Entschlüssen gefasst, die die Fortentwicklung des Datenschutzes fördern sollen. Sie sind im Anhang zu diesem Bericht zu finden. Im Jahr 2004 geht der Vorsitz auf den Saarländischen Datenschutzbeauftragten über.

Angesichts der weiterhin rasanten technischen Entwicklung auf allen Gebieten der Informationsverarbeitung und unter engen personellen Ressourcen bei fast allen für den Datenschutz zuständigen Kontrollstellen, ist die Zusammenarbeit in den Arbeitskreisen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ein Gebot der Vernunft. Ich versuche im Rahmen der Möglichkeiten meines Reisekostenbudgets eine Teilnahme Bremens sicherzustellen.

Im Laufe des Jahres hat es wieder Wechsel unter den Datenschutzbeauftragten gegeben, so in Hessen und in Sachsen. Hervorheben möchte ich an dieser Stelle die Neuwahl von Peter Schaar zum Bundesbeauftragten für den Datenschutz (Plenarprotokoll 15/76, 14.11.2003, S. 6572 und S. 6584) und das Ausscheiden von Dr. Joachim Jacob nach Ablauf seiner zweiten Amtsperiode. Der Bundesbeauftragte für den Datenschutz wird auf fünf Jahre gewählt.

Weiter unterstütze ich das "Virtuelle Datenschutzbüro", dies ist der gemeinsame Internetauftritt der Datenschutzbeauftragten aus Deutschland, der Schweiz, den Niederlanden und Kanada. Das Virtuelle Datenschutzbüro hat sein Angebot erneut erweitert und verbessert. Es ist unter www.datenschutz.de zu erreichen.

Im Berichtszeitraum hat auch wieder ein Meinungsaustausch mit dem Datenschutzbeauftragten von Radio Bremen stattgefunden. Die Erörterung von Fragen gemeinsamen Interesses soll im kommenden Jahr fortgesetzt werden.

Auch mit der landeseigenen "datenschutz nord GmbH" hat es wieder eine Zusammenarbeit in verschiedenen Projekten, die nicht meiner Datenschutzkontrolle unterliegen, gegeben. Die GmbH hat mittlerweile in verschiedenen Projekten im Land Bremen zur Verbesserung des Datenschutzniveaus beigetragen. Ihre Unterstützung wird mittlerweile auch von Datenschutzkontrollinstanzen anderer Länder nachgefragt. Ich pflege mit der GmbH einen regelmäßigen Gedankenaustausch.

Was im öffentlichen Bereich durch die Konferenz der Datenschutzbeauftragten u. a. erreicht wird, nämlich die Findung gemeinsamer Positionen zu Themen mit länderübergreifenden Inhalten, wird im nicht öffentlichen Bereich durch den "Düsseldorfer Kreis" sichergestellt. Der „Düsseldorfer Kreis“ ist das Abstimmungsgremium unter den Datenschutzaufsichtsbehörden, um eine einheitliche Auslegung der Vorschriften des Bundesdatenschutzgesetzes für den privaten Bereich zu gewährleisten. Einige Ergebnisse finden sich im Abschnitt Ziff. 16. dieses Berichtes wieder.

Abgerundet werden soll der Bericht über die Kooperationen mit dem Hinweis, dass ich in der Funktion der Datenschutzaufsichtsbehörde für den nicht öffentlichen Bereich auch in 2003 wieder mit dem GDD Erfakreis Bremen/Weser-Ems, ein Kreis, in dem sich die betrieblichen Datenschutzbeauftragten der Region zusammengeschlossen haben und einen Meinungs- und Erfahrungsaustausch pflegen, zusammengearbeitet habe. Die Datenschutzaufsichtsbehörde informiert den Erfakreis oder seine Unterarbeitskreise gelegentlich in Vorträgen über neuere Entwicklungen. Wesentlicher Bestandteil der Zusammenarbeit sind technische und rechtliche Fragen, hier insbesondere Fragen der Auslegung des Bundesdatenschutzgesetzes und anderer spezialrechtlicher Regelungen des Datenschutzes, wie zum Beispiel des Teledienstedatenschutzgesetzes (TDDSG).

1.17 Entwicklungen in der Informationsgesellschaft

Im Dezember 2003 kam die internationale Staatengemeinschaft erstmals im Rahmen eines Weltgipfels der Vereinten Nationen zusammen, um Fragen der globalen Informationsgesellschaft zu erörtern. In diesem Zusammenhang hat die Bundesregierung den Deutschen Bundestag mit einem "Aktionsprogramm Informationsgesellschaft Deutschland 2006" über Stand und Perspektiven unterrichtet. Dem Bericht zufolge soll der Anteil der Internetnutzerinnen und -nutzer an der Bevölkerung ab 14 Jahren bis 2005 auf 75 Prozent steigen. Der Bericht enthält eine Vielzahl von interessanten Entwicklungen, zum Teil vergleichend in Diagrammen dargestellt und gibt am Ende eine Übersicht über die verschiedenen auf Bundesebene laufenden IT-Projekte (BT-Drs. 510/2315 vom 23.12.2003). Leider kommt der Datenschutz in dem Bericht entschieden zu kurz. Es wurde wieder einmal nicht erkannt, dass nicht nur Datensicherheit, sondern gerade auch der Datenschutz ein wichtiger Faktor für die Akzeptanz neuer Datenverarbeitungssysteme ist.

1.18 Schutz der Intimsphäre

Es treten immer wieder Fälle auf, in denen in Hotelzimmern, Toiletten, Dusch- und Umkleidekabinen oder gar im Badezimmer einer gemieteten Wohnung mit einer an einem versteckten Ort installierten Linse (Kamera) elektronisch beobachtet oder aufgezeichnet wird. Es kommt auch vor, dass heimlich in fremde Wohnungen oder andere gegen Einblick geschützte Bereiche hinein gefilmt oder fotografiert wird. Es ist unstrittig, dass die so traktierten Personen dagegen unzureichend geschützt sind.

Gegenwärtig besteht eine strafrechtliche Lücke im Bereich der Verletzung des höchstpersönlichen Lebens- und Geheimbereichs durch Bildaufnahmen. Während die Verletzung der Vertraulichkeit des Wortes (§ 201 Strafgesetzbuch (StGB)), die Verletzung des Briefgeheimnisses (§ 202 StGB), das unbefugte Ausspähen von Daten (§ 202a StGB) oder die Verletzung von Privatgeheimnissen (§ 203 StGB) strafbar sind, ist der Schutz der Intimsphäre vor unbefugten Bildaufnahmen nicht ausreichend strafrechtlich geschützt. Der Bundesrat hat daher am 26. September 2003 einen Gesetzesentwurf "zum verbesserten Schutz der Intimsphäre" verabschiedet und beschlossen, diesen beim Deutschen Bundestag einzubringen (BR-Drs. 164/03). Diese Gesetzesinitiative ist zu begrüßen. Der Gesetzesentwurf stellt dabei nur den höchstpersönlichen Lebensbereich in Wohnungen und geschützten Räumen unter einen besonderen strafrechtlichen Schutz.

Derzeit häufen sich die Klagen von Personen über mittels Multimedia-Handys mit eingebauter Kamera im öffentlichen Raum gemachte Bilder, die unbemerkt aufgenommen und weitergeleitet werden, ohne dass die Bürger dies unmittelbar wahrnehmen. Die so belästigten Personen würden wegen des von der Gesetzesinitiative gezogenen Schutzbereichs nicht daran teilhaben. Sie sind weiterhin auf den Schutz durch die Vorschriften des Kunsturhebergesetzes (Recht am eigenen Bild) angewiesen.

1.19 Ausweisdokumente und Biometrie

Es ist beschlossene Sache, dass auch die Personalausweise und Pässe der Bundesbürger mit einem Chip ausgestattet werden, auf dem biometrische Merkmale gespeichert werden sollen. Der Druck auf die EU wächst, insbesondere, weil die USA angekündigt haben, auch allen Europäern bei der Einreise Fingerabdrücke abzunehmen, wenn nicht bis Ende 2004 die Einreisedokumente eindeutig überprüfbare biometrische Merkmale enthalten. Bei der EU-Kommission und bei den G 8 Staaten wird über gemeinsame Lösungen beraten. Derzeit ist nicht abzusehen, ob noch im Jahr 2004 eine Entscheidung getroffen wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat schon im März 2002 (vgl. 25. JB, Ziff. 15.1) hierzu eine EntschlieÙung gefasst und darauf hingewiesen, dass die biometrischen Merkmale nur auf dem Chip im Ausweis und nicht in zentralen Datenbanken (Referenzdateien) hinterlegt werden sollen, damit der Bürger selbst die Verwendung seiner biometrischen Merkmale in den Händen behält. Gleiches gilt, denke ich, für die Auswahl zwischen den verschiedenen möglichen biometrischen Merkmalen (genauer vgl. 25. JB, Ziff. 3.3), die zur Verfügung stehen. Neben der Sicherheit muss ein zentrales Kriterium sein, dass der Bürger nur bewusst dieses Merkmal einem Prüfcomputer zur Verfügung stellt. Deshalb hielte ich einen Gesichtsscanner, der auch im Vorbeigehen unbemerkt per Gesichtserkennung einen Abgleich vornehmen kann, aus Sicht des Datenschutzes für nicht wünschenswert.

1.20 Auf dem Weg zum gläsernen Steuerbürger

Hatte die Gesetzgebung der letzten Jahre die Steuerflüchtlinge und die organisierte Kriminalität ins Auge gefasst, erinnert sei an das Gesetz zur Bekämpfung der Geldwäsche, das u. a. beim Bundeskriminalamt eine "Zentralstelle für Verdachtsanzeigen" geschaffen hat, das vierte Finanzmarktförderungsgesetz, das der Bundesanstalt für Finanzdienstleistungsaufsicht einen automatisierten Abruf von Kontoinformationen ermöglicht und eine Regelung zum sog. Konto-Screening enthält, so hat die jetzige Gesetzgebung den normalen Steuerbürger im Visier. Erkennbar wird, dass über die Kontrollmitteilungen der Banken an die Finanzbehörden hinaus der Steuerstaat sich immer stärker hin zu einer vorbeugenden Überwachung entwickelt. Vorsorgliche Ausforschung tritt an die Stelle anlassbezogener Ermittlungen und die Erhebung von Daten beim Betroffenen selbst. Die klassische Lohnsteuerkarte soll fortfallen, an ihre Stelle tritt die unmittelbare Übermittlung des Einkommens und der Steuerdaten durch den Arbeitgeber an das Finanzamt. Verbunden sind diese Änderungen mit der Einführung einer eindeutigen lebenslang geltenden Identifikationsnummer für Privatpersonen beziehungsweise eine Wirtschaftsidentifikationsnummer für wirtschaftlich arbeitende Betriebe und Personen, die vom Bundesamt für Finanzen vergeben wird.

Die datenschutzrechtlichen und tatsächlichen Auswirkungen der Einführung dieses Identifikationsmerkmals sind nicht einmal ansatzweise abzuschätzen, die Zweckbindung dieses Merkmals wird kaum sicherzustellen sein, die Verwendung wird erodieren (vgl. Ziff. 13.1 f. dieses Berichts). Die mit dem Steueränderungsgesetz 2003 vorgesehene Regelung sieht vor, unter einer "Electronic Taxpayer Identification Number" personenbezogene Daten der Meldeämter und Daten zu sämtlichen Steuerbereichen bundesweit zu speichern. Hinzutreten soll die Verpflichtung aller Kreditinstitute, alle Zinseinkünfte von Bürgern und Betrieben elektronisch an das Bundesamt für Finanzen zu melden. Damit ist der Grundstein für den Beginn einer lückenlosen Kontrolle der Steuerzahler gelegt. Da diese Entwicklung auf bundesgesetzlichen Ermächtigungen beruht, ist der Einfluss, den der einzelne Landesdatenschutzbeauftragte nehmen kann, begrenzt.

1.21 Erweiterung der Überwachung von Telekommunikationsverkehr und der Internetnutzung

Die Zahl der Telefonüberwachungen steigt seit Jahren ständig an. So haben die Telekommunikationsunternehmen der Regulierungsbehörde für Telekommunikation und Post für das Jahr 2001 19.896 Anordnungen und für das Jahr 2002 21.874 Anordnungen gemeldet, also ein deutlicher Anstieg binnen eines Jahres um über zehn Prozent. Die Zahl der Anordnungen steigt von Jahr zu Jahr beachtlich und hat sich seit 1995 bereits verfünffacht. Eine nachvollziehbare befriedigende Erklärung gibt es hierfür nach wie vor nicht. Auch das beim Max-Planck-Institut in Auftrag gegebene und von der Universität Münster durchgeführte Forschungsprojekt gibt hierzu keine hinreichenden Antworten. Die Datenschutzbeauftragten des Bundes und der Länder haben die Ergebnisse zum Anlass genommen und dem Gesetzgeber Vorschläge zur Verbesserung des Datenschutzes unterbreitet (vgl. Ziff. 18.14 dieses Berichts).

Über den Umfang, in dem der IMSI-Catcher (International Mobile Subscriber Identity) von Polizei und Geheimdiensten eingesetzt wird, gibt es keine publizierten Zahlen. Gleichwohl bedürfte auch der Einsatz dieses Instruments politischer Kontrolle. Der IMSI-Catcher simuliert eine Basisstation eines Mobilfunknetzes, bei der sich Handys in einem bestimmten Umkreis aus technischen Gründen anmelden. Durch den Einsatz des Gerätes können aber nicht nur die Karten- und Gerätedaten eines konkret gesuchten Handys zur Identifizierung des Anschlussinhabers genutzt werden, sondern auch alle anderen aktiven Mobiltelefone in seinem räumlichen Umfeld werden erfasst. Die Datenschutzbedenken bestehen darin, dass in die Überwachung mit dem IMSI-Catcher wegen der Umfeldererfassung zwangsläufig eine Vielzahl unverdächtiger Personen einbezogen werden. Darüber hinaus sind die in § 100i Strafprozessordnung (StPO) genannten Anordnungsvoraussetzungen zu weit gefasst.

In eine ähnliche Richtung geht der Einsatz der sog. "Stillen SMS". Dabei kann ein bestimmtes Handy gezielt angesprochen werden, ohne dass der Handybesitzer Kenntnis davon erlangt. Beim Handy-Provider werden daraufhin Nutzungsdaten erzeugt, die problemlos zur Standortbestimmung des Handys genutzt werden können. Weiterhin besteht die Möglichkeit, die Anfrage bei vorübergehend nicht erreichbaren Mobiltelefonen in eine Warteschleife zu stellen, so dass diese sofort, nachdem sie eingeschaltet wurden, antworten. Die genaue Wirkungsweise und die damit verbundenen Datenspeicherungen sind noch mit den Providern zu klären, Gleiches gilt für die rechtlichen Rahmenbedingungen.

Auch die Initiative des Bundesministeriums für Wirtschaft und Technologie, im Telekommunikationsgesetz (TKG) die Anbieter von Telekommunikationsdienstleistungen zu verpflichten, vor Herausgabe von Prepaid-Cards die Kundendaten zu erheben, und zwar unabhängig davon, ob sie die Daten für die Vertragsabwicklung benötigen, zielt darauf ab, die Bürger zu deanonymisieren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist mit einer EntschlieÙung (vgl. 25. JB, Ziff. 15.5) diesem Gesetzesvorhaben entgegengetreten.

In die Reihe technischer Unzulänglichkeiten hingegen gehört das Telefonieren im Internet. Hintergrund ist, dass beim Transport von Datenpaketen zeitliche Verzögerungen eintreten können und dadurch keine unterbrechungsfreie Kommunikation zustande käme. Deshalb wurde für Internet-Telefonie, die sog. "Voice over IP", ein "Real Time Transport Protocol (RTP)" entwickelt, das aber ein unsicheres Datentransportprotokoll nutzt, so dass Gespräche mit einfachen technischen Mitteln mitgehört werden können. Hier sind neue, sicherere technische Lösungen gefordert.

Während sich in den vergangenen Jahren die Bemühungen der Sicherheitsbehörden auf den Zugriff der bei den Anbietern von Telekommunikations- und Internetdienstleistungen bereits gespeicherten Daten konzentrierten, richten sich nunmehr die Bestrebungen der Politik, angetrieben durch die Sicherheitsbehörden, darauf, die Anbieter dazu zu verpflichten, insbesondere Bestands-, Verbindungs- und Nutzungsdaten ihrer Kunden "vorbeugend" für einen längeren Zeitraum für Zwecke der Strafverfolgung und der Nachrichtendienste zu speichern. Diese Speicherung soll unabhängig davon erfolgen, ob die Anbieter diese Daten selbst für die Abrechnung in Anspruch genommener Dienstleistungen mit ihren Kunden benötigen. Derartige Vorschläge stellen den Grundrechtsschutz im Bereich der Telekommunikation und der Internetnutzung und insbesondere den Schutz des Telekommunikationsgeheimnisses prinzipiell in Frage. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in mehreren Entschlüssen auf die Gefahren hingewiesen, die mit einer derartigen Entwicklung verbunden wären (vgl. Ziffern 18.6, 18.13 und 18.14 dieses Berichts).

Im Bereich der Telekommunikationsüberwachung bis hin zur Erstellung von Bewegungsbildern sind die Aktivitäten, Eingriffe in die Rechte der Bürger vorzubereiten, besonders stark ausgeprägt. Ständig werden neue Initiativen gestartet; dies macht auch die Vielzahl der Entschlüsse deutlich, die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder allein in den letzten zwei Jahren verabschiedet haben. Es ist Aufgabe aller demokratischen Kräfte, darüber zu wachen, dass das grundrechtlich garantierte Fernmeldegeheimnis nicht Stück für Stück ausgehöhlt wird und sich in Deutschland schleichend und fast unbemerkt eine Überwachungskultur entwickelt, deren tatsächliche Notwendigkeit und Effizienz nicht nachweisbar ist. Dies gilt auch im Hinblick auf die in den Koalitionsverhandlungen in Bremen getroffene Vereinbarung, die Telefonüberwachung zu präventiven Zwecken zuzulassen.

1.22 Keine Sicherheit im Haifischbecken Internet

So geht es vielen Internetsurfern: Das Netz spült ihnen Viren, Bugs und Würmer auf den Rechner, Programme installieren sich selbst und verändern den Rechner, Spyware und andere Programme saugen Daten vom Rechner an unbekannte Orte.

Einige empfinden die Unsicherheit der digitalen Medien, insbesondere des Internets, gerade als deren ungeheuren Reiz. Der Rechner nimmt insofern nur an ständigen Veränderungen teil. Während man mit dem Rechner arbeitet, holt er sich selbstständig etwas aus dem Netz und verändert sich, man partizipiert sozusagen an den ständigen Wandlungen im Netz. Dadurch entsteht für sie die besondere Faszination an dem Medium.

Andere hingegen wollen ein verlässliches Medium, sie wollen sich nicht fremdbestimmt mit ständigen Änderungen auseinandersetzen. Vielleicht benötigen sie die Leistung ihres Rechners für den Beruf, jedenfalls möchten sie selbst entscheiden, wann und was sich auf ihrem Rechner verändert.

Nun ist allenthalben klar, dass das Internet ein unsicheres Medium ist. Dafür ist es auch überhaupt nicht konzipiert. Im Gegenteil, vielen Surfern wird allmählich klar, dass sie die vielen schönen, kostenlosen Internetangebote häufig in Wahrheit mit ihren personenbezogenen Daten bezahlen müssen. Das Internet sicher zu machen, ist also ein zu großes, ja sogar unmögliches Unterfangen. Jeder ist, wie ich mit meiner Kampagne "Selbstverteidigung im Internet" im letzten Jahr deutlich gemacht habe, zunächst einmal selbst aufgefordert, für seine Rechtersicherheit zu sorgen und die jeweilige Defence-Software zu installieren und dann auch zu aktualisieren.

Darüber hinaus hält das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Plattform bereit, auf der weitere Sicherheitsinformationen zur Verfügung stehen. Auch große Industrieunternehmen haben bereits vor einigen Jahren einen eigenen Arbeitskreis zur Internetsicherheit (Arbeitskreis Schutz von Infrastrukturen/Aksis) gegründet. In ähnliche Richtung geht eine von der Bundesregierung eingesetzte Arbeitsgruppe "Kritische Infrastrukturen (Kritis)", die Abwehrstrategien für Risikoszenarien entwickelt.

Dass PCs sicherer werden müssen, darüber sind sich ausnahmsweise einmal alle Experten einig. Sobald es aber um das konkrete "Wie" geht, scheiden sich die Geister. Führende Hard- und Softwarehersteller versuchen, mit Palladium und TCPA (Trusted Computing Platform Alliance) den PC zu "versiegeln". Sie haben sich in einem Firmenkonsortium zusammengeschlossen, um eine neue, sicherere Hardwareplattform für PCs und andere vernetzte Geräte zu schaffen. Deren Kernstück ist das "Trusted Platform Module (TPM)", in dem sich ein eigener Prozessor und ein gesicherter Speicher befinden. In dem TPM werden Prüfsummen von BIOS, Bootsektor und anderen Hardwarekomponenten gespeichert, um ein sicheres Betriebssystem zu booten. Dieses identifiziert den Rechner über den TPM bei einem Server oder Diensteanbieter im Internet. Und hier setzen nun die Forderungen der Datenschutzbeauftragten an: Wäre der TPM nicht ein fest installierter Chip, dessen Funktionen für den Benutzer nicht klar erkennbar sind, insbesondere nicht, ob er Informationen über das Netz an die Hersteller weitergibt, sondern könnte der Benutzer frei darüber entscheiden, wann er mit dem Chip die Sicherheit aktiviert und nutzt und wann nicht, wäre sicherlich

vielen wohler (zu den Gefahren vgl. Ziff. 18.2, zu automatischen Software-Updates Ziff. 18.11 dieses Berichts).

Vielen Anwendern, die Sicherheit haben wollen und die erwarten, dass ihre persönlichen und personenbezogenen Daten nur für bestimmte Zwecke genutzt werden, vertraulich bleiben und nicht unautorisiert verändert werden können, fehlt das notwendige Wissen, um beurteilen zu können, ob die eingesetzten Systeme vertrauenswürdig sind. Auf Marketingaussagen und Versicherungen der Softwarehersteller möchte sich niemand wirklich abschließend verlassen. Auch ist für den Verbraucher nicht zu erkennen, ob ein Datenverarbeitungssystem nur das Allernötigste für den Datenschutz tut, ob Lücken vorhanden sind oder ob ein hoher Datenschutzstandard implementiert ist. Und gerade hier setzt der Gedanke der Auditierung an (vgl. auch Ziffern 3.4 und 18.3 dieses Berichts). Ein von Sachverständigen untersuchtes System wird nach festgelegten Datenschutzkriterien bewertet und erhält, wenn es alle Datenschutzerfordernungen erfüllt, ein Gütesiegel verliehen.

1.23 Weitere Folgen der Anschläge vom 11. September 2001

Dass die Folgen des 11. September 2001 noch lange wirken würden, habe ich bereits in meinem 24. Jahresbericht (dort Ziff. 1.1) prognostiziert. Dabei meinte ich nicht die kriegerischen Aktionen in Afghanistan oder im Irak, sondern die tiefen Eingriffe in das informationelle Selbstbestimmungsrecht. In einer ersten Reaktion wurden in der Bundesrepublik, insbesondere den Nachrichtendiensten im Terrorismusbekämpfungsgesetz vom 9. Januar 2002, weiterreichende zusätzliche Befugnisse eingeräumt.

Eine weitere tiefgreifende Maßnahme war die jetzt abgeschlossene Rasterfahndung, in die Datensätze von mehreren hunderttausend Bürgern einfließen; ein damit verbundener Fahndungserfolg wurde bisher nicht publik.

Die Einführung von biometrischen Merkmalen in Visa bei der Einreise in die Bundesrepublik ist in 2003 vollzogen, am 28. November 2003 haben sich die Innen- und Justizminister/innen der EU in Brüssel über die Einführung biometrischer Merkmale in Visa und Aufenthaltstiteln für Drittstaatenangehörige geeinigt. Die geplante Einführung von biometrischen Merkmalen in Pass und Personalausweis gegen die eigene Bevölkerung werden folgen. Einreisende in die USA aus Nicht-EU-Ländern dürfen sich jetzt schon wie Schwerekriminelle fühlen, müssen sie doch seit Anfang des Jahres ihre Fingerabdrücke nehmen lassen. Darüber hinaus wird weltweit ein kostenintensiver Kontroll- und Überwachungsapparat zur maritimen und zur Luftsicherheit aufgebaut (vgl. Ziffern 12.1 und 12.2 dieses Berichts)

Im "Kampf gegen die Achse des Bösen" versuchte die US-Bundesregierung auch bei den Flugdaten, unter Hintanstellung europäischen und nationalen Rechts eine Vorrangstellung zu erzwingen. Den Rahmen hierfür bilden folgende Zahlen: Allein rund 100.000 Menschen arbeiten für die CIA (Central Intelligence Agency), weitere US-Geheimdienste sind die NSA (National Security Agency), die die weltweiten Abhörtätigkeiten steuert, die NRO (National Reconnaissance Office), die sich mit der Auswertung von Satellitenbildern befasst, die DIA (Defence Intelligence Agency), die Spionageabteilung der Armee sowie Teile des FBI (Federal Bureau of Investigation) und Abteilungen des Außen-, Energie- und des Finanzministeriums. Mehr als 170.000 Menschen sollen in Zukunft dem Department of Homeland Security (DHS) dienen, einem Superministerium, das nur die Aufgabe hat, die Vereinigten Staaten vor terroristischen Angriffen zu schützen. Sicherheitsspezialisten aus 22 US-Behörden haben in den vier Hauptabteilungen des DHS künftig ein neues Aufgabenfeld.

Und nun greift das von den USA neu gegründete DHS auf europäische Flugreservierungssysteme zu. Darin können in weit mehr als einhundert Datenfeldern besondere Daten zu jedem einzelnen Fluggast gespeichert werden (vgl. Ziff. 17.3 dieses Berichts). Die USA dürfen sich derzeit uneingeschränkt bedienen. Hier sind nicht nur die Flüge in die USA, sondern auch alle anderen, z. B. innereuropäischen Flüge gespeichert. Die USA interessieren sich dabei nicht nur für die Identität der einzelnen Flugpassagiere, sondern auch, z. B., wer neben wem im Flugzeug gesessen hat und mit welchen Kreditkarten und -nummern bezahlt wurde. Die Anträge der DHS, auf Banken- und Kreditkartensysteme in den USA Zugriff nehmen zu können, sollen schon gestellt sein. Das Szenario

wird deutlicher, wenn man die Leistungsfähigkeit modernster Data-Mining-Produkte hinzu denkt. Diese Software kann in beliebig vielen Schichten in hoch komplexen Informationssystemen Daten auffinden und korrelieren.

Hat das DHS den Zugriff auf Banken- und die Kreditkartensysteme, kann man in den USA, wo fast ausschließlich bargeldlos bezahlt wird, jederzeit feststellen, z. B. wann und wo der Fluggast einen Hamburger gegessen oder ein Hotel bezahlt hat. Und bei manchen Kreditkartensystemen wird sich das sicherlich nicht nur auf die USA beschränken. Damit wird deutlich: Das ganze System verdächtigt prinzipiell alle und stellt damit einen Ansatz dar, der in krassem Widerspruch zum europäischen Datenschutzgedanken steht, der sich in der Europäischen Datenschutzrichtlinie manifestiert. Viele der grundlegenden Prinzipien, wie die Erforderlichkeit, die Zweckbindung, die vorrangige Erhebung der Daten beim Betroffenen etc. werden außer Kraft gesetzt. Es besteht damit die Gefahr, dass unter der Vorgabe, Demokratie und Freiheit zu schützen, diese Werte gefährdet werden.

1.24 Die neue elektronische Gesundheit (eGesundheit)

Einen weiteren Schwerpunkt meiner Beratungen stellte in den letzten Jahren und stellt auch in der Zukunft die Gesundheitsreform dar. Der Umbau des Gesundheitssystems bringt radikale Einschnitte mit sich, die mehr Kontrolle der Leistungen und Kosten beinhalten und daher auf völlig neue Datenbasen gestellt werden sollen (vgl. Ziff. 8.8.3 dieses Berichts). Damit einher geht die zunehmende elektronische Erfassung und Übermittlung von Gesundheits- und Abrechnungsdaten, die u. a. eine verbesserte Datenbasis für die Behandlung bringen sollen (Lipobay-Skandal), die Leistungsabwicklung transparenter und kontrollierbarer machen sowie die Kostenkontrolle vereinfachen soll. Dabei bedient man sich umfassender elektronischer Datenverarbeitung in der Hoffnung, die Verwaltungs- und Abrechnungsabläufe zu effektivieren. Da an allen Ecken des Gesundheitssystems zugleich verändert wird, ist im Moment schwer einzuschätzen, welche DV-Verfahren sich durchsetzen oder Bestand haben werden. Hinzu kommt, dass viele neue Projekte mit unterschiedlichsten Ansätzen zur Datenverarbeitung entwickelt werden, wobei teilweise Pilotprojekte nicht einmal zu Ende geführt sind, geschweige denn deren Ergebnisse evaluiert sind, da werden sie schon bundesweit eingeführt. Neue chipkartenbasierte Projekte, die mit Piloten in verschiedenen Teilen Deutschlands durchgeführt werden, treten hinzu. Da ist es angesichts der geringen personellen Kapazitäten bei den Datenschutzbeauftragten kaum mehr leistbar, eine solide Datenschutzberatung durchzuführen. Gelegentlich könnte auch der Eindruck entstehen, dieser Rat werde gar nicht verlangt. Während die gesetzlichen Krankenkassen mit erheblichem finanziellen und technischen Aufwand versuchen, das Gesundheitssystem grundlegend zu verändern, ist bei den privaten Krankenversicherungen eher eine gewisse Zurückhaltung festzustellen. Die Hoffnung, mit großen Datenmengen und komplexen Datenverarbeitungssystemen zum Erfolg zu gelangen, hat sich schon in anderen Bereichen als Holzweg erwiesen. Je mehr Beraterverträge man vergibt, desto mehr Ratschläge hat man im nachhinein zu koordinieren. Im Moment scheint nicht hektischer Aktionismus gefragt, sondern ein wenig Besinnung auf das Wesentliche.

1.25 Mikrochips zum Aufbügeln

Warenhersteller und Handel setzen zunehmend weltweit Radio-frequenz-gestützte Mikrochips (RFID-tags) zur Kennzeichnung von Warenbeständen wie auch zur Preisauszeichnung ein. Diese im Mikrobereich weniger als Millimeter großen Chips sollen als „schlaue Etiketten“ den bisherigen Strichcode (Barcode) ersetzen. Darüber hinaus sind Verfahren angedacht, die Verfolgung von Gegenständen mit den RFID-tags zu ermöglichen. Die RFID-tags sind miniaturisierte IT-Systeme, die über eine Antenne Funksignale empfangen oder abgeben können. Die dafür erforderliche elektrische Energie wird über das Funksignal eines RFID-Lesegerätes bereit gestellt, so dass das RFID-tag ohne eigene Energiequelle funktionieren kann. Die Entfernung, auf die diese RFID-tags angesprochen werden können, kann im Zentimeterbereich liegen, es gibt aber auch Reichweiten bis zu 30 Metern. Die RFID-Technologie wird sich aufgrund geringer Herstellungskosten in naher Zukunft weltweit ausbreiten. Der Anwendungsbereich liegt bei der Kennzeichnung von Waren, der Markierung von Gegenständen, um sie auf diese Weise vor Diebstahl zu sichern, bis hin zur Verfolgung von Gegenständen in der Produktion und im Vertrieb. Damit könnte das verloren gegangene Hemd in der Reinigung bald der Vergangenheit angehören, ein im Kragen mit eingewebtes RFID-tag könnte jederzeit darüber Auskunft geben, wo sich das Hemd gerade befindet. Die Europäische Zentralbank hat zudem bereits angekündigt, Eurobanknoten mit entsprechenden Mikrochips auszustatten.

Die neue Technologie ist Teil der globalen Entwicklung hin zu einer „intelligenten Umgebung“ und zur allgegenwärtigen Datenverarbeitung. Diese Entwicklung fordert aber auch neue Antworten durch den Datenschutz. Hierauf hat die Internationale Konferenz der Datenschutzbeauftragten in einer EntschlieÙung hingewiesen (vgl. Ziff. 19.2 dieses Berichts).

Bei einer weiten Verbreitung der RFID-tags ist auch daran gedacht, dass diese untereinander kommunizieren können. Auf diese Weise könnte eine neue Dimension von Bewegungsprofilen entstehen. Um bei dem vorgenannten Beispiel zu bleiben: Genauso wie der Weg des Hemdes in der Reinigung verfolgbar ist, wäre auch der Weg des Trägers eines solchen Hemdes verfolgbar. Würde darüber hinaus noch der Käufer bei Zahlung mit Kreditkarte festgehalten, wäre die Personenbeziehbarkeit hergestellt. Sollten die Banknoten, wie angekündigt, mit entsprechenden RFID-tags ausgestattet werden, würde damit auch das Geld seine Anonymität verlieren, würde bei der Auszahlung am Geldautomaten festgehalten, an wen ein bestimmter Geldschein ausgegeben wurde, lieÙe sich auch der Weg des Geldes weiter verfolgen. Wichtig wird also sein, sicher zu stellen, dass der Eigentümer selbst darüber entscheiden kann, ob bzw. in welchem Umfang Funktionen eines RFID-tags aktiviert sind.