

1. Vorwort

Der Schwerpunkt meines Jahresberichts liegt auf dem Datenschutz im Land Bremen. Gleichwohl nehme ich wie in jedem Jahre im Vorwort die Gelegenheit wahr, über technische und gesellschaftliche Entwicklungen zu berichten, die zwar nicht in Bremen entstanden sind, die aber das Recht auf informationelle Selbstbestimmung tangieren und deren Auswirkungen auch die Bremer Bürgerinnen und Bürger zu spüren bekommen. Rückblickend betrachtet lässt sich die eine oder andere Entwicklung im Lande so besser einordnen.

Dies gilt z. B. auch für das wohl herausragendste datenschutzrechtliche Ereignis des vergangenen Jahres, das Urteil des Bundesverfassungsgerichts zum Lauschangriff. Obwohl es unmittelbar nur für die Strafprozessordnung gilt, hat es doch auch Auswirkungen auf das Bremische Polizeigesetz und die geplante Novellierung des bremischen Verfassungsschutzgesetzes.

Im Lande Bremen selbst hat der Datenschutz in den letzten Jahren ein Ziel erreicht. Er muss sich von wenigen Ausnahmen abgesehen nicht mehr in Erinnerung rufen, sondern die öffentlichen Stellen kommen mit ihren Problemen zu mir und lassen sich umfassend beraten oder entwickeln selbst gute Datenschutzkonzepte. So enthält dieser Bericht auch weitestgehend keine Mängellisten über Datenschutzverstöße, sondern kann über viele Erfolge berichten. Ebenso ist im privaten Sektor ein deutlicher Sinneswandel zu verspüren. „Privacy sells!“. Auch hier hat man verstanden, was dieser Slogan in knapper Form zum Ausdruck bringt.

1.1 Auditverordnung zum Bremischen Datenschutzgesetz

Die nach § 7 b Bremisches Datenschutzgesetz (BremDSG) vorgesehene Auditverordnung ist am 15. Oktober 2004 in Kraft getreten (Brem.GBl. 2004, S. 515). Bremen hat damit den Bund überholt, der seine Auditregelung noch nicht umgesetzt hat, und ist nach Schleswig-Holstein das zweite Bundesland mit einem Datenschutzaudit. In Bremen kann jetzt das Datenschutzaudit in der Praxis zum Einsatz kommen. Öffentliche Stellen Bremens können zur Verbesserung des Datenschutzes und der Datensicherheit ihre Verfahren einschließlich der dazugehörigen technischen Einrichtungen durch unabhängige Gutachter prüfen und bewerten lassen.

Ziel des Datenschutzaudits ist die Verbesserung des Datenschutzes und der Datensicherheit. Nach erfolgreicher Durchführung eines Datenschutzauditverfahrens durch einen externen Gutachter wird dem geprüften Verfahren ein datenschutzrechtliches Gütesiegel verliehen, mit dem die datenverarbeitende Stelle hinsichtlich ihrer Vertrauenswürdigkeit werben kann. Durch das Audit soll die Selbstverantwortung der Datenverarbeiter gefördert werden. Ein geprüftes Verfahren erhält durch die Auditierung Akzeptanz nach außen. Das Datenschutzgütesiegel ermöglicht es Bremer Stellen darüber hinaus, z. B. ihre Software-Produkte in anderen Ländern besser zu vermarkten, und schafft so auditierten Stellen einen Wettbewerbsvorteil. Wegen der rasanten technischen Weiterentwicklung wird das Datenschutzaudit-Gütesiegel auf zwei Jahre befristet erteilt. Für Verlängerungen besteht aber die Möglichkeit eines vereinfachten Verfahrens.

1.2 Einführung der elektronischen Arbeitszeiterfassung

Der Rechnungshof hat im Jahr 1992 die Einführung einer elektronischen Arbeitszeiterfassung in der bremischen Verwaltung gefordert. In der Folgezeit sind verschiedene Modelle erörtert und von mir datenschutzrechtlich begleitet worden. Daraus sind die „Grundsätze für die gleitende Arbeitszeit“ entstanden, die festlegen, dass ein Datenschutz- und ein Sicherheitskonzept sowie eine Verfahrensbeschreibung zu erstellen sind. Rechtliche Grundlage für die Arbeitszeiterfassung ist eine Dienstvereinbarung vom März 1999. Darin werden auch die zulässigen Kontrollen durch Vorgesetzte geregelt. Besonderes Augenmerk habe ich darauf gerichtet, dass keine heimlichen Kontrollen hinter dem Rücken der Beschäftigten stattfinden. Über die Datenschutzaspekte habe ich auch im Rechtsausschuss berichtet. Ende des Jahres waren ca. 30 Dienststellen an das zentrale System angeschlossen.

1.3 eGovernment

Die staatlichen und kommunalen Stellen im Land Bremen bieten ihre Serviceleistungen zunehmend auf elektronischem Wege an, um damit unabhängig von Öffnungs- oder Wartezeiten, Parkplatzproblemen und anderen Hürden den Kontakt zu ihnen zu ermöglichen. Das Motto der elektronischen Verwaltung lautet: "Nicht die Bürger sollen laufen, sondern die Daten". Umfangreiche Online-Informationen über Verwaltungsdienstleistungen, Erreichbarkeit der Beschäftigten per E-Mail, Formular-Downloads und andere Internetanwendungen vereinfachen die Verfahrensabläufe und sollen die Kosten für die öffentliche Verwaltung senken. Dieser Prozess wird sich auch in den nächsten Jahren fortsetzen.

Die Bürger erwarten dabei von der Verwaltung kürzere Bearbeitungszeiten und niedrigere Kosten. Ob sich dabei die Hoffnungen auf weniger Bürokratie durch eGovernment verwirklichen lassen oder sich, wie einige befürchten, doch nur eine E-Bürokratie entwickelt, bleibt abzuwarten. Die Reformaktivitäten zielen dabei vornehmlich auf Massenverfahren wie im Bereich Melde- und Kfz-Wesen oder bei den elektronischen Steuererklärungen ab.

Untersuchungen haben ergeben, dass die Mehrheit der Bürger die Web-Angebote der öffentlichen Verwaltung in erster Linie zur reinen Informationsbeschaffung nutzen. Immerhin 47 % der regelmäßigen Internet-Nutzer nehmen Verwaltungsdienstleistungen über das Internet in Anspruch. Deutschland liegt im internationalen eGovernment-Ranking im hinteren Mittelfeld auf Platz 14. Rund 18 % der Web-User haben Bedenken, dass der Datenschutz beim eGovernment möglicherweise unzureichend sei.

Dies verdeutlicht einmal mehr, dass eine hohe Akzeptanz der Bürger nur dann erreicht werden kann, wenn Datenschutz und Datensicherheit gewährleistet sind. Voraussetzung dafür ist eine sichere und vertrauliche Kommunikation zwischen Bürgern und der Verwaltung, die einen angemessenen Schutz der personenbezogenen Daten gewährleistet. Ich habe gemeinsam mit den anderen Datenschutzbeauftragten des Bundes und der Länder Handlungsempfehlungen für ein "Datenschutzgerechtes eGovernment" erarbeitet. Darin werden die spezifischen Anforderungen und Risiken, die mit dem eGovernment verbunden sind, ausführlich beschrieben. Einen großen Raum nehmen konkrete Empfehlungen und die Beschreibung von technischen und organisatorischen Schutzmaßnahmen ein. In einer Risikoanalyse sind die spezifischen Gegebenheiten zu betrachten und daraus technische und organisatorische Maßnahmen abzuleiten. IT-Verantwortliche können die aufgelisteten Handlungsempfehlungen als Checklisten nutzen, um Maßnahmen und Vorkehrungen für datenschutzgerechte und sichere eGovernment-Anwendungen festzulegen. Für die Bürger sind insbesondere die vorgestellten Instrumente des Selbst-Datenschutzes von großer Bedeutung.

Darüber hinaus habe ich mich im Berichtszeitraum intensiv um die Entwicklung der virtuellen Poststelle gekümmert. Dabei habe ich selbst an dem Pilotverfahren der bremischen Verwaltung teilgenommen, um so praktische Erfahrungen zu sammeln. Dadurch fällt es mir leichter, die notwendigen Schutzkonzepte zu entwickeln (Näheres vgl. Ziff. 3.1 dieses Berichts). In diesem

Zusammenhang verweise ich auf die Ausarbeitung „Die virtuelle Poststelle im datenschutzgerechten Einsatz“. Das Dokument kann in Kürze von meiner Homepage heruntergeladen werden.

1.4 Behördliche Datenschutzbeauftragte

Mit der Novellierung des Bremischen Datenschutzgesetzes (BremDSG) im Dezember 2002 wurde eine Norm aufgenommen, die die öffentlichen Stellen in Bremen und Bremerhaven zur Bestellung eines behördlichen Datenschutzbeauftragten verpflichtet (vgl. § 7 a BremDSG). Die Bestimmung regelt die Stellung des behördlichen Datenschutzbeauftragten innerhalb der öffentlichen Stelle, seine Aufgaben sowie Anforderungen an Eignung und Qualifikation. Die öffentlichen Stellen haben dem Landesbeauftragten für den Datenschutz die Bestellung und Beendigung eines behördlichen Datenschutzbeauftragten zu melden. Entsprechende Regelungen gibt es auch im Bundesdatenschutzgesetz und in Datenschutzgesetzen anderer Länder. Die Privatwirtschaft ist seit jeher verpflichtet, betriebliche Datenschutzbeauftragte zu bestellen.

Bedauerlicherweise hatte ich von einem Großteil der verpflichteten Stellen in 2003 keine Meldung über eine Bestellung gem. § 7 a Abs. 5 BremDSG erhalten. Entweder hatte man die Bestellung nicht vorgenommen oder mir nach einer Bestellung diese nicht gemeldet. Diese Stellen forderte ich auf, ihrer gesetzlichen Verpflichtung nachzukommen. In diesem Zusammenhang wies ich darauf hin, dass mehrere Stellen gemeinsam einen behördlichen Datenschutzbeauftragten bestellen können, nicht jede Stelle also einen eigenen Datenschutzbeauftragten bestellen muss, was insbesondere für kleinere Einrichtungen von Bedeutung sein dürfte.

Mittlerweile haben ca. 80 % aller Dienststellen der bremischen Verwaltung einen behördlichen Datenschutzbeauftragten gemeldet. In den restlichen Fällen sind häufig noch Rechtsfragen zu klären, die z. B. die Eignung und Qualifikation eines für das Amt des behördlichen Datenschutzbeauftragten vorgesehenen Mitarbeiters betreffen. Zur Qualifizierung biete ich Schulungen im Aus- und Fortbildungszentrum der bremischen Verwaltung an. Die bisherige Resonanz war sehr gut.

Aus dem Bereich des Magistrats der Stadt Bremerhaven habe ich bisher keine Meldung nach § 7 a Abs. 5 BremDSG erhalten. Ende 2004 sind mir vom Magistrat Überlegungen vorgestellt worden, grundsätzlich für jeweils ein Dezernat einen behördlichen Datenschutzbeauftragten zu bestellen. Aufgrund der Größe der Ämter und Einrichtungen in einem Dezernat oder besonderer für sie geltender Rechtsvorschriften ist geplant, für ein Amt allein oder dezernatsübergreifend einen behördlichen Datenschutzbeauftragten zu bestellen. Auch bei den Wirtschafts- und Eigenbetrieben stehen noch einige Meldungen über die Bestellung eines behördlichen Datenschutzbeauftragten aus.

1.5 Datenschutzrechtliche Beratung neuer Rechtsvorschriften im Land

Im Juli 2004 traten die Vorschriften des Bremischen Hafensicherheitsgesetzes in Kraft (Brem.GBl. 2004, S. 405). Mit den Änderungen soll den Anforderungen aus dem Konzept zur „Maritimen Sicherheit“ Rechnung getragen werden, ich berichtete hierzu ausführlich (vgl. 26. JB, Ziff. 12.2). Weiter habe ich Änderungen im Landesmediengesetz (vgl. Ziff. 2.3 dieses Berichts) und im Bremischen Wassergesetz beraten (Brem.GBl. 2004, S. 595), die die Erhebung von Daten zum Zwecke von Hochwasserschutzgebühren bei Grundstücksbesitzern betreffen. Zu erwähnen ist auch die Einfügung des § 46 a in das Bremische Abgeordnetengesetz (Brem.GBl. 2004, S. 597). Anlass war die beabsichtigte Nutzung der aus den USA zurückgeführten sog. Rosenholzdateien. Die Überprüfung von Abgeordneten auf Stasi-Kontakte ist ein Eingriff in deren informationelles Selbstbestimmungsrecht und kann daher nur auf Grund einer Einwilligung oder einer gesetzlichen Ermächtigung erfolgen. Ein mehrheitlicher Beschluss des Parlaments wäre hingegen keine ausreichende Grundlage für eine solche Datenabfrage. Es ist daher zu begrüßen, dass mit der Schaffung einer gesetzlichen Grundlage Rechtsklarheit geschaffen wurde. Schließlich habe ich den aus dem Hause des Senators für Bildung und Wissenschaft stammenden Arbeitsentwurf zur Novellierung des bremischen Schuldatenschutzgesetzes beraten, der sich nunmehr in der hausinternen Abstimmung befindet (vgl. Ziff. 10.3 dieses Berichts). Auch zu Novellierungsvorschlägen aus dem Innenressort, das Bremische Polizeigesetz und das bremische Verfassungsschutzgesetz betreffend, habe ich Stellungnahmen abgegeben (vgl. Ziff. 6.9 und Ziff. 6.10 dieses Berichts).

1.6 **www.datenschutz4school ist gestartet**

Mit Unterstützung aus dem Hause des Senators für Bildung und Wissenschaft habe ich das Online-Lernprojekt „datenschutz4school“ entwickelt. Am 22. Dezember 2004 ging die Lerneinheit online. Sie wird im Rahmen des Computerunterrichtes an Schulen eingesetzt, ein pädagogisches Konzept für die Lehrerinnen und Lehrer ist hinterlegt.

Zielgruppe sind Schülerinnen und Schüler zwischen zwölf und 15 Jahren. Schüler gehen schon in jungen Jahren ins Internet und haben häufig keine Vorstellung davon, wie viele Spuren sie dort hinterlassen. Um

Lebenslagen der
Informationen

sonst. Die

Mit dem Angebot



ein Bewusstsein dafür zu schaffen, habe ich an Jugendlichen orientiert eine Reihe von zusammengestellt - im Internet natürlich, wo Adresse lautet: „www.datenschutz4school.de“.

sollen Jugendliche für den Datenschutz sensibilisiert werden. Sie sollen lernen, wie sie sich selbst um ihre Belange beim Datenschutz kümmern können und welche Rechte sie haben.

Die Lerneinheit „datenschutz4school“ gliedert sich in vier Kapitel. Jedes Kapitel wird durch ein Tier der Bremer Stadtmusikanten animiert. Die Kapitel beinhalten am Ende ein oder zwei im Quizformat aufgemachte Tests zur Überprüfung des Erlernten. Mit richtigen Antworten kann man Bonus-Punkte sammeln, die in einem anschließenden Spiel eingesetzt werden können. Spielziel ist die richtige Anordnung der Bremer Stadtmusikanten in einer Slotmaschine. Die besten Ergebnisse können in einer Top-10-Highscoreliste unter Angabe der Schule eingetragen werden. Die ständig wechselnden Eintragungen bereits in den ersten Wochen seit dem Start in der Liste zeigen, dass die Seite stark frequentiert wird.

1.7 Erweiterte Datenbasis bei der GEZ

Im Berichtsjahr habe ich zusammen mit anderen Datenschutzbeauftragten der Länder eine Datenschutzprüfung bei der GEZ durchgeführt. Da die GEZ gerade dabei ist, ein neues DV-Verfahren einzuführen, konnte dieses mit einbezogen werden. Der Prüfbericht befindet sich seit Anfang 2005 in der Abstimmung, die wesentlichen Ergebnisse können daher erst im nächsten Jahresbericht dargestellt werden.

Im Berichtsjahr wurden von den Ministerpräsidenten ohne vorhergehende Beteiligung der Datenschutzbeauftragten - wie es z. B. im Bremischen Datenschutzgesetz (BremDSG) vorgesehen ist - Änderungen im Rundfunkgebührenstaatsvertrag beschlossen. Unter anderem darf sich danach die GEZ bei kommerziellen Adresshändlern Daten beschaffen. Damit wird zusätzlich zu dem aus Sicht des Datenschutzes problematischen Zugriff auf Daten des Melderegisters im Zusammenhang mit der Gebührenerhebung der Rundfunkanstalten ein weiteres Tor für eine unverhältnismäßige Datensammlung geöffnet. Die Konferenz der Datenschutzbeauftragten hat stets die Praxis der GEZ kritisiert, jährlich mehrere Millionen Adressen ohne Kenntnis der Betroffenen beim kommerziellen Adresshandel zu beschaffen (Näheres vgl. Ziff. 2.2 dieses Berichts). Einen nicht unwesentlichen Anteil machen bei mir jedes Jahr Bürgerbeschwerden über oft unsinnige Schreiben aus Mailingverfahren der GEZ aus, bei denen offensichtlich Daten aus dem Adresshandel verwendet wurden. Es wäre daher an der Zeit, stattdessen die von den Datenschutzbeauftragten seit langem geforderte grundsätzliche datenschutzfreundliche Neuorientierung bei der Finanzierung des öffentlich-rechtlichen Rundfunks in Angriff zu nehmen (vgl. Entschließung der Konferenz „Neuordnung in der Rundfunkfinanzierung“, 26. JB, Ziff. 18.9).

1.8 Gravierende Datenschutzmängel beim Arbeitslosengeld II (ALG II)

Immer neue Probleme und Pannen tauchen mit dem Computerprogramm „A2LL“ auf, das die Grundlage für die Gewährung und Abrechnung des Arbeitslosengeldes II (ALG II) bildet. Verzögerte erst ein Stellenfehler bei den Kontonummern der Leistungsempfänger in Teilbereichen die Auszahlung des Arbeitslosengeldes, konnten danach Barschecks mit der Post nicht zugestellt werden, weil das Programm nach einer bestimmten Anzahl von Zeichen die Straßennamen abkürzte. In diese Reihe gliedern sich auch die zahlreichen, zum Teil erheblichen technischen und tatsächlichen Datenschutzmängel ein, die bei der praktischen Umsetzung der Zusammenführung von Arbeitslosen- und Sozialhilfe aufgetreten sind. Sie betreffen sowohl die Datenerhebung als auch die Leistungsberechnung. Besonders gravierend sind die unbeschränkten bundesweiten Zugriffsmöglichkeiten der sachbearbeitenden Kräfte auf alle von ALG II erfassten Daten. Wie sensibel diese Daten sein können, braucht an dieser Stelle nicht näher hervorgehoben werden. Da keine Protokollierung der Datenzugriffe erfolgt, können Missbräuche nicht erkannt und daher auch nicht aufgeklärt und abgestellt werden.

Auch in Bremen lief die Einführung des Computerprogramms „A2LL“ nicht reibungslos, in Bremerhaven kam es darüber hinaus im Vorfeld der Datenerhebung zu datenschutzrechtlichen Unzulänglichkeiten (vgl. Ziff. 9. dieses Berichts).

1.9 Steuerzahler in der informationellen Zwangsjacke

Es scheint, als handele der Gesetzgeber nach dem Motto: „Wozu brauchen wir noch die Angaben des Steuerbürgers, holen wir uns doch die Angaben lieber gleich direkt bei den Banken und anderen Stellen“. Will man sich ein Bild von der Entwicklung der steuerrechtlichen Überwachungsinstrumente machen, muss man die verschiedenen gesetzlichen Initiativen in diesem Bereich im Zusammenhang sehen. Zu nennen sind z. B. die elektronische Übertragung des Jahreseinkommens durch den Arbeitgeber an die Steuerverwaltung, die Mitteilungen der Kreditwirtschaft über die Inanspruchnahme von Freistellungsaufträgen, die Regelungen im Gesetz zur Förderung der Steuerehrlichkeit und die Einführung der Steueridentifikationsnummer wie auch verschiedene sog. Kontrollmitteilungen.

Die Steueridentifikationsnummer wird jedem Neugeborenen bereits in die Wiege gelegt. Auf die mit dieser Entwicklung verbundenen Gefahren, insbesondere eines verfassungsrechtlich unzulässigen Personenkennzeichens, hat die Konferenz der Datenschutzbeauftragten in der Entschließung „Personennummern“ hingewiesen (vgl. Ziff. 15.1 dieses Berichts).

Aber auch das Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003 (BGBl. I 2003, S. 2928) steht nach dem Auslaufen der Amnestieregelung im Blickpunkt des öffentlichen Interesses. Die Regelungen in § 93 Abs. 7 und 8 sowie in § 93 b der Abgabenordnung (AO) räumen Behörden und Gerichten weitreichende Möglichkeiten ein, sich durch automatisierten Datenabruf einen Überblick über alle Kontostammdaten einer Person zu verschaffen; sie sollen am 1. April 2005 in Kraft treten. Damit wird einer Vielzahl weiterer öffentlicher Stellen der Zugriff auf einen Datenpool ermöglicht, der nach § 24 c des Kreditwesengesetzes (KWG) im Rahmen der Terrorismusbekämpfung bisher nur den Finanzaufsichtsbehörden und den Strafverfolgungsbehörden zur Verfügung stand. Viele finden es bedenklich, wenn der Staat das gleiche System, das er zur Bekämpfung des Terrorismus eingeführt hat, für die umfassende Kontrollen aller redlichen Steuerbürger einsetzen will. Dabei gibt es bisher keine Untersuchungen darüber, ob Steuerhinterziehung, der das Gesetz entgegen treten will, wirklich ein allgemeines Phänomen ist.

Bei den in Rede stehenden Kontoinformationen handelt es sich neben den Depot- oder Kontonummern insbesondere um die Namen und Geburtsdaten der Inhaber und der Verfügungsberechtigten sowie um die Namen und Anschriften der sonst wirtschaftlich Berechtigten. Die Kontostände sind nicht Bestandteil der Abrufinformation, sie können aber unter Umständen im Rahmen weiterer Überprüfungen erhoben werden.

Damit stellt der Gesetzgeber den Finanzbehörden ein totales Überwachungsinstrument zur Verfügung. Alle Konten befinden sich im Zugriff der Finanzbehörden, das Taschengeldkonto eines Kindes ebenso wie die Konten vieler Bürgerinnen und Bürger, die nicht steuerpflichtig sind. Das Gesetz schießt damit über das Ziel weit hinaus.

Zusammengefasst wird mit der Einführung dieses umfassenden Kontrollsystems unterstellt, eine Vielzahl der Steuerpflichtigen nehme es mit der Steuerehrlichkeit nicht ernst. Ich bin mir hingegen sicher, dass die ganz überwiegende Mehrzahl der Betroffenen allein auf Grund ihres

Beschäftigungsverhältnisses oder ihrer wirtschaftlichen Situation keine Möglichkeiten hat, Steuern zu hinterziehen.

Die vorgesehenen Regelungen begegnen in mehrfacher Hinsicht datenschutzrechtlichen Bedenken. Der Abruf kann hinter dem Rücken der Betroffenen erfolgen, denn es ist nicht sichergestellt, dass die Betroffenen von einem automatisierten Abruf ihrer Daten überhaupt etwas erfahren. Nach den bis dato bekannt gewordenen Vorstellungen des Bundesfinanzministeriums sollen die Betroffenen von einer automatisierten Anfrage ihrer Daten nur dann etwas erfahren, wenn diese Abfrage zu klärungsbedürftigen Tatbeständen führt und die Betroffenen damit konfrontiert werden. Damit würde es von Zufälligkeiten abhängen, ob die Betroffenen vom Datenabruf erfahren oder nicht. Hier wird verkannt, dass jeder Datenabruf ein Eingriff in das informationelle Selbstbestimmungsrecht bedeutet. Eine solche Vorgehensweise widerspricht daher dem verfassungsrechtlichen Transparenzgebot und würde auch die Rechtsschutzgarantie des Art. 19 Abs. 4 Grundgesetz (GG) unterlaufen.

Die Finanzbehörden sollen darüber hinaus für andere Behörden - welche dies sind, wird im Gesetz nicht hinreichend genau bezeichnet - Kontoinformationen abfragen. Nach § 93 Abs. 8 AO sollen diese Behörden auf ein entsprechendes an die Finanzbehörden gerichtetes Ersuchen im Wege eines automatisierten Abrufs Kontodaten erhalten können, wenn sie ein Gesetz anwenden, das „an Begriffe des Einkommensteuergesetzes anknüpft“, und eigene Ermittlungen ihrer Versicherung nach nicht zum Ziel geführt haben oder aber keinen Erfolg versprechen.

Die Regelungen in diesem Teil des Gesetzes sind nicht normenklar. Außerdem hat es die Finanzbehörden nicht zu interessieren, mit welchen anderen Behörden jemand mit welchen Fragen im Kontakt steht. Die funktionale Trennung bei der Informationsverarbeitung wird durch diese Regelung nicht eingehalten. Angesichts der Vielzahl von Begriffen im Einkommensteuergesetz ist ein „Anknüpfen“ an solche Begriffe sehr weitreichend und nur schwer eingrenzbar. Damit bleibt für den Bürger letztlich unklar, welche Behörden unter welchen Voraussetzungen berechtigt sind, solche Ersuchen an die Finanzbehörden zu richten.

Die Datenschutzbeauftragten des Bundes und der Länder sind sich einig, dass diese Regelungen so keinen Bestand haben dürfen. Dies haben sie in ihrer EntschlieÙung „Staatliche Kontrolle muss auf den Prüfstand“ zum Ausdruck gebracht (vgl. Ziff. 15.10 dieses Berichts).

1.10 JobCard

Das Bundeswirtschaftsministerium plant die Einführung einer zentralen Speicherstelle (ZSS), in der Arbeits- und Einkommensdaten der abhängig beschäftigten Bevölkerung Deutschlands gespeichert werden sollen. Dabei handelt es sich nicht um eine Chipkartenanwendung, auf der sämtliche Daten gespeichert werden, sondern um ein DV-Verfahren unter Einsatz einer Chipkarte. Mit der Entwicklung dieser zentralen Datenbank soll eine Entlastung der Wirtschaft einhergehen, die zur Zeit entsprechende Bescheinigungen ausstellen muss, wenn staatliche oder kommunale Leistungen wie Arbeitslosengeld, Wohngeld, Kindergeld etc. beantragt werden. Wie Arbeitgeber mit nur wenigen Beschäftigten dem gerecht werden können, bleibt abzuwarten.

So sieht das Verfahren zum Beispiel vor, dass bei einer Kündigung des Arbeitsverhältnisses dem Arbeitnehmer keine Arbeitsbescheinigung in Papierform mehr ausgestellt wird, sondern die Daten in elektronischer Form an die ZSS übermittelt werden. Der Arbeitgeber wird so davon entbunden, eine Arbeitsbescheinigung auszudrucken und zu archivieren. Die Bundesagentur für Arbeit soll dann mit den elektronisch zur Verfügung gestellten Daten ohne Nachfrage bei den Betroffenen den Leistungsanspruch berechnen und einen Bewilligungsbescheid erstellen. Da die Daten der Arbeitsbescheinigungen über sieben Jahre gespeichert werden sollen und auch eine Widerspruchsfrist einzurechnen ist, muss davon ausgegangen werden, dass in der ZSS mehrere Millionen Datensätze gespeichert sein werden. Vorgesehen ist dabei, dass der Arbeitgeber grundsätzlich das Entgelt und die Beschäftigungsdauer eines jeden Arbeitnehmers zur ZSS meldet, ungeachtet dessen, ob diese Daten tatsächlich einmal für eine Leistungsberechnung benötigt werden oder nicht. Damit wäre eine Gesamtsicht über das Berufsleben der gespeicherten Personen möglich. Ist dies schon allein aus datenschutzrechtlicher Sicht bedenklich, tritt hinzu, dass es Überlegungen gibt, die Rentenversicherungsnummer zur Generierung einer Identifikationsnummer zu nutzen. Das vollständige Szenario ist damit aber bei weitem noch nicht entwickelt. Denn ist erst einmal die Infrastruktur mit dem JobCard-Verfahren geschaffen, gehen die weiteren Überlegungen dahin, die abrufberechtigten Stellen um jene Behörden und Institutionen zu erweitern, die für die Leistungsgewährung zuständig sind. Derzeit laufen bereits Modellversuche zur technischen Machbarkeit, die bis zum 30. Juni 2005 abgeschlossen sein sollen. Anschließend soll mit der bundesweiten Realisierung begonnen werden; geplant ist, das Verfahren zum 1. Januar 2007 für alle Arbeitnehmer verpflichtend einzuführen.

Ich habe prinzipielle Bedenken gegen alle DV-Verfahren, die mit einem totalen Ansatz zentral in einer Datei und nicht in verteilten Systemen die Daten verwalten. Nur wenn neben rechtlichen Sicherungen auch die technische Umsetzung Gefährdungen für das Recht auf informationelle Selbstbestimmung ausschließt, kann eine zentrale Lösung gegebenenfalls hingenommen werden. Die Konferenz der Datenschutzbeauftragten hat eine gemeinsame Arbeitsgruppe gebildet, an der auch ich mich beteilige, und diese beauftragt, das Vorhaben zu begleiten. Die in der Arbeitsgruppe vertretenen Landesbeauftragten für den Datenschutz haben eine Revision des bisherigen Konzepts gefordert mit dem Ziel, die schon bisher vorgesehene Verschlüsselung der Daten in die Hände der betroffenen Beschäftigten zu geben. Damit soll vermieden werden, dass eine Zweckentfremdung oder ein

Missbrauch der bei der ZSS gespeicherten Daten stattfinden kann. Die Konferenz der Datenschutzbeauftragten vom 28. und 29. Oktober 2004 hat den Vorschlag der Arbeitsgruppe einer Ende-zu-Ende-Verschlüsselung mit einem in den Händen des Betroffenen liegenden Schlüssels aufgegriffen und das Bundeswirtschaftsministerium gebeten, die Realisierbarkeit dieses Konzepts durch einen neutralen Gutachter überprüfen zu lassen.

1.11 Droht der genetisch gläserne Mensch?

In dem Maße, wie die Kosten für genetische Tests sinken, steigt das Interesse vieler Stellen, das menschliche Erbgut zu untersuchen und die Ergebnisse der Analyse für verschiedene Zwecke zu verwerten. An vorderster Stelle sind Forschungslabors, Pharmaindustrie, Versicherungen und Arbeitgeber zu nennen. Zurzeit sind die hoch sensiblen Informationen, die in der DNS eines jeden Menschen enthalten sind, nicht ausreichend gegen Untersuchungen geschützt, die auch heimlich durchgeführt werden können. Hierauf hat die Konferenz der Datenschutzbeauftragten bereits vor Jahren hingewiesen und in einer Entschließung in 2001 gesetzliche Regelungen über die Durchführung von genetischen Untersuchungen gefordert (vgl. 24. JB, Ziff. 15.11).

Diesen Forderungen wurde leider bis heute nicht Rechnung getragen. Erst als eine Krankenkasse im Zusammenwirken mit der Medizinischen Hochschule Hannover bei 6.000 ihrer Versicherten einen Massengentest durchführen wollte, wurden in Reaktionen darauf erneut Stimmen laut, die rasche gesetzliche Regelungen verlangten. Das Gesundheitsministerium ist unter dem Arbeitstitel „Gesetzentwurf zur Gendiagnostik“ dabei, entsprechende Regelungen vorzubereiten. Leider wurde diese unterstützenswerte Arbeit in der Öffentlichkeit bisher generell nicht genügend gewürdigt und kritisch begleitet; nur eine nicht einmal den Kernbereich tangierende Facette wurde in den Medien und an den Stammtischen diskutiert: Der (heimliche) Vaterschaftstest. Allen Zweiflern in der Frage hat dann der BGH in seinem Urteil vom 12. Januar 2005 (AZ. XII ZR 60 und 227/03) den rechten Weg gewiesen und entschieden, dass die Untersuchung des genetischen Materials eines anderen Menschen ohne dessen ausdrückliche Zustimmung gegen das Grundrecht auf informationelle Selbstbestimmung verstoße und rechtswidrig sei. Dieses Grundrecht des Kindes brauche auch nicht hinter dem Interesse des als Vater geltenden Mannes zurückzustehen, der sich Gewissheit über seine biologische Vaterschaft verschaffen möchte.

Die Abwägungen, die im Zentrum solcher diesen Bereich regelnden Normen stehen, sind nicht nur verfassungs- und datenschutzrechtlicher, sondern auch ethischer und medizinischer Natur. Es geht im Wesentlichen darum, den Betroffenen vor ungewollten und unzulässigen Ausforschungen seiner Erbinformationen zu schützen und sein Selbstbestimmungsrecht auch in diesem Bereich zu sichern. Dies beinhaltet auch, nicht zu wissen, ggf. welche problematischen Genkonstellationen man selbst hat. Nur so kann sichergestellt werden, dass erbliche Veranlagungen und kritische genetische Konstellationen nicht missbraucht werden oder zu einer Diskriminierung führen.

Gentests bei Neugeborenen und Gen-Datenbanken: Alarmiert durch die Meldungen der Presse, die EU plane Gentests für alle Neugeborenen, sah ich mich veranlasst, den Hintergründen nachzugehen. Ein solches Screening würde die reihenweise Untersuchung einer bestimmten Gruppe auf eine oder mehrere definierte Krankheiten beinhalten. Das Interesse an genetischen Untersuchungen auch bei Erwachsenen wächst. Auf die mit diesen Tendenzen verbundenen Datenschutzprobleme gehe ich im Bericht näher ein (vgl. Ziff. 8.3 dieses Berichts). Besondere Aufmerksamkeit verdient aus datenschutzrechtlicher Sicht das Vorhaben, genetische Daten zu Forschungszwecken in Datenbanken einzuspeisen.

Zusammenfassend lässt sich sagen: Das Interesse an Erbgutinformationen muss gesteuert werden, sonst droht der genetisch gläserne Mensch!

Genanalyse im Strafverfahren: Auf die Idee muss man erst einmal kommen: Den Mord an dem Prominenten Moshammer zum Anlass für eine Debatte zur Erweiterung der DNA-Analyse zu nehmen. Ja, hat man den vermeintlichen Täter denn nicht gefasst? Und hatte man ihn nicht binnen eines Tages identifiziert? Gab es Probleme mit den DNA-Analysedaten? Der Fall ist für diese Debatte völlig ungeeignet, verdeutlicht er doch vielmehr, dass die vom Gesetzgeber zur Verfügung gestellten Instrumente in der Strafprozessordnung ausreichen, um einen schnellen Fahndungserfolg sicherzustellen. Gleichwohl, der Fall Moshammer war Kumulationspunkt für eine unterschwellig seit Jahren insbesondere von Innenpolitikern auch in unserem Bundesland geführte Debatte zur Absenkung der Eingriffsvoraussetzungen und der verfahrenssichernden Maßnahmen für die personenbezogene Speicherung von DNA-Analyseergebnissen in einer Datei beim BKA.

Die Konferenz der Datenschutzbeauftragten hat sich in der Vergangenheit schon mehrfach mit Entschlüssen zum Datenschutz bei der DNA-Analyse im Strafverfahren an die Öffentlichkeit gewandt und, als habe sie es kommen gesehen, bereits im Juli 2003 (vgl. 26. JB, Ziff. 18.10) mit der Entschlüsselung „Bei der Erweiterung der DNA-Analyse Augenmaß bewahren“ die Antworten auf die jetzt entbrannte Diskussion formuliert.

Die Abschaffung des Richtervorbehalts würde die Bedeutung und Tragweite des von der Verfassung verbürgten Rechts auf informationelle Selbstbestimmung verkennen. Nur durch den Richtervorbehalt und der damit vorgeschalteten Überprüfungsentscheidung der Ermittlungsbehörden kann der Schwere des Eingriffs hinreichend Rechnung getragen werden. Die besondere Qualität des Grundrechtseingriffs schließt außerdem eine routinemäßige und undifferenzierte Anwendung des besonderen Ermittlungswerkzeuges DNA-Analyse bei Straftaten geringer Schwere aus.

Die Kritiker sollten die durch verfassungs- und obergerichtliche Entscheidungen getroffenen Festlegungen zur richterlichen Prüfpflicht nicht weiter in Frage stellen. Vielmehr sollten einige Bundesländer erst einmal die retrograde Erfassung aller nach den jetzigen Regelungen zulässigen Altfälle abschließen. Weiterhin erscheint statt einer Verbreiterung der Datenbasis wichtig, dass wenigstens europaweit ein einheitliches Testverfahren zugrunde gelegt wird, um die Vergleichbarkeit grenzüberschreitend sicherzustellen. Lediglich bei der Untersuchung anonymer Spuren und für die Durchführung von DNA-Massengentests besteht ein gesetzgeberischer Handlungsbedarf. Letzteres sage ich nicht zuletzt wegen der Erfahrungen, die ich beim in Bremerhaven durchgeführten DNA-Massentestverfahren an rund 2.200 Männern sammeln konnte (vgl. Ziff. 6.3 dieses Berichts).

1.12 Kein Lauschangriff im Kernbereich privater Lebensgestaltung

Am 3. März 2004 hat das Bundesverfassungsgericht (BVerfG) sein Urteil zum so genannten großen Lauschangriff gesprochen und die gesetzlichen Regelungen zur Wohnraumüberwachung in großen Teilen für verfassungswidrig erklärt (BVerfGE 1BvR 2378/98). Kritiker des Urteils beklagen, dass durch das Urteil das Instrument der akustischen Wohnraumüberwachung wertlos werde. Für mich hingegen stellt sich die Frage, ob nach dem Urteil des BVerfG der hohe Aufwand der Verfassungsänderung seinerzeit gerechtfertigt war.

Kernaussage in dem Urteil des BVerfG ist, dass die Anforderungen an die Rechtmäßigkeit der Wohnraumüberwachung umso strenger sein müssen, je größer das Risiko ist, dass mit ihnen Gespräche höchstpersönlichen Inhalts erfasst werden können. Führe die Überwachung unerwartet zur Erhebung von absolut geschützten Informationen, müssten die Überwachung abgebrochen und erhobene Aufzeichnungen gelöscht werden. Jegliche Verwendung solcher im Rahmen der Strafverfolgung erhobener geschützter Daten sei ausgeschlossen. Das Risiko, solche Daten zu erfassen, bestehe typischerweise beim Abhören von Gesprächen mit engsten Familienangehörigen, sonstigen engsten Vertrauten und Personen, zu denen ein besonderes Vertrauensverhältnis bestehe, wie z. B. bei Pastoren, Ärzten oder Strafverteidigern.

Die Datenschutzbeauftragten haben sich mit den Auswirkungen der Entscheidung zur akustischen Wohnraumüberwachung auseinandergesetzt und darauf aufmerksam gemacht, dass die Prinzipien der Entscheidung auch auf die Rechtslage in der Polizei und in den Nachrichtendiensten übertragen werden müssen (Entschließung vom 28./29. Oktober 2004, vgl. Ziff. 15.7 dieses Berichts). In diesem Zusammenhang bekräftigten die Datenschutzbeauftragten ihre Forderung, alle Formen der verdeckten Datenerhebung des Verfassungsschutzes, der Polizei sowie von Strafverfolgungsbehörden und anderen Sicherheitsbehörden an die Anforderungen der verfassungsgerichtlichen Entscheidung auszurichten und dazu zügig die gesetzlichen Änderungsverfahren einzuleiten.

Zur Novellierung der akustischen Wohnraumüberwachung hat die Bundesregierung den zweiten Entwurf einer Änderung der Bestimmungen der Strafprozessordnung vorgelegt. Nachdem der erste Entwurf insbesondere wegen der Einbeziehung der Berufsgeheimnisträger, wie beispielsweise Ärzte, Rechtsanwälte, Seelsorger und Journalisten, heftigen Protest hervorgerufen hat, werden diese Berufsgruppen als Instrument der akustischen Wohnraumüberwachung in der jetzigen Änderung nur dann mit erfasst, wenn sie als Teilnehmer des kriminellen Geschehens ebenfalls in Verdacht stehen. Zu den übrigen aus dem Urteil resultierenden Änderungen anderer Rechtsvorschriften stehen allerdings Gesetzgebungsvorhaben noch aus. Das gilt auch für die entsprechende Regelung im Bremischen Polizeigesetz. Hierauf habe ich den Senator für Inneres und Sport hingewiesen und ihm mitgeteilt, dass ich erwarte, dass von der Anwendung dieser Vorschrift abgesehen werde, bis eine verfassungskonforme Rechtslage hergestellt ist. Ein Vertreter des Senators für Inneres und Sport hat im Rechtsausschuss hierzu erklärt, man werde die Verfassungsrechtsprechung respektieren, man wolle aber zunächst die Gesetzgebung im Bund abwarten, bevor man die Rechtslage im Land Bremen anpasse.

1.13 Ausweise mit biometrischen Merkmalen

Welche Probleme mit der Einführung von Ausweisdokumenten mit integriertem Chip auf den biometrischen Merkmalen verbunden sind, habe ich bereits im letzten Jahr dargelegt (vgl. 26. JB, Ziff. 1.19). Nachrichten wie "Ausweise mit digitalen Merkmalen kosten über 600 Millionen Euro im Jahr" oder den Berechnungen des Büros für Technikfolgenabschätzung des Bundestages, das bis zu 300 Euro pro Pass annimmt, haben Bundesinnenminister Schily nicht davon abbringen können, die ersten Pässe dieser Art bereits im Herbst 2005 einführen zu wollen. Dabei sollen die Betriebskosten für Hard- und Software in den Meldestellen ein bestimmender Faktor sein, der die Kosten in die Höhe treibt.

Das Europäische Parlament hat Anfang Dezember 2004 in seiner Stellungnahme zur geplanten EU-Pass-Verordnung deutliche Verbesserungen zur Sicherung des Persönlichkeitsrechts gefordert. Mit der Pass-Verordnung sollen neben einheitlichen Sichtmerkmalen auch biometrische Merkmale in die Pässe und andere Reisedokumente der EU-Bürger eingeführt werden. Das Parlament lehnte die Speicherung der Passdaten aller EU-Bürger in einer zentralen Datei ab. Eine derartige Datenbank würde unverhältnismäßig sein und das Risiko des Missbrauchs und der Zweckentfremdung der sensiblen Daten erhöhen. Ebenfalls wurde durch das Europäische Parlament eine verpflichtende Aufnahme eines zweiten biometrischen Merkmals neben der Gesichtserkennung in die Ausweispapiere abgelehnt. Schließlich hat das EU-Parlament gefordert, die Behörden und sonstigen Stellen, die Zugang zu den in den Ausweispapieren auf einem integrierten Chip gespeicherten Daten haben sollen, in ein Register aufzunehmen, damit die notwendige Transparenz erreicht und Missbrauch weitestgehend vermieden wird. Damit werden viele Forderungen der Datenschutzbeauftragten aufgegriffen. Der Bundesbeauftragte für den Datenschutz hat in 2004 in einem Schreiben an den Vorsitzenden des EU-Rates auf Berichte aufmerksam gemacht, in denen darauf hingewiesen wird, dass bei Tests der biometrischen Verfahren diese die angestrebte Sicherheit nicht garantiert hätten. Die Zahl der Fälle, in denen das System Berechtigte zu Unrecht zurückgewiesen habe, sei ausgesprochen hoch gewesen.

1.14 Gläserner Kunde – Befürchtung oder Realität

Nicht nur im öffentlichen Sektor, sondern auch in der Privatwirtschaft geht der Trend zu immer umfangreicheren Datensammlungen und Datenverbundsystemen. Hierzu zählen Data-Mining-Systeme (zur Kritik an den Data-Mining-Systemen im Internet vgl. 23. JB, Ziff. 1.2 und CD „25 Jahre Datenschutz in Bremen“, Ziff. 4.1.3) ebenso wie das immer dichter werdende Netz verschiedener Warndateien. Neben zahlreichen Kreditauskunftssystemen entwickelt jetzt die Wohnungswirtschaft eigene Warndateien oder integriert diese in vorhandene Auskunftssysteme (vgl. Ziff. 14.8.1 dieses Berichts), aber auch die Versicherungswirtschaft verfügt über zentrale Warn- und Hinweissysteme. Anzuerkennen ist das legitime Interesse der Wirtschaft, sich vor Betrügern, schwarzen Schafen und zahlungsunfähigen oder -unwilligen Kunden zu schützen. Die einzelnen Auskunftssysteme sind in der Regel datenschutzrechtlich nicht zu beanstanden, gleichwohl müssen bei der Ausgestaltung dieser Systeme auch die schutzwürdigen Belange der Betroffenen in hinreichendem Maße Berücksichtigung finden. Gefahren entstehen dort, wo verschiedene Systeme vernetzt werden oder durch die Recherche über verschiedene Bereiche den einzelnen Kunden in seinen vielfältigen wirtschaftlichen Beziehungen durchleuchten. Es darf nicht dazu kommen, dass zum Beispiel ein junger Mensch, der mit 18 Jahren seine Handy-Rechnung nicht bezahlen konnte, anschließend kein Konto mehr eröffnen kann, keine Wohnung findet oder keine Versicherung mehr abschließen kann.

Auch die rasant zunehmende Einführung der RFID-Chip-Technologie gibt Anlass zur Besorgnis. Warenhersteller und Handel setzen zunehmend weltweit Radio-frequenz-gestützte Mikrochips (RFID-tags) zur Kennzeichnung von Warenbeständen wie auch zur Preisauszeichnung ein (Näheres vgl. 26. JB, Ziff. 1.25 „Mikrochips zum Aufbügeln“). Diese funkenden Mikrochips werden voraussichtlich in Kürze zu unserer täglichen Umgebung gehören. Ihre möglichen Auswirkungen auf die Privatsphäre sind weitreichend. Die Gefahr besteht, dass sie ein umfassendes Konsum-, Nutzungs-, Verhaltens- und Bewegungsprofil ermöglichen. Ich habe es daher für nötig gehalten, mich im Berichtsjahr umfassend über die technische Funktionsweise und die Gestaltungsmöglichkeiten zu informieren. Die wesentlichen Ergebnisse sind im Arbeitskreis „Technik“ der Datenschutzbeauftragten des Bundes und der Länder zusammengetragen worden, ich werde sie in Kürze auf meiner Homepage veröffentlichen.

1.15 Zur Entwicklung in der Telekommunikation

Der Bundesbeauftragte für den Datenschutz (BfD) berichtet, dass die Zahl der Telefonüberwachungen wiederum weiter deutlich angestiegen ist. So haben die Telekommunikationsunternehmen der Regulierungsbehörde für Telekommunikation und Post für das Jahr 2002 21.874 Anordnungen gemeldet. Die anschließende Zahl für das Jahr 2003 beträgt 24.441 Anordnungen (vgl. Graphik Ziff. 16.4 dieses Berichts). Der BfD berichtet, dass die Zahl der Anordnungen von Jahr zu Jahr steige und sich seit 1995 fast verfünffacht habe. Eine nachvollziehbare, befriedigende Erklärung hierfür gebe es nach wie vor nicht. Auch der Präsident des Bundesverfassungsgerichts äußerte sich im April 2004 zu dieser Entwicklung kritisch. Vor dem Hintergrund der internationalen Terrorgefahr warne er "dringend davor, das durchaus legitime Sicherheitsbedürfnis der Bevölkerung zu nutzen, um Freiheitsrechte gewissermaßen schon einmal vorsorglich und über das Maß der Verhältnismäßigkeit hinaus einzuschränken". Die Zahl der Telefonüberwachungen in Deutschland sei hoch und das Grundrecht des Fernmeldegeheimnisses werde „bereits in erheblichem Maße eingeschränkt“.

Aber auch mit der Forderung nach einer im Bremischen Polizeigesetz geregelten präventiven Telefonüberwachung musste ich mich auseinandersetzen. Bislang ist das Abhören nur für Zwecke der Strafverfolgung zulässig, und zwar nur unter der Voraussetzung, dass eine Straftat von besonderem Gewicht vorliegt, besondere Tatsachen einen Verdacht begründen und ein Richter die Maßnahme angeordnet hat. Im Innenressort gibt es jedoch Überlegungen, Abhörmaßnahmen künftig auch für präventive Zwecke zuzulassen.

Zu bedenken ist, dass es im präventiven Bereich noch keine Beschuldigten gibt. Auch gibt es keine Gewissheit, dass bestimmte Straftaten tatsächlich begangen werden, wenn die Polizei sie nicht verhindert. In diesem unsicheren Raum würde durch eine solche Regelung die Überwachung der Bürger zulässig. Die präventive Telekommunikationsüberwachung als rein polizeiliches Mittel zur Gefahrenabwehr einzuführen, kann hinsichtlich der Anwendungsfälle problematisch sein. Gleichwohl gibt es in einigen Ländern bereits eine solche Regelung. Gegen die niedersächsische Regelung wurde eine Verfassungsbeschwerde beim Bundesverfassungsgericht erhoben. Die Konferenz der Datenschutzbeauftragten, die diesem Instrument kritisch gegenüber eingestellt ist, hat daher den Landesgesetzgebern empfohlen, vor der Schaffung neuer Bestimmungen in den Polizeigesetzen der Länder die voraussichtlich richtungsweisende Entscheidung des Bundesverfassungsgerichts abzuwarten.

Eine umfassende Vorratsspeicherung von Telekommunikationsdaten, wie sie im EU-Ministerrat beraten wird (vgl. Rats-Dok. 8958/04), wird von den Datenschutzbeauftragten des Bundes und der Länder kategorisch abgelehnt. Die Speicherung und Auswertung von ausgesuchten Internetadressen verrät etwas über die Interessen, Vorlieben und politischen Präferenzen der Nutzer. Damit verbunden wäre zugleich eine Verletzung der Grundrechte auf freie Meinungsäußerung und auf ungehinderte Unterrichtung aus allgemein zugänglichen Quellen. Das novellierte TKG enthält denn auch zum Glück eine solche Regelung nicht. Der Deutsche Bundestag hat seine mit diesen Regelungen zum Ausdruck kommende Ablehnung Anfang 2005 noch einmal bekräftigt (BT-Drs. 15/4597).

Leider enthält das im Berichtsjahr novellierte TKG (BGBl. I S. 1190) auch einige datenschutzrechtliche Verschlechterungen. So ist die Möglichkeit des anonymen Telefonierens mittels Prepaid-Cards (Entschließung der Konferenz „Geplanter genetischer Identifikationszwang in der Telekommunikation“, vgl. 25. JB, Ziff. 15.5) nicht mehr möglich, weil man sich beim Kauf einer solchen Karte nunmehr ausweisen muss. Ebenso wurde die Inverssuche grundsätzlich zugelassen. Wer mit dieser nicht einverstanden ist, muss aktiv werden und widersprechen (Näheres vgl. Ziff. 2.1 dieses Berichts).

1.16 Bürgeranfragen

Auch im Jahr 2004 erhielt ich zahlreiche Eingaben per Post oder E-Mail sowie durch Anrufe von Bürgern, Unternehmen und Behörden, die mich um die Klärung ihrer datenschutzrechtlichen Probleme baten. Dabei betrafen die Anfragen die unterschiedlichsten Bereiche der Datenverarbeitung. Am häufigsten ging es um Fragen des Arbeitnehmerdatenschutzes, der Datenverarbeitung der Auskunfteien, der Übermittlung personenbezogener Daten ins Ausland, der Videoüberwachung und der Tätigkeit behördlicher bzw. betrieblicher Datenschutzbeauftragter.

Etwa zwei Drittel der telefonischen Anfragen betrafen die Datenverarbeitung im nicht öffentlichen Bereich. Um die Vielfalt der Anfragen, die ich telefonisch erledigen konnte, zu dokumentieren, habe ich auszugsweise einige dieser Themen aus 2004 in einer Tabelle zusammengestellt (vgl. Anlage Ziff. 16.4 dieses Berichts).

Immer wieder möchten Bürger ihre Anliegen auch persönlich vortragen. Dies können sie nicht nur in meiner Dienststelle in Bremerhaven, sondern donnerstags in der Zeit von 15.00 Uhr bis 18.00 Uhr auch in Bremen, wo ich eine Bürgersprechstunde anbiete.

1.17 Öffentlichkeitsarbeit und Presseresonanz

Im vergangenen Berichtszeitraum habe ich zu diversen datenschutzrechtlichen Themen Pressemitteilungen herausgegeben, um insbesondere die Bremer Bürgerinnen und Bürger auf neue Entwicklungen im Datenschutz aufmerksam zu machen. Die Pressemitteilungen sind jeweils aktuell auf meiner Homepage www.datenschutz.bremen.de unter „Pressemitteilungen“ abrufbar. Darüber hinaus bin ich Anfragen der Medien nachgekommen und habe mich im Rahmen von Interviews und Stellungnahmen zu datenschutzrechtlichen Fragestellungen geäußert. Ein Überblick über die in der Presse behandelten Datenschutzthemen ist im Anhang (vgl. Pressespiegel Ziff. 16.1 dieses Berichts) zu finden.

Auf meiner Homepage veröffentliche ich neben den Pressemitteilungen weitere aktuelle Informationen zum Datenschutz unter „Aktuelles“ und „Tipps für Bürger“, die eine gute Resonanz finden.

1.18 Fortbildungsbeiträge vom LfD

Auch im letzten Berichtsjahr haben die in meiner Dienststelle Beschäftigten eine Vielzahl von Seminaren und Schulungen durchgeführt. Einige interessante Veranstaltungen führe ich nachfolgend auf:

- Fortbildung für den Führungskräftepool beim Senator für Finanzen im Aus- und Fortbildungszentrum Bremen,
- Referat „Data Mining/Data Warehouse: Elektronische Profile oder Datenschutz“ auf dem Workshop „Wissen ist was wert, Wissen ist flüchtig“ der Vereinten Dienstleistungsgewerkschaft ver.di e. V. in Bremen,
- Referat zum Mammographie-Screening im „Multidisziplinären Kurs“ am Klinikum Bremen-Mitte,
- Seminar zum Arbeitnehmerdatenschutz bei der Arbeitnehmerkammer Bremen,
- Seminar „Datenschutz im Personalwesen“ beim Aus- und Fortbildungszentrum Bremen,
- Vorlesungen über juristische Grundlagen in Datenschutz und Datensicherheit an der Hochschule Bremerhaven,
- Vortrag in Garlstedt vor behördlichen Datenschutzbeauftragten der Bundeswehr (auf Anfrage des BfD),
- Seminar für behördliche Datenschutzbeauftragte beim Aus- und Fortbildungszentrum Bremen,
- Vortrag „WLAN aus Sicht des Datenschutzes“ beim Senator für Finanzen,
- Mehrere Seminare „Sicherheit im Internet“ bei der Wirtschafts- und Sozialakademie der Arbeitnehmerkammer Bremen,
- Vortrag „eGovernment bei den Sicherheitsbehörden“ als Kooperationsveranstaltung des Senators für Finanzen und der Firma SEL,
- Seminar „Einführung in das Datenschutzrecht“ beim Aus- und Fortbildungszentrum Bremen.

1.19 Zur Situation der Dienststelle

Rückblickend muss ich feststellen: Es ist schon erstaunlich, wie schnell man sich an Gutes gewöhnen kann. Zur Erinnerung: Noch vor fünf Jahren verfügte die Dienststelle nur über Einzelplatz-PCs. Im Jahre 2000 konnte ich erreichen, dass ein Hausnetz in Betrieb ging, und erst vor drei Jahren waren alle Arbeitsplätze mit einem Internetanschluss ausgestattet. In 2003 wurde dann im Hause ein Dokumentenmanagementsystem eingeführt, das bisher voll und ganz die Erwartungen an eine Effektivierung der Bürokommunikation und Archivierung erfüllt hat. Die Administration des Hausnetzes wird intern durchgeführt. Im Berichtsjahr mussten der E-Mail-Server ersetzt und die technischen Vorbereitungen zur Einführung der elektronischen Arbeitszeiterfassung getroffen werden, die über ein zentrales Verfahren in Bremen abgewickelt wird.

Eine besondere Herausforderung war die Fertigstellung des Projekts "datenschutz4school" und die Durchführung des Workshops der Datenschutzaufsichtsbehörden (vgl. Ziff. 14.10 dieses Berichts), der mit freundlicher Unterstützung des Präsidenten der Bremischen Bürgerschaft in seinem Hause stattfinden konnte. Hierfür wie auch für andere offensichtlich gern gegebene Hilfestellungen aus seinem Hause sei an dieser Stelle gedankt.

Es ist nicht immer leicht, die vielen neuen technischen Entwicklungen datenschutzrechtlich zu bewerten. Hinzu kommen viele andere Anforderungen an meine Dienststelle, vielleicht vermitteln die Punkte „Durchgeführte Fortbildungsveranstaltungen“ (vgl. Ziff. 1.18 dieses Berichts) und „Telefonische Anfragen“ (vgl. Ziff. 1.16 und Ziff. 16.2 dieses Berichts) neben den inhaltlichen Darstellungen der einzelnen Punkte eine gewisse Vorstellung von der Bandbreite der Fragestellungen und dem Arbeitseinsatz, der von allen Beschäftigten meiner Dienststelle erbracht werden muss, um den vielfältigen Anforderungen gerecht zu werden. Die Beschäftigten haben daher mit Genugtuung die Anerkennung, die im Rahmen der Parlamentsdebatte über den Bericht und Antrag des Rechtsausschusses zum 25. Jahresbericht in der Bremischen Bürgerschaft ausgesprochen wurde, zur Kenntnis genommen.

1.20 Kooperationen

Das Bremische Datenschutzgesetz beschreibt in § 27 Abs. 4 BremDSG die Zusammenarbeit mit anderen Datenschutzkontrollenrichtungen. Die Zusammenarbeit mit den Datenschutzbeauftragten des Bundes und der Länder wie auch mit den Datenschutzaufsichtsbehörden, zuständig für den nicht öffentlichen Bereich, ist unabdingbare Voraussetzung, um den tatsächlichen, vielfältigen Herausforderungen einigermaßen gerecht zu werden. Die Entscheidungsschwerpunkte liegen dabei in der Konferenz der Datenschutzbeauftragten und im Düsseldorfer Kreis, allerdings wäre eine Entscheidungsfindung ohne eine effektive Unterstützung aus den Arbeitskreisen nicht möglich. Wesentliche Ergebnisse der Zusammenarbeit in der Konferenz der Datenschutzbeauftragten spiegeln sich in den Entschlüssen der Konferenz wieder, die jeweils im Anhang meines Berichts zu finden sind (vgl. Ziff. 15 dieses Berichts).

Nicht unerwähnt bleiben soll an dieser Stelle auch die gute Kooperation mit der landeseigenen "datenschutz nord GmbH", mit der ich einen regelmäßigen Gedankenaustausch pflege und mit der ich auch im vergangenen Jahr wieder gemeinsam einige Projekte durchgeführt habe. Ebenso hervorzuheben ist die gute Zusammenarbeit mit dem Erfa-Kreis der betrieblichen Beauftragten für den Datenschutz der Region, an dessen Sitzungen ich regelmäßig teilnehme. Umgekehrt haben Mitglieder des Erfa-Kreises mich bei Lehrveranstaltungen und beim Workshop der Datenschutzaufsichtsbehörden unterstützt und diese durch ihre praktischen Erfahrungen belebt.