BREMISCHE BÜRGERSCHAFT
Landtag
13. Wahlperiode

Drucksache 13/520
31. 03. 93

69 Seiten

Fünfzehnter Jahresbericht des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats meinen 15. Bericht über das Ergebnis meiner Tätigkeit im Jahre 1992 zum 31. März 1993 (§ 33 Abs. 1 Bremisches Datenschutzgesetz – BrDSG).

Dr. Stefan Walz, Landesbeauftragter für den Datenschutz

Inhaltsübersicht Seite

1. Vorwort

1.1 Zur Situation des Datenschutzes

Das Jahr 1993 begann für den Datenschutz mit einem ebenso bedauerlichen wie für die gegenwärtige Situation kennzeichnenden Ereignis. Die von den Datenschutzbeauftragten nachdrücklich unterstützte Initiative, im Rahmen der Reform des Grundgesetzes ein ausdrückliches **Grundrecht auf Datenschutz** zu schaffen, ist im Februar 1993 in der Gemeinsamen Verfassungskommission von Bundestag und Bundesrat gescheitert (s. a. Ziffer 16.3). Eine Korrektur dieser Entscheidung durch die beiden gesetzgebenden Gremien ist zu erhoffen, aber wenig wahrscheinlich. Dabei sollten sich in der gesamtdeutschen Verfassung Meinungsbildungsprozesse gerade aus den neuen Bundesländern wiederfinden. Dort haben die Erfahrungen der Bevölkerung mit den Möglichkeiten totaler Kontrolle und ihr Bestreben, staatlicher Überwachung klare rechtsstaatliche Grenzen zu ziehen, in mehreren Länderverfassungen zu der Aufnahme eines Datenschutz-Grundrechts geführt. Der Trend geht in die entgegengesetzte Richtung: Für viele ist es jetzt an der Zeit, Grundrechte als angeblich liberales Luxusgut der stabilen, inzwischen aber unwiederbringlich vergangenen Nachkriegsepoche in Frage zu stellen.

Aktuellstes Beispiel dafür ist der sogenannte **„große Lauschangriff"**, d. h. die optische und elektronische Überwachung in der Privatwohnung, mit dessen Zulassung die Grundrechte sowohl auf informationelle Selbstbestimmung als auch auf Unverletzlichkeit der Wohnung im Kern getroffen würden (s. a. Ziffer 16.4). Als zentrales Losungswort — vielfach gleichzeitig auch als alleinige Begründung — dient dabei die „Organisierte Kriminalität", deren Bekämpfung im Zweifel Vorrang haben soll vor den Freiheitsrechten der Bürger. Niemand wird und darf die Ängste um die persönliche Sicherheit, aber auch um die Integrität der gesellschaftlichen und politischen Institutionen, die durch die organisierte Kriminalität ausgelöst werden, verharmlosen. Doch ist es Aufgabe der Datenschutzbeauftragten, darauf zu achten, daß die Grenze zwischen dem Eingriffsinstrumentarium des Staates und dem Grundrechtsschutz des einzelnen nicht immer weiter zu Lasten des Individiums verschoben wird. Der jetzt geforderte „große Lauschangriff" ist nur ein Glied in einer langen Kette von Befugnissen, die den Sicherheitsbehörden in den letzten beiden Jahren eingeräumt wurden. Sie reichen von den Abhörmöglichkeiten zur Bekämpfung des illegalen Waffenexports über die Rasterfahndung bis hin zum Einsatz verdeckter Ermittler. Die erweiterten Handlungsmöglichkeiten werden verlangt, bevor eine Evaluation der vorhandenen — in den Länderpolizeigesetzen z. T. bereits seit längerem vorgesehenen — Instrumente überhaupt stattgefunden hat. Alternative Aktionsmittel, vor allem die nachhaltige Kontrolle und ggf. Unterbindung kriminell induzierter Geldflüsse, werden nur zögerlich behandelt; das sogenannte Gewinnaufspürungsgesetz ist bis heute nicht in Kraft. Zu wenig wurde bisher auch dafür getan, die Datenverarbeitung in den zentralen Polizeibehörden, deren Kapazität zur Bekämpfung des Terrorismus stark erweitert wurde, auf die neuen Tätertypen des organisierten Verbrechens einzustellen.

Kernpunkte der Kritik an dem im vergangenen Jahr verabschiedeten **Gesetz zur Bekämpfung der organisierten Kriminalität** (OK) bleiben die Unbestimmtheit der Eingriffsvoraussetzungen sowie das Fehlen klarer Tatbestandskataloge. Es fehlt die Gewähr dafür, daß das neue Recht auf die Strafverfolgung bei schweren OK-Delikten beschränkt bleibt. Die aus diesen Gründen erfolgte Ablehnung des Gesetzes im Bundesrat durch den Bremer Senat habe ich begrüßt und hoffe, daß er die gleiche Haltung zu den anstehenden Vorschlägen zur elektronischen Überwachung von Privatwohnungen einnehmen wird.

Doch wäre es verfehlt, für den Stand und die Risiken der „Verdatung" des Bürgers allein den Sicherheitsbereich zum Maßstab zu nehmen. Auch im **Sozialleistungsbereich** — um ein anderes Beispiel zu nennen — wird das Kontrollnetz engmaschiger. Sicherlich ist der Hinweis auf die notwendige Kontrolle des Leistungsbezugs angesichts knapper öffentlicher Haushalte legitim, auch um Verteilungsgerechtigkeit zu sichern. Andererseits läßt sich immer wieder feststellen, daß die Bekämpfung angeblicher oder wirklicher **Leistungsmißbräuche** zu sensiblen Spezialdateien und Datenabgleichen führt, deren Eingriffsintensität außer Verhältnis zum angestrebten Überprüfungszweck steht. Arme, Ausländer sowie andere Minderheiten und Randgruppen sind derzeit von dieser Entwicklung in besonderem Maße betroffen. Den Datenschutzbeauftragten obliegt es, das zunehmend bedrohte Sozialgeheimnis, Eckpfeiler rechtsstaatlicher Sozialverwaltung, sichern zu helfen. In Arztpraxis, Krankenhaus und Krankenkasse heißen die Maximen Effektivitätskontrolle und Rationalisierung, unter denen die automatisierte Verar-

beitung von Patientendaten vorangetrieben wird. Die Krankenversicherungskarte als maschinenlesbare **Chipkarte** eröffnet eine neue Dimension des Zugriffs auf sensible medizinische Angaben.

Keine Trendumkehr gibt es im Verhältnis zwischen der **Technikentwicklung** und einem Datenschutzrecht, das seine Steuerungsfunktion zunehmend einbüßt. Angesichts einer dezentralen IuK-Landschaft, der zunehmenden Nutzung und Vernetzung von Arbeitsplatzcomputern sowie der raschen Ausbreitung des Mobilfunks droht bereits die klassische Forderung nach der „Ordnungsmäßigkeit", also nach präzise programmierter, aussagefähig dokumentierter und überprüfbar protokollierter Datenverarbeitung zur Illusion zu werden. Um so mehr kommt es auch in diesem Bundesland darauf an, die Gesamtplanung des Einsatzes von Informations- und Kommunikationstechnologie anhand klarer Ziele, mit präzisen Konzepten und entscheidungsbefugten Lenkungsgremien durchzuführen, wobei Datenschutz und Datensicherung jeweils integrale Bestandteile sein müssen (s. Ziffer 2.2). Die beträchtliche Nachfragemacht der öffentlichen Hand muß genutzt werden, gegenüber den Herstellern, ggf. auch gegen deren Verkaufsinteressen, Datenschutzstandards durchzusetzen, wie dies in Bremen ansatzweise etwa bei der Beschaffung von ISDN-fähigen Telefonanlagen geschieht.

Die Datenschutzentwicklung **auf europäischer Ebene** ist gekennzeichnet durch die Diskussion über den Richtlinien-Entwurf der EG-Kommission. Wer nicht nur ein Europa der Händler, sondern auch ein Europa der Bürger und der Bürgerrechte will, muß sich für einen EG-weiten Schutz des informationellen Selbstbestimmungsrechts auf hohem Niveau einsetzen. Nur so kann ein Gegengewicht geschaffen werden gegen die Risiken der rapide zunehmenden Internationalisierung der Datenverarbeitung und der Datenflüsse, die mit der Vollendung des Binnenmarktes noch zunehmen werden. Polizeidienststellen, Zollbehörden, aber auch Banken und Versicherungen mit Auslandsfilialen sind auf wachsenden grenzüberschreitenden Datenaustausch angewiesen. Die europäische Harmonisierung der Schutzbestimmungen hat auch zur Konsequenz, daß sich die Regelungsebenen EG, Bund und Land zunehmend verzahnen. Anders ausgedrückt: Datenschutzregelungen können zunehmend weniger isoliert im Landes- bzw. nationalen Kontext diskutiert und erarbeitet werden. Ein gutes Beispiel dafür ist die EG-Richtlinie zum Einsichtsrecht in Umweltakten, die von Bund und Ländern — jeweils im Bereich ihrer Gesetzgebungszuständigkeit — umgesetzt werden muß.

1.2 Schwerpunkte, Gliederung und Redaktion des Berichts

Dieser 15. Jahresbericht ist der erste, den ich nach meiner Amtsübernahme am 01. Juni 1992 auch inhaltlich voll verantworte. An seiner Abfassung waren alle Referate der Dienststelle beteiligt. Der Aufbau enthält gegenüber den Vorgängern einige neue Elemente. Vorangestellt sind drei Abschnitte, die **Schwerpunkte** der Tätigkeit meiner Dienststelle wiedergeben. Im Kapitel 2.1 möchte ich — u. a. an Hand einiger statistischer Zahlen — deutlich machen, daß die Beratung der Bürgerinnen und Bürger, die Bearbeitung ihrer Anfragen, Eingaben und Beschwerden, kurz: die **„Ombudsmann-Funktion"** des Datenschutzbeauftragten im Vordergrund steht. Wer Bürgerrechte in der „Informationsgesellschaft" sichern will, kann dies nur mit der aktiven Mitwirkung der Betroffenen leisten; deren kritische Wachsamkeit gegenüber dem „Datenhunger" von Verwaltung und Wirtschaft ist unverzichtbare Hilfe für den Landesbeauftragten. Nur die Bearbeitung eines breiten Spektrums von Einzelfällen vermag sicherzustellen, daß die Tätigkeit meiner Dienststelle nicht zur reinen Regelungsberatung für die senatorischen Behörden degeneriert. Die wenigen wichtigen Einzelfälle, die aus Raumgründen im Bericht dokumentiert werden können, sind jeweils der besseren Anschaulichkeit halber in der Überschrift ausdrücklich markiert („Fall:").

Das zweite Schwerpunktkapitel (s. u. Ziffer 2.2) zur **Entwicklung der Informations- und Kommunikationstechnik** greift als das zur Zeit wohl aktuellste Thema die Datenschutzrisiken im **Mobilfunk**, einem rasant wachsenden Segment der Kommunikationstechnik, auf. Der andere Unterabschnitt gilt der **Situation im Land Bremen;** aus ihm wird deutlich, daß die Entscheidungen über die künftige Rolle des ADV-Ausschusses, über Rolle und Rechtsstellung des Rechenzentrums der bremischen Verwaltung sowie des Fernmeldetechnischen Amtes sowie über ein Gesamtprogramm der PC-Vernetzung möglichst bald fallen müssen, wenn einerseits eine optimale, funktionsgerechte DV-Unterstützung der bremischen Verwaltung erreicht und andererseits eine Verschwendung knapper Ressourcen verhindert werden sollen. Der Beitrag zeigt auch, wie notwendig es war, die „Technikkompetenz" meiner Dienststelle zu erweitern, was mit der Besetzung der

längere Zeit vakanten Informatiker-Stelle zum 01. November 1992 möglich wurde. Zusätzlich nutze ich u. a. die vielfältigen Kooperationsmöglichkeiten mit Informatikspezialisten der Universität Bremen.

Die eminente Bedeutung der im dritten Kapitel (Ziffer 2.3) behandelten **europäischen Datenschutzentwicklung** wurde bereits oben dargelegt (vgl. Ziffer 1.1). Als Vertreter der Landesbeauftragten in der deutschen Delegation bei der EG-Datenschutzkonferenz beteilige ich mich persönlich an dem mühsamen Versuch, einen gemeinsamen Standpunkt der unabhängigen Kontrollbehörden zu den Vorschlägen der EG-Kommission zu erarbeiten und gegenüber den EG-Gremien wie auch den nationalen Regierungen zu vertreten.

Nach den Schwerpunktkapiteln folgt die Gliederung dem bisherigen Schema, d. h. insbesondere der Zuordnung der Berichtsabschnitte zu senatorischen Behörden. Insoweit dadurch thematisch eigentlich zusammengehörende Komplexe getrennt werden, wird dies in Kauf genommen, um die betroffenen Ansprechpartner leichter erkennen zu können und damit auch die Beratungen im Datenschutzausschuß zu erleichtern.

1.3 Ausblick auf 1993

Im Vordergrund der bremischen Rechtsentwicklung wird 1993 die **Novellierung des Landesdatenschutzgesetzes** stehen. Der Justizsenator will dafür bis zur Sommerpause einen Entwurf vorlegen. Kernpunkte sind dabei die Verbesserung der Betroffenenrechte durch Einführung eines Schadensersatzanspruches und die Stärkung der Rechtsstellung des Landesbeauftragten für den Datenschutz. Die Forderung nach bereichsspezifischen Rechtsvorschriften ergänzend zum Bremischen Datenschutzgesetz werde ich auf diejenigen Materien beschränken, in denen dies nach den Vorgaben des Volkszählungsurteils des Bundesverfassungsgerichts wegen der besonderen Eingriffsintensität notwendig ist.

Wichtiges Beispiel dafür ist der **öffentliche Gesundheitsdienst.** Eckpunkte für ein Gesetz, das Aufgaben und Befugnisse der Gesundheitsämter zeitgemäß, d. h. im Hinblick auf ihr geändertes Funktionsspektrum, regeln soll, liegen seit kurzem vor. Entscheidend wird sein, daß die Aufgabentrennung — etwa zwischen Amtsarzt und Beratungstätigkeit — einer strikten Zweckbindung bei der Nutzung der Klientendaten entspricht.

Die beabsichtigte Neufassung des **Verfassungsschutzgesetzes** bietet Gelegenheit für eine Neudefinition der Aufgaben des Landesamtes angesichts der veränderten Welt- und Sicherheitslage und damit auch seiner Befugnisse zu nachrichtendienstlicher Datenspeicherung und -nutzung. Aktueller Kontext wird dabei vor allem der Rechtsextremismus und seine Bekämpfung sein. Doch gilt es der auch in Bremen vorhandenen Versuchung zu widerstehen, das Verfahren der Überprüfung von Einstellungsbewerbern mit Hilfe des Verfassungsschutzes entsprechend dem verhängnisvollen „Radikalenerlaß" von 1972 wieder zu beleben. Der Bericht enthält eine Reihe weiterer Beispiele für Regelungsanforderungen an den Landesgesetzgeber, etwa für die **Sicherheitsüberprüfung** und das **Einsichtsrecht in Umweltakten.**

Im **nicht-öffentlichen Bereich** habe ich es mir zur Aufgabe gestellt, Beratung und Kontrolle — insbesondere bei den Unternehmen im Dienstleistungsbereich — zu verstärken. Das seit dem 01. 06. 1991 geltende Bundesdatenschutzgesetz bietet immer noch eine Reihe von ungelösten Zweifels- und Auslegungsfragen. Hinzu kommt, daß die Umstellung von Großrechnersystemen auf PC-Netze auch in privaten Unternehmen rapide zunimmt, ohne daß die daraus resultierenden neuen Anforderungen an die Datensicherung ausreichend bewältigt werden. Überhaupt wäre es verfehlt, die datenschutzrechtliche Begleitung der DV-Entwicklung in der Privatwirtschaft gegenüber der in der öffentlichen Verwaltung zu vernachlässigen. Die Information über den nicht-öffentlichen Bereich im Jahresbericht ist daher — auch wenn einzelne Firmen und Verbände daran Kritik üben — unverzichtbar.

Jeder Datenschutzbeauftragte ist auf ein gutes Verhältnis zum Parlament angewiesen. Die Vorstellung und die Diskussion meiner Tätigkeit im **Datenschutzausschuß** der Bürgerschaft ist von großer Bedeutung. Bei der Beratung des 14. Jahresberichts konnten in einer Reihe von Punkten Fortschritte erreicht werden; z. T. wird in diesem Bericht auf die erzielten Ergebnisse eingegangen. Darüber hinaus ist mir daran gelegen, im kommenden Jahr mehr als bisher im Einzelfall meinen

Standpunkt zu Regelungsvorhaben und Automationsprojekten in den **Fachdeputationen** darlegen zu können. In diesem Anliegen werde ich vom Datenschutzausschuß unterstützt.

2. Schwerpunkte

2.1 Eingaben und Bürgerkontakte

Im Jahr 1992 erhielt ich insgesamt 99 schriftliche Eingaben und Beschwerden. Davon betrafen 30 den **nicht-öffentlichen Bereich.** Die Mehrzahl davon richtete sich gegen Versicherungsgesellschaften, Banken, Auskunfteien und Ärzte. Allein in zehn Schreiben beklagten sich die Petenten über die aus ihrer Sicht unzulässige Weitergabe ihrer Daten.

Von den 69 die **öffentliche Verwaltung** betreffenden Eingaben und Beschwerden bezogen sich 42 auf Dienststellen des Senats, 16 auf Ämter des Magistrats Bremerhaven sowie 11 auf sonstige Stellen. Was den Senat angeht, waren insbesondere die Ressorts Inneres und Sport, Justiz und Verfassung sowie der Bereich Jugend und Soziales angesprochen. Auch im öffentlichen Bereich stand die Kritik an wirklich und vermeintlich unerlaubten Datenübermittlungen im Vordergrund.

Zu den schriftlichen Vorgängen kam eine nicht im einzelnen festgehaltene große Zahl telefonischer Anfragen, Hinweise oder Beratungsersuchen hinzu. Zahlreiche Eingeber haben direkt meine Dienststelle aufgesucht und mündlich ihr Anliegen vorgetragen. Einfachere Rechtsfragen und Informationswünsche konnten umgehend beantwortet werden. Die meisten Fälle, in denen Bürgerinnen und Bürger den Landesbeauftragten eingeschaltet haben, konnten allerdings erst nach weitergehender Sachaufklärung oder örtlicher Prüfung bei der betroffenen speichernden Stelle erledigt werden.

Eine behördliche Verfahrensweise, die immer wieder Bürger verärgert, greife ich heraus. Dabei geht es um die gängige Praxis vieler Ämter, bei Beschwerden, Hinweisen und Auskünften aus der Bevölkerung die **Personalien des Informanten** dem betroffenen Dritten, gleich ob Privatperson oder Unternehmen, **mitzuteilen** und damit nachteilige Konsequenzen für den Hinweisgeber auszulösen bzw. zumindest diese Befürchtung zu wecken. Dies geschieht wiederholt auch dann, wenn ausdrücklich um vertrauliche Behandlung gebeten wurde.

Ich habe die betroffenen Dienststellen darauf aufmerksam gemacht, daß eine derartige Offenlegung der Identität eine Datenübermittlung in den privaten Bereich hinein darstellt und daher nur unter den engen Voraussetzungen des § 17 Bremisches Datenschutzgesetz (BrDSG) zulässig ist. Die Personalien des Informanten dürfen danach im Regelfall nur weitergegeben werden, wenn dieser zugestimmt oder aber der betroffene Dritte ein besonderes rechtliches Interesse an der Kenntnis der Identität hat. Ein einfaches „berechtigtes" Interesse reicht für eine Offenbarung nicht aus.

In mehreren Fällen behaupteten die Behörden, die Hinweisgeber hätten nicht ausreichend deutlich auf die gewünschte Vertraulichkeit aufmerksam gemacht. Deshalb hätten sie angenommen, befugt zu sein, deren Personalien weiterzugeben. In einem anderen Fall war ein Amt der Auffassung, aus der Tatsache, daß in einem gerichtlichen Verfahren die Verwaltungsakten ohnehin vollständig dem Gericht und dem Kläger oder dem Rechtsvertreter offengelegt werden müssen, schließen zu dürfen, daß der Berechtigte schon vorher unverzüglich zu unterrichten sei, um sich gegen das Vorbringen des Bürgers wehren zu können. Diese Auffassungen sind unzutreffend; Kontrollbehörden haben grundsätzlich Beschwerden oder Hinweisen von Amts wegen nachzugehen. Bei der Fallaufklärung stellt sich ohnehin oft heraus, daß die Information des Bürgers unbeachtlich oder für die Ermittlung des Sachverhalts von nachrangiger Bedeutung ist. Sollte es im Einzelfall unerläßlich sein, den Betroffenen mit dem Textinhalt der einzelnen Beschwerde zu konfrontieren, ist zunächst durch Schwärzung der Adresse, auszugsweise Wiedergabe oder Umschreibungen der gewählten Formulierungen die Anonymisierung soweit wie möglich sicherzustellen. Kann die Behörde einem Hinweis oder einer Beschwerde nicht nachgehen ohne die Offenbarung der Personalien des Eingebers, so ist er grundsätzlich vorher zu fragen. Nur auf diese Weise werden seine berechtigten Geheimhaltungsinteressen, die auch gegenüber den Auskunfts- und Akteneinsichtsrechten nach dem Verwaltungsverfahrensgesetz und dem BrDSG greifen, hinreichend geschützt.

In den vorliegenden Fällen haben im übrigen die betroffenen Verwaltungsbehörden in keinem Fall einen Verwaltungsakt erlassen, d. h. ein rechtliches Verbot oder Gebot ausgesprochen. Deshalb war es erst recht nicht erforderlich und rechtlich geboten, die personenbezogenen Daten der Bürger, die die Mitteilung gemacht hatten, offenzulegen. Die von mir angesprochenen Dienststellen haben zugesagt, ihre Praxis in Zukunft entsprechend zu ändern.

Notwendiges Gegenstück individueller Bürgerkontakte ist eine intensive **Öffentlichkeitsarbeit**, die die Bevölkerung über ihre Rechte gegenüber den datenverarbeitenden Stellen aufklärt und die für die Entgegennahme von Beschwerden zuständigen Stellen nennt. Solchen Aktivitäten setzt jedoch mein schmales Budget enge Grenzen. Im Berichtsjahr wurde die lange vergriffene Broschüre mit dem Text des Bremischen Datenschutzgesetzes wieder aufgelegt und das novellierte Bundesdatenschutzgesetz von 1990 mit aufgenommen. Ein Faltblatt zur Information der Öffentlichkeit über die Rechte des Betroffenen bei Nutzung seiner Daten zu Werbezwecken befindet sich in Vorbereitung.

2.2 Entwicklung der Informations- und Kommunikationstechnik

2.2.1 Situation im Land Bremen

Die technischen Veränderungen im EDV-Bereich machen auch vor der bremischen Verwaltung nicht halt. Teilweise bedingen diese technischen Entwicklungen neue Probleme im Bereich des Datenschutzes.

So ziehen in die bremische Verwaltung inzwischen vermehrt auch PC-Netze und tragbare Computer (Laptops, Notebooks) ein. Beide Entwicklungen haben eines gemeinsam: Die Daten werden mobil. Dies erfordert die Entwicklung von Sicherheitsstandards für „mobile Daten" (s. u. Ziffern 2.2.1.1 und 2.2.1.2).

Manche Weiterentwicklungen im technischen Bereich bieten allerdings Möglichkeiten, die dem Datenschutz zugute kommen. Dies gilt z.B. für die Weiterentwicklung der in der bremischen Verwaltung eingesetzten Datenschutz- und sicherheitssoftware (s. u. Ziffer 2.2.1.3).

— Organisatorische Veränderungen

Neben technischen Entwicklungen, die es zu beobachten gilt, sind auch organisatorische Veränderungen in der bremischen Verwaltung geplant, die Auswirkungen auf den Datenschutz haben können.

— ADV-Ausschuß

Die Koordinierung der technischen Entwicklung in der bremischen Verwaltung ist eine Aufgabe des ADV-Ausschusses (AADV). Dieser ist z. Zt. dabei, sein Selbstverständnis und seine Verfahrensweisen zu überdenken. Dabei geht es auch darum, ob die zur Zeit noch vorhandene Entscheidungskompetenz des AADV auf eine Beratungs- bzw. Empfehlungskompetenz reduziert wird. Bisher habe ich im AADV beratende Stimme und erhalte daher auch alle dazugehörigen Unterlagen. Bei der Neukonzipierung des AADV ist es wichtig, daß es für mich gegenüber der bisherigen Regelung keinen Informationsverlust gibt, d. h. daß ich nach wie vor über alle Planungen im ADV-Bereich rechtzeitig und umfassend informiert werde. Dies ist zur Erfüllung meiner Beratungsaufgabe, die sich aus dem Bremischen Datenschutzgesetz (BrDSG) ergibt, erforderlich.

2.2.1.1 PC-Netze

Durch die Vernetzung von PC's werden die Daten eines PC's grundsätzlich für alle an diesem Netz angeschlossenen PC's ohne Zeitverzögerung verfügbar. Ohne besondere Schutzvorkehrungen kann von jedem an das Netz angeschlossenen PC auf alle Daten aller am Netz hängenden PC's zugegriffen werden.

Zur Zeit werden von der Senatskommission für das Personalwesen (SKP) zwei Pilotprojekte zur „abteilungsbezogenen Datenhaltung auf PC-Netzen" in der Bremischen Verwaltung durchgeführt. Ich werde an diesen Pilotprojekten beteiligt. Aus meiner Sicht dienen diese Pilotprojekte auch dazu festzustellen, inwieweit sich Datenschutzanforderungen auf vernetzten PC's technisch bzw. organisatorisch umsetzen lassen. Erste Gespräche zwischen der SKP und mir haben bereits stattgefunden, in denen die weitere Vorgehensweise abgestimmt wurde. Schon jetzt lassen sich einige **Mindestanforderungen** festhalten, da bereits auf die

Erfahrung einiger Netzinstallationen in der bremischen Verwaltung zurückgegriffen werden kann. Zu diesen Forderungen zählen u.a.:

- Netze sollen nur dort eingesetzt werden, wo die Arbeitsorganisation und -strukturen es erfordern, d. h. wo von mehreren Personen auf die gleichen Datenbestände zugegriffen werden muß.
- Der als Netz- bzw. Fileserver eingesetzte PC darf nicht als Arbeitsplatzrechner, sondern nur für diese Serverzwecke eingesetzt werden.
- Sobald auf einem der am Netz angeschlossenen PC's wegen der auf ihm zu verarbeitenden personenbezogenen Daten Schutzmaßnahmen einzurichten sind, sind diese auf allen anderen an das Netz angeschlossenen PC's ebenfalls zu installieren.
- Es muß sichergestellt sein, daß nur auf die Daten, die zur gemeinsamen Nutzung vorgesehen sind, von anderen Benutzerinnen und Benutzern zugegriffen werden kann und alle anderen Daten abgeschottet sind, d. h., daß die lokalen Festplatten nur von dem jeweiligen PC aus gelesen werden können und die Netzzugriffe auf Serverfestplatte(n) beschränkt werden.

Weitere Anforderungen ergeben sich aus den jeweiligen Anwendungen, für die das Netz eingerichtet werden soll.

2.2.1.2 Laptops und Notebooks

Durch tragbare PC's (Laptops, Notebooks, etc.) werden Daten mitsamt ihren Anwendungen mobil. Die Datenverarbeitungs- und Datenspeicherungskapazitäten der tragbaren PC's stehen denen der anderen in nichts nach, auch wenn die Gehäuse wesentlich kleiner sind. Die besondere Bedeutung für den Datenschutz ergibt sich aus dem Umstand, daß mobile PC's wesentlich leichter abhanden kommen können (z. B. durch Diebstahl, Verlust) als ortsgebundene. Gerade dadurch, daß tragbare PC's im allgemeinen die Diensträume verlassen, sind sie besonders gefährdet und erfordern weitergehende Schutzvorkehrungen als „normale" PC's.

Bei der Anschaffung der Geräte sollte von vornherein auf eine **Sicherheitsausstattung** Wert gelegt werden. Dazu gehören unter anderem das Vorhandensein

- eines Sicherheitsschlosses,
- eines festen Behältnisses mit Zahlenschloßkombination für den Transport, aber auch
- von Schutzvorrichtungen für die vorhandenen Schnittstellen.

Neben diesen Maßnahmen zum Schutz der Geräte sind u. a. folgende **Mindestanforderungen an den Einsatz** von tragbaren PC's zu stellen:

- Verarbeitung personenbezogener Daten auf tragbaren PC's darf nur erfolgen, wo dies aufgrund der Aufgaben unvermeidbar ist.
- Falls personenbezogene Daten auf dem PC verarbeitet werden, ist die Installation einer Schutzsoftware erforderlich, die die verschlüsselte Abspeicherung der Daten auch auf der Festplatte sicherstellt, sowie den Zugriff auf den PC nur nach Eingabe von Kennung und Paßwortabfrage zuläßt. Paßwörter müssen verschlüsselt abgelegt sein.
- Eine Umgehung des Sicherheitssystems auf der Festplatte ist durch eine Sperrung des Diskettenlaufwerks sicherzustellen. Dies bietet gleichzeitig die Gewähr, daß über das Diskettenlaufwerk kein ungesichertes Einspielen von Anwendungsprogrammen und keine unkontrollierte Datenübertragung über das Diskettenlaufwerk erfolgt.
- Die Schnittstellen des tragbaren PC's sind zu sperren, um eine unbefugte Weitergabe von Programmen und Daten zu verhindern. Die Berechtigung zur Entsperrung der Schnittstellen zur internen Weiterverarbeitung der Daten sollte bei der Systemverwalterin bzw. beim Systemverwalter liegen.
- Für die tragbaren PC's müssen in den Dienststellen, in denen sie eingesetzt werden, verschließbare Schränke vorhanden sein, in die sie nach Dienstschluß eingeschlossen werden.
- Besonders sensible Daten dürfen grundsätzlich nicht auf tragbaren PC's verarbeitet, erfaßt oder gespeichert werden. Nach §28 Abs. 2 Nr. 1 Satz 2 Bundesdatenschutzgesetz (BDSG) gehören hierzu insbesondere solche Daten, die sich

auf gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten, religiöse oder politische Anschauungen oder auf arbeitsrechtliche Verhältnisse beziehen.

Auch hier ergeben sich je nach den auf dem tragbaren PC gehaltenen Daten noch weitere Anforderungen an die Datenschutzmaßnahmen. Daher werde ich die Entwicklung aufmerksam verfolgen.

2.2.1.3 Protokollierung bei „Safeguard"

Nachdem ich bereits im März 1990 (s. a. 13. Jahresbericht, Ziffer 2.12.2) darauf hinwies, daß die Protokollierung der damals eingesetzten Sicherungssoftware für die Datenschutzkontrollen wenig geeignet ist, gibt es inzwischen eine neue Version dieser Software. Allerdings ist auch diese Version noch nicht einsatzfähig. Deren Protokollierungsmöglichkeiten sind wesentlich flexibler und auch ausführlicher. Aus meiner Sicht fehlt nur noch die Protokollierung des Schließens von Dateien. Es besteht der Wunsch des Beratungszentrums der SKP, auf den Einsatz dieser neuen Version zu verzichten und auf die Bereitstellung einer Version mit graphischer Oberfläche (WINDOWS) zu warten. Sofern mir in Kürze eine akzeptable verbindliche Terminzusage über die Verfügbarkeit der WINDOWS-Version gegeben wird, erscheint es sachgerecht, in der Regel auf den Einsatz der „Zwischenlösung" zu verzichten. Bei der weiteren Konzeptionierung der Verwendung von „Safeguard" werde ich beteiligt.

2.2.2 Fernwartung von DV-Systemen

DV-Systeme müssen wie alle technischen Systeme gewartet werden, um funktionsfähig zu bleiben oder wieder zu werden. Die Wartung bezieht sich dabei auf die Hardware (sogenannte Hardware- oder Gerätewartung) und auf die Software, vor allem die Betriebs- und Netzsoftware und wichtige andere Fremdsoftware (sogenannte Software-Wartung).

Kamen früher die Wartungstechniker der Herstellerfirmen zum Kunden, um dort ihre Wartungsarbeiten (z. B. Systemzustands- und Fehlermeldungen prüfen, Funktionen überprüfen, Hard- und Softwarefehler beheben etc.) zu verrichten, geschieht dies heute in großem Umfang — auch bei kleineren Systemen und im PC-Bereich — durch sogenannte Fernwartung. Techniker verrichten ihre Arbeit nicht mehr primär vor Ort beim Kunden, sondern von entfernten Wartungs- bzw. Servicezentralen aus, die zu diesem Zweck über Kommunikationsnetze mit den zu wartenden DV-Systemen verbunden sind.

Die Fernwartung (Hard- und/oder Software-Wartung) birgt **Risiken**, denen mit besonderen technisch-organisatorischen Maßnahmen begegnet werden muß. Die Risiken liegen darin, daß ein neuer online-Zugang zum Rechner geschaffen wird, über den sich Personen anmelden, die eine hohe Priorität und weitgehende Rechte auf dem Rechner besitzen. Der Rechnerbetreiber kann nur begrenzt kontrollieren, welche Person tatsächlich die Fernwartung vornimmt und welche Daten evtl. zur Wartungs- bzw. Servicezentrale übertragen werden. Ihm ist in der Regel auch nicht bekannt, welche Sicherungsmaßnahmen in der Wartungs- bzw. Servicezentrale getroffen sind. Auch ist nicht ausgeschlossen, daß „Hacker" über die Wartungsverbindung Zugriff auf den Rechner erhalten. Viele DV-Anwender, vor allem im Bereich der kleineren Systeme und im Bereich der PC-Installationen, machen sich über die Risiken der Fernwartung keine Gedanken. Sie lassen sich von den Kostenargumenten beeindrucken, ohne zu bedenken, daß ihre Systeme und ihre Datenverarbeitung betroffen sind und sie — soweit personenbezogene Daten verarbeitet werden — die volle datenschutzrechtliche Verantwortung tragen. Ein Beispiel für die Arglosigkeit findet sich im Beitrag über die Kontrolle einiger kommunaler Krankenhäuser (s. u. Ziffer 10.1.3).

In meinem 5. Jahresbericht (vor zehn Jahren!) habe ich bereits **Anforderungen zur Ausgestaltung der Fernwartung** formuliert, die sich nach dem Stand der Technik damals auf die großen Rechnersysteme bezogen. Inzwischen wird die Fernwartung auch bei kleineren Rechnersystemen und bei PC-Installationen praktiziert, was bedeutet, daß die seinerzeitigen Anforderungen auf ihre heutige Anwendbarkeit hin überprüft und ggf. angepaßt werden müssen. Hierbei hat sich gezeigt, daß die damaligen Anforderungen im wesentlichen auch heute noch gültig sind. In Übereinstimmung mit meinen Kollegen halte ich bei der Fernwartung folgende technische Anforderungen für angemessen:

1. Der Systembetreiber bzw. das Rechenzentrum und nicht die Wartungsfirma definiert Art und Umfang der Fernwartung (Eindringtiefe) und dokumentiert die Einzelheiten in prüffähiger Form.

2. Die Software-Fernwartung wird entweder ganz ausgeschlossen oder auf bestimmte Ausnahmefälle beschränkt.

3. Die Fernwartungsverbindung darf nur vom zu wartenden Rechner her aufgebaut werden. Der Aufbau der Verbindung sollte im Normalfall automatisch über festgelegte Rufnummern erfolgen, die im Rechner hinterlegt sind. Der Wartungstechniker muß sich bei jedem Wartungsvorgang durch ein vereinbartes Paßwort autorisieren.

4. Fernwartungsaktivitäten müssen lokal mitverfolgt (z. B. auf Bildschirm oder Drucker) und ggf. unterbrochen werden können. Hierzu sollte bei der verantwortlichen Stelle vor Ort ein Systemexperte vorhanden sein.

5. Das Wartungszentrum darf nur Zugriff auf Dateien erhalten, die unter der Zugriffskennung der Wartung vom Systembetreiber/Rechenzentrum eingerichtet wurden.

6. Der Zugriff auf **personenbezogene** Daten sollte ausgeschlossen werden, z. B. dadurch, daß Daten auf Verzeichnissen oder Datenträgern gespeichert werden, die während des Wartungsvorganges nicht verfügbar sind. Ist dies nicht zu realisieren, ist auf eine Fernwartung zu verzichten. Eine Fernwartung parallel zum laufenden Rechenbetrieb sollte ausgeschlossen sein.

7. Werden Test- und Serviceprogramme der Wartungsfirma auf der Anlage gespeichert, sind diese unter einer besonderen Kennung abzuspeichern.

8. Die Wartungstechnik darf keinen Systemverwalter-Status erlangen können. Sofern eine physikalische Abkopplung der Benutzerdateien nicht möglich ist, ist das Einspielen von Änderungen ins Betriebssystem und in systemnahe Software durch die Fernwartungszentrale abzulehnen und ausschließlich vor Ort durchzuführen. Die Übernahme der Änderungen ist erst nach Freigabe der speichernden Stelle vorzunehmen. Anwendungsprogramme sollten durch Fernwartung nicht aktiviert werden können.

9. Sämtliche Fernwartungsaktivitäten sind revisionssicher aufzuzeichnen. Die Protokolle müssen durch entsprechende Programme ausgewertet werden können. Im Konsolprotokoll sollten alle die Fernwartung betreffenden Systemnachrichten besonders gekennzeichnet und durch Handzeichen der verantwortlichen Mitarbeiter abgezeichnet werden. Im Logbuch sollten Beginn und Ende der Fernwartung sowie Ort und Rufnummer der Wartungszentrale protokolliert werden.

Darüber hinaus sind **organisatorische** Maßnahmen zu treffen, die weitgehend auch für die traditionelle Wartung gelten. Im Wartungsvertrag sind klare Regelungen hinsichtlich der Abgrenzung der Kompetenzen und Pflichten zwischen Wartungspersonal und Personal der verantwortlichen Stelle festzuschreiben. Insbesondere sind Art und Umfang der Wartung schriftlich festzulegen. Grundsätzlich sollte das Wartungspersonal auf das Datengeheimnis verpflichtet werden. Falls personenbezogene Daten bei der Wartung den Technikern zur Kenntnis gelangen (weil z. B. nach dem Wartungsvertrag Speicherauszüge/Dumps zu übergeben sind), ist ihre Nutzung für andere Zwecke ausdrücklich zu untersagen. Nach Abschluß der Arbeiten sind diese Daten oder Unterlagen unverzüglich zu löschen. Sofern die Fernwartung durch ausländische Stellen durchgeführt werden soll, ist sicherzustellen, daß die jeweiligen Regelungen über die Übermittlung von personenbezogenen Daten an Stellen außerhalb der Bundesrepublik Deutschland (z. B. § 18 Bremisches Datenschutzgesetz — BrDSG, § 17 Bundesdatenschutzgesetz — BDSG) angewendet werden, d. h. ggf. bei fehlendem Datenschutzrecht im Drittland die Auftragsvergabe unterbleibt. Die Fernwartungszentrale darf von sich aus keine Daten an andere Stellen weiterübermitteln.

Maßnahmen und Vorkehrungen dieser Art bilden insgesamt ein wirksames Instrumentarium, das eine ordnungsgemäße und vom Betreiber des Systems verantwortbare Datenverarbeitung gewährleistet und unbefugte Offenbarungen von personenbezogenen Daten soweit wie möglich ausschließt.

2.2.3 Abhörrisiken im Mobilfunk

2.2.3.1 Aufhebung der Funkfrequenzbeschränkungen

Die bislang gültige Beschränkung der zulässigen Empfangsbereiche für Rundfunkempfänger wurde zum 30. Juni 1992 durch das Bundesministerium für Post und Telekommunikation (BMPT) aufgehoben.

Bisher war bereits der Besitz von Empfängern (speziellen Scannern oder auch nur manipulierten Radioempfängern) verboten, mit denen die Sonderfrequenzen von Polizei, Rettungswesen, Bundesbahn, Schiffsfunk, von mobilen Telefonen (B- und C-Netz), aber auch von schnurlosen Telefonen abgehört werden können. Zuwiderhandlungen konnten zu einer Bestrafung und zur Beschlagnahme der Geräte führen. Durch die Neuregelung ist nun der Besitz und auch der Betrieb von Empfängern erlaubt, mit denen diese Sonderfrequenzen abgehört werden können. Solche Geräte sind bereits jetzt im Handel. Mit einer schnellen Verbreitung dieser Geräte ist zu rechnen.

Das BMPT hat in einer Presseerklärung die Auffassung vertreten, „der Empfang (solcher) Aussendungen, die nicht für die Allgemeinheit vorgesehen sind, bleibt aber zum Schutz des Fernmeldegeheimnisses untersagt". Diese Auffassung ist nicht unbestritten. Bei den juristischen Diskussionen darüber, ob bereits das Empfangen solcher Sendungen auf den Sonderfrequenzen unerlaubt ist oder erst die Verwertung des Gehörten bzw. ob ein eventuelles Verbot strafbewehrt ist oder nicht, ist immer zu berücksichtigen, daß sich eine Übertretung eines etwaigen Verbotes selten nachweisen läßt.

Ausgangspunkt aller Überlegungen muß daher sein, daß das Abhören der Sonderfrequenzen mit Geräten möglich ist, deren Besitz und Betrieb seit Juli 1992 erlaubt ist. Die **Vertraulichkeit des gesprochenen Wortes** bei schnurlosen Telefonen, bei Mobiltelefonen und beim Funkverkehr der Sonderdienste ist somit durch die Aufhebung der Funkfrequenzbeschränkungen nicht mehr gewährleistet.

Die Deutsche Bundespost TELEKOM wäre verpflichtet, ihre Kundinnen und Kunden darauf hinzuweisen, daß sowohl schnurlose Telefone als auch Mobiltelefone relativ einfach abgehört werden können (vgl. § 3 Abs. 5 TELEKOM-Datenschutzverordnung — TDSV).

Für Rettungsdienste, Feuerwehr, Polizei u. ä. ergibt sich die Problematik, daß über den Funkverkehr häufig z. T. sehr sensible personenbezogene Daten übermittelt werden, die leicht von Unbefugten abgehört werden können. Auch wäre das Szenario denkbar, daß Rettungsfahrzeuge eine Katastrophenstelle nicht erreichen können, weil Massen von Schaulustigen, die aus Sensationsgier die Sonderfrequenzen abgehört haben, zum Ort des Geschehens fahren und die Zufahrtswege verstopfen!

2.2.3.2 Regelungsinitiative der Innenministerkonferenz

Aus Sorge um die öffentliche Sicherheit hat die Ständige Konferenz der Innenminister und -senatoren der Länder am 20. 11. 1992 gefordert, „die bisher geltenden Funkfrequenzbeschränkungen wieder einzurichten und darüber hinaus in das Gesetz über Fernmeldeanlagen (FAG) durchsetzbare Verbote für den Vertrieb, Besitz und die Inbetriebnahme von Breitbandempfängern sowie das Abhören von geschützten Frequenzbereichen durch Unberechtigte aufzunehmen".

Damit wäre wieder bereits der Besitz von Geräten, mit denen die Sonderfrequenzen abgehört werden können, verboten. Dieses Verbot ließe sich auch kontrollieren und z. B. durch Beschlagnahme unerlaubter Geräte durchsetzen. Diese Regelungen würden die Hemmschwelle für den Kauf und die Benutzung dieser unerlaubten Geräte stark heraufsetzen. Gegen vorsätzliches Abhören aus kriminellem Interesse bieten sie allerdings keinen Schutz.

2.2.3.3 Technische Gegenmittel

Schon vor der Freigabe der Sonderfrequenzen war der Schutz, den das Verbot der abhörgeeigneten Geräte für die Bedürfnisse besonders der Sicherheitsbehörden (Militär, bestimmte Polizeidienststellen u. a.) darstellte, nicht ausreichend. In diesen Bereichen lief und läuft der Telefon- und Funkverkehr teilweise verschlüsselt bzw. verschleiert ab. So wird z. B. bei der Polizei Bremens ein — wenn auch

veraltetes — IDA-System zur Verschleierung von sensiblen Daten im Funkverkehr angewendet.

Eine **Verschlüsselung** der Funkstrecken, ob nun zwischen schnurlosem Telefon und Basispunkt oder z. B. zwischen Rettungswagen und Leitstelle, würde das Abhören dieser Gespräche sehr erschweren bzw. nahezu unmöglich machen. Ein zufälliges Mithören wäre ausgeschlossen; nur mit hohem technischem Aufwand und viel krimineller Energie wäre das Abhören noch möglich.

Die Verschlüsselungstechnik wird aus Kostengründen weder im Bereich von Feuerwehr und Rettungsdienst noch in allen Bereichen der Polizei noch beim Fernsprechen (einschließlich der schnurlosen Telefone und der Mobiltelefone) eingesetzt. In wenigen Fällen werden Mobiltelefone in digitaler Technik (D1-, D2-Netz) verwendet, bei denen das Abhören schwieriger ist. Bei entsprechender Nachfrage nach Ver- bzw. Entschlüsselungstechnik wäre allerdings mit einer drastischen Preissenkung zu rechnen, so daß die Kosten nicht mehr als Grund gegen einen Einsatz dieser Technik angeführt werden könnten.

Durch die Verwendung eines schnurlosen Telefons, bei dem die Übertragung zwischen Basisstation und Handapparat digitalisiert geschieht, wird das Abhören zumindest erschwert. Einer der oben genannten Scanner reicht dazu nicht mehr aus, da die digitalisierten Funksignale auch wieder analogisiert werden müssen, wozu eine entsprechende Synchronisation erforderlich ist. Dies erfordert einen höheren technischen Aufwand.

2.2.3.4 Maßnahmen in Bremen

Seit September 1992 gibt es beim Senator für Inneres und Sport einen ad-hoc-Ausschuß, der anhand der taktischen, technischen und betrieblichen Forderungen und unter Berücksichtigung der Kosten-Nutzen-Relation kurzfristige Lösungsmöglichkeiten untersuchen soll. Dies bedeutet allerdings nicht, daß bei allen zuständigen Stellen die erforderliche Sensibilität zu erwarten wäre. In dem für die Neuplanung der Feuerwehrleitstelle zuständigen Ausschuß wurde das Abhörrisiko bagatellisiert.

Im November 1992 bat ich in einem Schreiben an den Senator für Inneres und Sport sowie an das Fernmeldetechnische Amt der Stadt Bremen (FTA) darum, das Problem der Abhörmöglichkeit aufzugreifen und entsprechende organisatorische und soweit möglich auch technische Gegenmaßnahmen zu treffen. Ende Dezember erstellte das FTA den Entwurf eines „Merkblattes für alle Benutzer von schnurlosen Telefonen", der inhaltlich mit mir abgestimmt wurde und nun in der Endfassung vorliegt. Ein Merkblatt für die Funktelefone soll folgen.

2.3 Europäische Entwicklungen

2.3.1 Europarat: Bedeutungszuwachs für die Datenschutz-Konvention von 1981

Der Datenschutz in Europa befindet sich derzeit in einer Phase dynamischer Fortentwicklung. Die Diskussion konzentriert sich in erster Linie auf den **Richtlinienvorschlag der EG-Kommission**, den sie am 15. Oktober 1992 in 2. Fassung vorgelegt hat (Geänderter Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt der EG Nr. C 311, S. 30 ff.).

Doch muß, wer über Datenschutz auf europäischer Ebene spricht, mit der **Konvention des Europarates von 1981** beginnen. Das **„Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten"** versuchte erstmals, für den Bereich der Mitgliedstaaten des Europarates ein Mindestmaß an einheitlichem Datenschutz zu schaffen. Die Regelungsziele des Übereinkommens waren denen des heutigen EG-Richtlinienvorschlags durchaus vergleichbar: Die Harmonisierung des Datenschutzstandards im Bereich des Europarates sollte zur Konsequenz haben, daß der grenzüberschreitende Verkehr personenbezogener Daten — von bestimmten Ausnahmen abgesehen — nicht mehr beschränkt werden können sollte. In den Erwägungsgründen der Richtlinie wird an mehreren Stellen auf die Bedeutung der Vorarbeiten des Europarates und die Parallelität der grundlegenden Zielsetzung hingewiesen, gleichzeitig aber deutlich gemacht, daß die EG im Hinblick auf den materiellen Datenschutzstandard deutlich über die Konvention von 1981 hinausgehen will. Das Regelungswerk des Europarates ist im Laufe der vergangenen Dekade durch zahlreiche bereichsspezifische **Empfehlungen** verfeinert und präzisiert worden; sie betreffen

u. a. medizinische Datenbanken, Personalinformationssysteme, die Direktwerbung und die Datenverarbeitung durch die Polizei. In den letzten drei Jahren, d. h. seit dem **Systemwechsel in den osteuropäischen Staaten**, hat die Europarats-Konvention dort eine vorher nicht erwartete neue Bedeutung erhalten. Der Anschluß an die westliche Wertegemeinschaft vollzieht sich in einer Reihe von Staaten des früheren „Ostblocks" über die Unterzeichnung bzw. Ratifikation von Vereinbarungen des Europarats. Dies gilt insbesondere für die Menschenrechts- und die Datenschutzkonvention, die beide aufgrund ihres Inhaltes besonders geeignet sind, die Abkehr vom früheren stalinistischen Regime zu symbolisieren.

2.3.2 Europäische Gemeinschaft: Harmonisierung durch Richtlinie

2.3.2.1 Regelungsziele: Gemeinschaftsweiter Schutz des Persönlichkeitsrechts und Freiheit des grenzüberschreitenden Datenverkehrs

Ausgangspunkt für die Initiative der Kommission war zunächst die Erkenntnis, daß der für 1993 angestrebte **Binnenmarkt** einen grenzüberschreitenden, möglichst freien und ungehinderten Informationsverkehr auch und gerade mit personenbezogenen Daten braucht. Einzelne Fälle des Verbots von Datenexporten aus Mitgliedstaaten der EG in Partnerländer ohne Datenschutzgesetzgebung (etwa der bekannte „Fiat-Fall" in Frankreich) hatten das Risiko eines „Flickenteppichs" unterschiedlicher nationaler Datenschutzgesetzgebungen — neben Staaten ohne jede eigene Regelung — deutlich gemacht.

Anders ausgedrückt: Die Konzeption des EG-Binnenmarktes als (auch) „informationeller Großraum" hat eine Harmonisierung der Regelungen über den Umgang mit personenbezogenen Daten im Zusammenhang mit dem Waren-, Dienstleistungs- und Kapitalverkehr zur zwingenden Voraussetzung. Es ist vor allem den vielfältigen Bemühungen der Datenschutzbeauftragten und -kommissionen in den EG-Ländern zu verdanken, daß dieser, auf die kommerziellen Aspekte der EG-Integration konzentrierten Sichtweise die Dimension der Grundrechtssicherung hinzugefügt wurde. Die EG-Kommission erkannte die Notwendigkeit des **europaweiten Schutzes des Persönlichkeitsrechts und der Privatsphäre** vor den Risiken der immer umfassender betriebenen Datenverarbeitung, nicht zuletzt auch dafür, die soziale Akzeptanz ihrer Vorschläge zu erhöhen.

Wenn, schlagwortartig formuliert, dem informationellen Großraum ein „Grundrechts-Großraum" entsprechen soll, kann der gleichwertige Schutz der personenbezogenen Daten auch nicht auf einem Mindestlevel, vielmehr muß er zwingend auf einem hohen Niveau hergestellt werden. Die Gleichwertigkeit des Schutzniveaus wiederum verhindert, daß „Datenoasen" entstehen oder bestehen bleiben, die zu Wettbewerbsverzerrungen führen könnten. Noch einmal: **Freier Informationsverkehr** und harmonisierter Schutz personenbezogener Daten auf hohem Niveau bilden die beiden Grundintentionen des Richtlinienvorschlages.

Harmonisierung heißt dabei, daß vorhandene Rechtssysteme angeglichen werden und Mitgliedstaaten ohne Datenschutz-Legislation verpflichtet werden, ein der Richtlinie entsprechendes nationales Gesetz zu erlassen. Die Richtlinie hat dabei, vergleichbar dem deutschen Bundesdatenschutzgesetzes (BDSG), die Funktion eines Rahmens, der durch bereichsspezifische Verordnungen und Richtlinien ausgefüllt werden kann. Für die ISDN-Problematik hat ja die Kommission — zusammen mit dem Vorschlag zur Harmonisierung — einen speziellen Richtlinien-Entwurf vorgelegt.

2.3.2.2 Vom 1. Entwurf zum Geänderten Vorschlag

Die Beratung der Richtlinie in den verschiedenen EG-Gremien benötigte ca. zwei Jahre und verlief mühevoll und kontrovers. Auf Einzelheiten gehe ich in diesem Jahresbericht nicht ein. Entscheidende Bedeutung für die Änderungen im zweiten Kommissionsvorschlag gegenüber dem ersten im September 1990 vorgelegten Text waren in erster Linie die Debatten und Beschlüsse des Europäischen Parlaments. Beigetragen haben aber auch die Stellungnahmen der Konferenz der Datenschutzbeauftragten und -kommissionen in der EG, an deren Sitzungen ich als Mitglied der deutschen Delegation teilgenommen habe. Einflußreiche Lobbygruppen haben sich intensiv um Korrekturen in ihrem Sinne bemüht und damit teilweise auch Erfolg gehabt; dies gilt beispielsweise für die Interessenverbände der Direktwerbung, der Kreditinstitute oder der Kreditkartenunternehmen.

2.3.2.3 Systemdivergenz als Hauptproblem

Hauptproblem für eine schnelle Verständigung auf EG-Ebene sind die prinzipiellen Divergenzen der in den Mitgliedstaaten vorhandenen Datenschutzkonzeptionen. Diese Unterschiede machen die Schwierigkeit der Aufgabe deutlich, die die Kommission zu bewältigen hatte und hat, um eine inhaltliche Angleichung zu erzielen. Nur wenn man diese **Systemdifferenzen** kennt und akzeptiert, daß ein Rechtsinstrument der EG Bestandteile verschiedener Rechtsordnungen integrieren muß, um in den Mitgliedstaaten akzeptiert zu werden, ist eine faire und gleichzeitig realistische Beurteilung des neuen Textvorschlages möglich.

Da gibt es den Unterschied zwischen Lizensierungsmodellen, also Rechtsordnungen, die die Einrichtung und Nutzung von Datenverarbeitung von der Genehmigung durch eine Kontrollinstitution abhängig machen (z. B. Frankreich, Großbritannien), und dem deutschen Konzept der genehmigungsfreien Verarbeitungserlaubnis, wenn die Zulässigkeitsvoraussetzungen des Datenschutzrechts eingehalten sind. Stärker legalistisch orientierten Systemen, die nur staatlichem Recht effiziente Schutzqualität zubilligen, stehen Staaten gegenüber, die die Regelung des Umgangs mit personenbezogenen Daten mehr der Selbstregulierung durch die betroffenen Verbände und Interessengruppen überlassen wollen (z. B. die Niederlande). Die Datenschutzinstitutionen sind in mehreren Mitgliedstaaten strikt auf Funktionen hoheitlicher Genehmigungen und Kontrolle beschränkt, während im deutschen Modell das Element der Hilfestellung und Beratung der datenverarbeitenden Stellen im Vordergrund steht. Während mancherorts, z. B. in Frankreich, sensitive Datenkategorien benannt werden, die einem Sonderschutz unterstehen, folgt die Datenschutzdoktrin in Deutschland spätestens seit dem Volkszählungsurteil des Bundesverfassungsgerichts der These, daß die Schutzwürdigkeit personenbezogener Angaben ausschließlich vom Verwendungskontext abhängt. Während das Datenschutzrecht hierzulande das höhere Eingriffsrisiko eher dem öffentlichen Bereich zubilligt, also im Verhältnis zwischen Staat und Bürger sieht, sind es anderswo in erster Linie die privaten Datenverarbeiter, denen die Verarbeitungsrestriktionen gelten.

2.3.2.4 Abweichungen vom deutschen Datenschutzmodell

Der Richtlinienvorschlag weist in mehreren Bereichen Abweichungen vom BDSG bzw. generell vom deutschen Datenschutzkonzept auf, d. h. Regelungen, in denen — aus deutscher Sicht — systematische „Fremdkörper" auftauchen bzw. interpretationsbedürftige Anleihen bei ausländischen Rechtsordnungen gemacht wurden.

Dies gilt zunächst für den **Anwendungsbereich.** Hier knüpft die Richtlinie (Art. 3) an den Begriff der „Verarbeitung" an und folgt dabei dem französischen Beispiel. Dadurch wird allerdings der Begriff der Datei nicht funktionslos; vielmehr gilt die Richtlinie bei der nicht-automatisierten Datenverarbeitung nur bei Vorliegen einer Datei. Die Kommission konnte sich also — entgegen den Wünschen des Parlaments — nicht dazu verstehen, Datenverarbeitung ohne Rücksicht auf den Datenträger und damit auch den Datenumgang in und aus Akten einzubeziehen. Dies hat zur Folge, daß die Verarbeitung von Aktendaten durch die Richtlinie überhaupt nicht tangiert wird. Ohnehin greift diese nur für Rechtsmaterien, die der Regelungskompetenz der Europäischen Gemeinschaft unterliegen, also z. B. in aller Regel nicht für die Datenverarbeitung durch die Polizei oder andere Sicherheitsbehörden.

Besonders gewöhnungsbedürftig aus deutscher Sicht ist Art. 7, der die Voraussetzungen für die **Zulässigkeit der Datenverarbeitung** für den öffentlichen und den nicht-öffentlichen Bereich gemeinsam regelt. Dies entspricht dem Wunsch des Europäischen Parlaments und auch der Mehrheit der EG-Datenschutzkonferenz. Die nach den Bereichen Verwaltung und Wirtschaft differenzierenden Zulässigkeitskataloge des ursprünglichen Richtlinienvorschlags wurden zu sehr allgemein formulierten Generalklauseln zusammengeschmolzen. Würde man den Text dieses Artikels wörtlich ins BDSG übernehmen — was aber nicht zwingend geboten ist — würde der Verarbeitungsrahmen zumindest für öffentliche Stellen erheblich ausgeweitet. Anders als im ursprünglichen Text finden sich im geänderten Vorschlag auch keine speziellen Bestimmungen mehr über erlaubte Zweckänderungen und die Zulässigkeitsbedingungen für Übermittlungen. Anders ausgedrückt: Im Vergleich mit dem Urtext hat sich die neue Richtlinien-Version noch stärker von der Systematik des deutschen Datenschutzrechts entfernt.

Für **sensitive Daten** — Art. 8 zählt dazu Angaben über die rassische und ethnische Herkunft, die politische Meinung, die religiöse, philosophische oder moralische

Überzeugung, die Gewerkschaftszugehörigkeit oder die Gesundheit — stellt die Richtlinie ein grundsätzliches Verarbeitungsverbot auf, das nur unter engen Voraussetzungen aufgehoben werden kann. Eine dieser Möglichkeiten besteht darin, daß die Mitgliedstaaten aus Gründen wichtiger öffentlicher Interessen gesetzliche Ausnahmen vorsehen. Im deutschen Regelungskontext wäre als Konsequenz dieser neuen Regel-Ausnahme-Systematik eine Reihe spezieller gesetzlicher Erlaubnisse zu schaffen, z. B. für die Nutzung des Merkmals Gewerkschaftszugehörigkeit durch den Arbeitgeber beim tarifvertraglich vereinbarten Direkteinzug der Beiträge.

Die Abweichung mit der wahrscheinlich größten praktischen Bedeutung ist die Einführung der **Meldepflicht** für alle Dateien, also auch für die der privaten datenverarbeitenden Stellen, zu einem von der Datenschutz-Kontrollbehörde zu führenden Register (Art. 18). Mit dieser umfassenden Registrierung folgt die Kommission dem Beispiel einer ganzen Reihe nationaler Rechte: Die vorherige Anmeldung und Überprüfung bzw. sogar Genehmigung von Dateien bildet den Eckpfeiler des Datenschutzsystems u. a. in Frankreich, Großbritannien und den Niederlanden. Allerdings wird der zu erwartende Zuwachs an Bürokratisierung für Unternehmen und Betriebe dadurch stark abgemildert, daß für zahlreiche Verarbeitungskategorien, etwa Textverarbeitung oder Erfüllung gesetzlicher Verarbeitungspflichten, die Meldung vereinfacht werden oder sogar ganz entfallen kann (Art. 19). Insofern handelt es sich in der Tat, wie die Kommission in der Begründung formuliert, um ein System der „selektiven Kontrolle". Ich trete — ebenso wie die Aufsichtsbehörden der anderen Bundesländer — dafür ein, den Mitgliedstaaten in diesem Punkt noch mehr Regelungsspielraum einzuräumen, um jedenfalls im deutschen Rechtsraum den Aufbau einer neuen Registerbürokratie, die keine entsprechende Effektivierung der Kontrolle erwarten läßt, zu vermeiden.

In den Beratungen der EG-Gremien und in den Interventionen verschiedener Lobbygruppen — nicht zuletzt aus den USA — wurde die Regelung der Zulässigkeitsvoraussetzungen für die **Weitergabe personenbezogener Daten in Drittstaaten** (Art. 26, 27) besonders intensiv diskutiert und kritisiert. Für Zielländer, die nicht Mitglied der EG sind und die kein angemessenes Schutzniveau, also insbesondere keine Datenschutzgesetzgebung, aufweisen, geht die Richtlinie von einem grundsätzlichen Verbot des Datenexports aus. Diesem Prinzip steht ein abschließender Katalog von Ausnahmen gegenüber, wozu insbesondere der Fall gehört, daß die Übermittlung von Daten in einen Drittstaat ohne Datenschutzrecht zur Erfüllung eines Vertrages (z. B. eines Reisevertrages) notwendig ist (Art. 26 Abs. 1 Satz 2). Als Ausnahme läßt die Richtlinie auch die viel diskutierte „Vertragslösung" zu (Art. 27 Abs. 1), also die Absicherung der Einhaltung des Datenschutzrechts des Exportstaates durch einen Vertrag zwischen der übermittelnden Stelle und dem ausländischen Empfänger. § 17 BDSG, der die Datenübermittlung durch Bundesbehörden an Stellen außerhalb des Geltungsbereichs des BDSG normiert, müßte bei Inkraftreten der Richtlinie entsprechend neu gefaßt bzw. präzisiert werden; für die grenzüberschreitende Weitergabe durch nichtöffentliche Stellen müßte eine entsprechende Bestimmung neu geschaffen werden.

2.3.2.5 Akzeptanz der Rechtsangleichung

Der an ausgewählten Divergenzbeispielen gezogene Vergleich von Konzeption und Regelungsinhalten des Richtlinien-Vorschlags einerseits und des deutschen Datenschutzrechts andererseits darf nicht mißverstanden werden. Es wäre ein verfehlter Ansatz, aus der einzelstaatlichen Perspektive die Vorstellungen der Gemeinschaft ängstlich daraufhin abzuprüfen, inwieweit sie vom eigenen Recht abweichen, und dann alle Bemühungen daran zu setzen, im weiteren Beratungsverfahren noch so viel wie möglich von dem in Deutschland bestehenden Regelungsmodell „zu retten". Eine **integrationsfreundliche Sichtweise** muß die von unseren EG-Partnern entwickelten Lösungsmodelle zur Kenntnis nehmen, sich um deren Verständnis bemühen und sich auf den Versuch einlassen, gemeinsame Grundstrukturen herauszudestillieren und bewährte Elemente von unseren Nachbarstaaten zu übernehmen. Dies gilt auch dann, wenn das soeben reformierte BDSG oder die jüngeren Landesdatenschutzgesetze erneut novelliert werden müßten. Diese Konsequenz ergibt sich keineswegs nur im Bereich des Datenschutzes; die parallele Problematik stellt sich bei vielen anderen auf Harmonisierung angelegten Initiativen der Kommission, zuletzt vor allem im Bereich des Umweltschutzes.

2.3.3 Aktuelle Themen der deutschen Diskussion

2.3.3.1 Höchststandard oder Mindestniveau?

In den Mittelpunkt der deutschen Diskussion hat sich jüngst vor allem die Frage geschoben, ob die Richtlinie einen Höchststandard an Datenschutz festlegt, der vom einzelstaatlichen Recht nicht überschritten werden kann, oder ob die Mitgliedstaaten die Möglichkeit behalten, den Datenschutz auf nationaler Ebene intensiver auszugestalten und fortzuentwickeln. Das Rechtsinstrument der Richtlinie mit ihrem doppelstufigen Verfahren war zwar ursprünglich eindeutig für die Festlegung eines EG-weiten Mindestniveaus vorgesehen, wird inzwischen aber in der Rechtssetzungspraxis der EG-Institutionen vielfach ähnlich detailliert wie die in den Mitgliedstaaten unmittelbar verbindliche Verordnung ausgestaltet. Ähnlich wie in Deutschland der Bund seine Kompetenz zur Rahmengesetzgebung immer wieder zum Erlaß von Vollregelungen benutzt hat (z. B. im Melderecht), machen auch Rat und Kommission mit Richtlinien gelegentlich ins einzelne gehende Vorgaben, die den eigentlich vorgesehenen Spielraum für die Umsetzung in das einzelstaatliche Recht weitgehend einschränken.

Die Frage, ob die Datenschutz-Richtlinie „nach oben offen" ist oder nicht, läßt sich nicht pauschal beantworten, verlangt vielmehr eine präzise Analyse der in den einzelnen Bestimmungen enthaltenen Spielräume. Die Richtlinie enthält einerseits ausdrückliche **Öffnungsklauseln**, die mit der Formulierung „Die Mitgliedstaaten können vorsehen . . ." explizit der einzelstaatlichen Gesetzgebung Ergänzungs- und Erweiterungsmöglichkeiten einräumen. Beispiel dafür ist Art. 20, der die Erstreckung der Meldepflicht zum Register auf nicht-automatisierte Dateien zuläßt.

In der Richtlinie gibt es andererseits eine **allgemeine Interpretationsklausel**, wonach die Mitgliedstaaten „die Voraussetzungen näher bestimmen (können), unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist" (Art. 5 Abs. 2). Diese Formulierung erlaubt die Ausfüllung der zahlreichen Generalklauseln, etwa — wie die Begründung ausführt — die Feststellung der Fälle, in denen das Interesse der betroffenen Person dem Verarbeitungsinteresse der speichernden Stelle oder eines Dritten vorgeht (vgl. Art. 7 f). Die Konkretisierung einer solchen Interessenabwägung erlaubt mithin eine erhebliche Bandbreite bereichsspezifischer Regelungen. Gleiches gilt z. B. für die zahlreichen weit gefaßten Ausnahmen bei der Verarbeitung sensitiver Daten (Art. 8 Abs. 2 und 3).

Anders ausgedrückt: Die fehlende Präzision bei der Formulierung der Voraussetzungen für die Zulässigkeit der Datenverarbeitung (Art. 7) hat zwei Seiten: Die Offenheit der generalklauselartigen Formulierungen bietet zwar wenig konkrete Vorgaben für die Mitgliedstaaten, die derzeit kein Gesetz haben und sich darauf beschränken wollen, den Text der Richtlinie mehr oder weniger wörtlich zu übernehmen. Auf der anderen Seite bietet sich im Zusammenspiel mit der allgemeinen Interpretationsklausel des Art. 5 Abs. 2 für „datenschutzfreundlichere" Mitgliedstaaten die Chance, auf nationaler Ebene **bereichsspezifische Verschärfungen** beizubehalten oder einzuführen. Mit den deutschen Kollegen ebenso wie mit den Datenschutzbeauftragten der anderen EG-Mitgliedstaaten halte ich allerdings eine Ergänzung wenn nicht des Textes, dann zumindest der Erwägungsgründe für geboten, die klarstellt, daß ein über die Richtlinie hinausgehender Schutzstandard überall dort zulässig bleibt, wo es nicht um grenzüberschreitenden Datenverkehr und damit um binnenmarktrelevante Vorgänge geht.

Kollisionslagen können sich allerdings nur dort ergeben, wo es um einzelstaatliche bereichsspezifische Vorschriften im Geltungsbereich der Richtlinie geht; ein Großteil der sektoralen Regelungen dagegen — etwa im Recht der Sicherheitsbehörden — befindet sich außerhalb der Gemeinschaftskompetenz.

2.3.3.2 Kontrollinstitutionen

Jeder Mitgliedstaat muß eine oder mehrere staatliche Behörden benennen, die für die Überwachung der Einhaltung des Datenschutzes zuständig sind. Diese Behörden müssen „unabhängig" sein, was im deutschen **dualen Kontrollmodell** insoweit Probleme schaffen könnte, als die Aufsichtsbehörden für den nicht-öffentlichen Bereich anders als die Datenschutzbeauftragten des Bundes und der Länder in die Hierarchie der Verwaltungsbehörden eingeordnet sind. Das Erfordernis der **Unabhängigkeit** bezieht sich nach der Intention der EG-Kommission wohl in erster Linie auf das Verhältnis zur Regierung bzw. Exekutive und weniger auf die Abgrenzung von den zu kontrollierenden Stellen (Behörden, Unternehmen).

Bevor allerdings Abstriche an dieser Anforderung gemacht werden, sollten insbesondere die Organisationsmodelle der Nachbarstaaten auf übertragbare Elemente hin geprüft werden. Wird die Unabhängigkeit als institutionelle Bedingung der Kontrollinstitution in der Richtlinie wegen der deutschen Besonderheiten teilweise „geopfert", besteht zum einen die Gefahr, daß der freie Status der in den EG-Mitgliedstaaten bestehenden Datenschutzinstanzen wieder in Zweifel gezogen wird. In den EG-Ländern, die aufgrund der Richtlinie erstmals ein nationales Datenschutzgesetz verabschieden müssen, könnte die Regierungsabhängigkeit der Überwachungsbehörden die Kontrolleffizienz nachhaltig schwächen und die Implementation des neuen Rechts behindern.

2.3.3.3 Abschaffung des betrieblichen Datenschutzbeauftragten?

Eine Kontrollinstitution innerhalb der datenverarbeitenden Stelle ist in der Richtlinie nicht vorgesehen. Ich teile die Auffassung der Aufsichtsbehörden der anderen Bundesländer, daß im weiteren Beratungsverfahren versucht werden sollte, eine neue Bestimmung durchzusetzen, die es den Mitgliedsländern ausdrücklich ermöglicht, die Bestellung betrieblicher Datenschutzbeauftragter vorzusehen. Auf der anderen Seite hat die fehlende Erwähnung der internen Beauftragten auch nicht die Verpflichtung zur Folge, diese bewährte Einrichtung aus dem BDSG zu streichen. Vielmehr läßt sich die **unternehmenseigene Datenschutzkontrolle** den organisatorischen Maßnahmen zurechnen, die die datenverarbeitenden Stellen nach Art. 17 zu treffen haben, um jede Form unzulässiger Datenverarbeitung zu verhindern. Die Befürchtung, ein indirekter Druck zur Abschaffung der betrieblichen Beauftragten könne dadurch entstehen, daß sie für Unternehmen mit Sitz in Deutschland einen negativen Kosten- und damit Standortfaktor darstellen, der in anderen Mitgliedstaaten nicht anfällt, erscheint wenig fundiert. Zum einen sind die Ausgaben für den hauseigenen Datenschützer — bezogen auf die Gesamtbilanz — doch eher bescheiden, zum anderen hat seine Tätigkeit selbst vielfach rationalisierende und kostensparende Effekte.

Das **Funktionsspektrum für die Beauftragten für den Datenschutz** in deutschen Unternehmen würde nach einer Umsetzung der Richtlinie deutlich erweitert. Sie müßten zum einen darauf achten, daß die erweiterten Meldepflichten erfüllt werden bzw. festgestellt wird, ob die im Unternehmen vorhandenen Dateien unter ein vereinfachtes Anmeldeverfahren fallen oder von der Registerpflicht ganz befreit sind. Ein zweites Beispiel: Die gesamte grenzüberschreitende Datenübermittlung des Unternehmens wäre nach mehreren Kriterien zu überprüfen, zum einen daraufhin, ob es sich um Zielländer innerhalb oder außerhalb der EG handelt, im zweiten Fall dann unter dem Gesichtspunkt, ob im Empfängerstaat ein angemessenes Schutzniveau existiert oder ein ggf. fehlendes staatliches Datenschutzrecht durch entsprechende Maßnahmen wie Vertragslösungen kompensiert werden kann und muß. Zu diesem Zweck wären auch die Berichte der in der Richtlinie vorgesehenen transnationalen Gremien, d. h. der Datenschutzgruppe (Art. 31) und des Beratenden Ausschusses (Art. 34), auszuwerten. In der Einführungsphase der neuen Regelungen wird sich mit Sicherheit der Kontakt zur Aufsichtsbehörde erheblich intensivieren.

2.3.4 Gesamtbeurteilung und weiteres Verfahren

In den kommenden Monaten wird die Richtlinie in der zuständigen **Arbeitsgruppe „Wirtschaftsfragen" des Ministerrates** noch ausführlich diskutiert werden. Der dann festgelegte **„Gemeinsame Standpunkt" des Rates** geht dann an das Europäische Parlament zur zweiten Lesung. Nach dem von der Kommission angestrebten, wohl aber zu optimistischen Zeitplan sollen die Mitgliedstaaten die Vorschriften zur Umsetzung der Richtlinie bis spätestens 01. Juli 1994 erlassen haben. Eine Übergangsfrist für die Einbeziehung der „Altdateien" in die neuen der Richtlinie angepaßten Regelungen liefe dann bis zum 01. Juni 1997.

Trotz aller Kritikpunkte im einzelnen verdient der geänderte Vorschlag im ganzen ein **positives Urteil.** Gegenüber dem ersten Text vom September 1990 lassen sich ein leichter verständlicher Aufbau, eine klarere Systematik und eine größere Praktikabilität feststellen. Im weiteren Gesetzgebungsverfahren besteht noch die Möglichkeit, die eine oder andere Verbesserung aus der Sicht deutscher Erfahrungen zu erzielen, etwa die ausdrückliche Verankerung einer einzelstaatlichen Option für die Bestellung betrieblicher Beauftragter für den Datenschutz (s. o. Ziffer 2.3.3.3). Änderungswünsche sollten sich aber auf unverzichtbar erscheinende Kernforderungen beschränken. Sonst besteht die Gefahr, daß dieses sehr schwierige Harmonisierungsprojekt, bei dem bereits viel erreicht worden ist, zerredet

wird. Das derzeit vielbeschworene **„Subsidiaritätsprinzip"** darf nicht dafür herhalten, die Initiative der Kommission in einem Zusammenwirken einzelstaatlicher Regelungsegoismen untergehen zu lassen. Nicht zu vergessen ist schließlich, daß die EG-Staaten, die derzeit noch keine Datenschutzgesetzgebung haben, sich nur durch Druck aus Brüssel dazu bereitfinden werden, den Schutz des Persönlichkeitsrechts gesetzlich zu verankern.

3. Senatskanzlei

3.1 Schutz von Teilnehmerdaten beim Privatrundfunk

Radio Bremen als öffentlich-rechtliche Anstalt läßt die Daten seiner Teilnehmer im Auftrag bei der Gebühreneinzugszentrale (GEZ) in Köln verarbeiten. Die privaten Sender in der Bundesrepublik Deutschland finanzieren sich dagegen ausschließlich über Werbung und verarbeiten daher keine personenbezogenen Daten ihrer Zuschauer. Ausnahme ist ein Spielfilmkanal, bei dem eine Abonnementsgebühr zu entrichten ist. Diese gilt aber für den gesamten Kanal, nicht für den einzelnen Spielfilm. Rückschlüsse auf Vorlieben und Sehgewohnheiten sind daher nicht möglich.

Dies ist anders beim **pay-per-view**, einer vor allem in den USA verbreiteten Abrechnungsform. Der Kunde zahlt hier für die einzelne Sendung. Anhand der Abrechnungsdaten läßt sich ein **„Teilnehmerprofil"**, das Zeitpunkt, Art, Inhalt und Häufigkeit der eingeschalteten Sendungen ausweist, erstellen. Die Überwachung eines der wichtigsten Freizeitbereiche der Bürger wäre damit möglich.

Diese Form des „Bezahlfernsehens" gibt es in Deutschland zwar derzeit nicht, sie könnte aber jederzeit eingeführt werden. § 28 des am 01. 01. 1992 in Kraft getretenen Rundfunkstaatsvertrages enthält daher vorsorglich die Vorschrift, daß die Abrechnungsdaten in einer Form zu speichern sind, die „Teilnehmerprofile" verhindert, wenn nicht der Betroffene selbst ausdrücklich eine detaillierte Regelung verlangt.

Insoweit — wie an diesem Beispiel aufgezeigt — der Datenschutz bei privaten Veranstaltern im Rundfunkstaatsvertrag geregelt ist, bedarf es keiner Bestimmungen in den Landesmediengesetzen mehr. Letztere treffen nur ergänzende Regelungen, etwa was die Kontrollbefugnis angeht. Mit dieser Leitlinie habe ich gegenüber dem nichtständigen Ausschuß „Mediengesetze" zum Gesetzentwurf zur Änderung rundfunkrechtlicher Vorschriften (Bürgerschafts-Drucks. 13/171 vom 09. 06. 1992) Stellung genommen. Ich habe dafür plädiert, die einschlägigen Normen des Landesmediengesetzes von 1989 im wesentlichen zu übernehmen und nur in Details zu ergänzen. Entscheidend ist für mich, daß meine Kontrollbefugnis als Landesbeauftragter unverändert bestehen bleibt. Als Ergänzung habe ich u. a. eine Bestimmung angeregt, die das Verhältnis zwischen der Landesmedienanstalt und dem Landesbeauftragten für den Datenschutz bei Beanstandungsverfahren präzisiert.

Senatskanzlei und Bürgerschaftsausschuß sind meinen Vorschlägen gefolgt und haben sie in den Gesetzentwurf aufgenommen.

4. Personalwesen

4.1 Automatisierte Arbeitszeiterfassung in der bremischen Verwaltung

Der Rechnungshof hat in seinem Prüfungsbericht vom 18. 09. 1992 das bisherige Verfahren zur Arbeitszeiterfassung und -kontrolle problematisiert. Insbesondere könne es bei manueller Erfassung der Arbeitszeit passieren, daß Beginn, Ende und Unterbrechungen der Arbeitszeit unrichtig eingetragen werden. Außerdem würden vielfach die Arbeitszeiten gerundet und Überschreitungen der Mittagspause sowie Unterbrechungszeiten aus privater Veranlassung nicht oder nur unvollkommen eingetragen. Vergleiche des Rechnungshofs von Baden-Württemberg in zwei Dienststellen kurz nach dem Wechsel von einer manuellen zu einer automatisierten Zeiterfassung hätten u. a. ergeben, daß in einem Monat mit automatisierter Erfassung die Arbeit an wesentlich mehr Tagen früher begonnen und später beendet worden sei. Weil die manuelle Zeiterfassung zahlreiche Mängel habe, empfiehlt der Rechnungshof, grundsätzlich die elektronische Zeiterfassung einzuführen.

Aufgrund dieses Berichts hat die Senatskommission für das Personalwesen (SKP) einen Entwurf zur Änderung der Bremischen Arbeitszeitverordnung sowie einen Entwurf zur Änderung der „Grundsätze für die gleitende Arbeitszeit" vorgelegt.

Des weiteren beabsichtigt der Senator für Finanzen (SfF), in seinem Ressort die automatisierte Arbeitszeiterfassung einzuführen und hat dazu den Entwurf einer „Musterdienstvereinbarung für die Arbeitszeitregelung und -erfassung" vorgelegt.

— Verordnung zur Änderung der Bremischen Arbeitszeitverordnung (SKP)

Der Entwurf sieht in § 4 vor, daß entgegen der bisherigen Regelung alle Beamten — ausgenommen sind bestimmte Personalgruppen — an der gleitenden Arbeitszeit teilzunehmen haben und daß die tägliche Arbeitszeit automatisiert zu erfassen ist.

Ich habe die SKP darauf hingewiesen, daß die als Rechtsgrundlage für die Arbeitszeitverordnung bzw. deren Änderung herangezogene Vorschrift des § 71 Abs. 1 Bremisches Beamtengesetz (BremBG) möglicherweise die in § 4 Abs. 5 des Verordnungsentwurfs vorgesehene ausnahmslose automatisierte Erfassung nicht abdeckt. Die Ermächtigungsnorm im Gesetz besagt lediglich, daß der Senat die regelmäßige Arbeitszeit durch Rechtsverordnung regelt. Die SKP hat zugesagt zu prüfen, ob die Ermächtigungsnorm im BremBG im Hinblick auf die Erfordernisse des Art. 80 Abs. 1 Satz 2 Grundgesetz (GG) präzisiert werden muß, wonach Inhalt, Zweck und Ausmaß der erteilten Ermächtigung im Gesetz bestimmt werden müssen.

— Grundsätze für die gleitende Arbeitszeit (SKP)

Diese Grundsätze sollen im Gegensatz zur vorgenannten Verordnung für alle Beschäftigtengruppen gelten. Mit der in Nr. 2 vorgesehenen Regelung, wonach alle Bediensteten des bremischen öffentlichen Dienstes Beginn und Ende der täglichen Arbeitszeit innerhalb der Rahmenzeit selbst bestimmen können, sollen diese Grundsätze der vorgesehenen Änderungsverordnung angepaßt werden. Allerdings sind bestimmte Personalgruppen wegen der Art ihrer Tätigkeit hiervon ausgenommen (z. B. Polizei, Feuerwehr, Justizvollzugs- und Reinigungspersonal). Gleichwohl soll nach Nr. 7 dieser geänderten Grundsätze die tägliche Arbeitszeit für alle Bediensteten automatisiert erfaßt werden.

Ich habe der SKP mitgeteilt, daß eine Arbeitszeiterfassung der Personengruppen, die von der gleitenden Arbeitszeit ausgenommen sind, sowohl manuell als auch automatisiert arbeits- bzw. dienstrechtlich nicht erforderlich und damit nicht zulässig ist. Zweck der Arbeitszeiterfassung ist es, für jeden Beschäftigten ein individuelles „Arbeitszeitkonto" zu führen, d. h. die Einhaltung der Regelarbeitszeit zu überprüfen, Unterschreitungen nacharbeiten und Überschreitungen „abfeiern" zu lassen. Beginn und Ende der täglichen Arbeitszeit der Personalgruppen, die diese nicht selbst bestimmen können, können durch einfache Anwesenheitskontrolle des jeweiligen Vorgesetzten festgestellt werden. Bei fester Arbeitszeit, insbesondere bei Schichtdienst, können Fehlzeiten ohnehin nicht ausgeglichen werden.

Nach den neuen Grundsätzen ist beabsichtigt, daß die Bediensteten einen Ausdruck der erfaßten Zeiten sowie des Ergebnisses der Zeitsummenrechnung erhalten. Noch offengelassen ist, ob die Bediensteten diese durch Selbstausdruck aus dem Arbeitszeiterfassungsgerät erhalten oder ob die jeweilige Personalstelle die Ausdrucke anfertigt und den Bediensteten aushändigt. Beide Möglichkeiten sind zulässig, wenn die im Zeiterfassungsgerät gespeicherten Daten nur zur Herstellung der Ausdrucke verarbeitet werden. Dies ist nach den Grundsätzen vorgesehen. Die SKP hat zugesagt, mir die überarbeiteten Grundsätze erneut zur Prüfung vorzulegen.

— Musterentwurf einer Dienstvereinbarung (SfF)

Parallel zu den Entwürfen der Rechtsverordnung und der „Grundsätze" hat mir der Senator für Finanzen den „Musterentwurf einer Dienstvereinbarung über die Arbeitszeitregelung und -erfassung" zur Prüfung vorgelegt. Der Musterentwurf weicht in einigen Punkten von den beabsichtigten „Grundsätzen", die für die gesamte bremische Verwaltung gelten sollen, ab.

Auch hier ist vorgesehen, die tägliche Arbeitszeit durch automatisierte Zeiterfassungsgeräte an den Eingängen der Dienstgebäude zu erfassen. Die Dienstzeiten sollen für jeden Bediensteten auf einem Arbeitszeitkonto festgehalten werden, das in den Personalstellen der Beschäftigungsdienststellen geführt wird. Auch hier habe ich mich gegen die Einbeziehung der Beschäftigten ohne Gleitzeitoption gewandt und unterstrichen, daß als Zweck der automatisierten Erfassung eine

bloße „Pünktlichkeitskontrolle" nicht in Betracht kommt (s. o). Der Senator für Finanzen teilt meine Auffassung nicht und beabsichtigt nach wie vor, auch die Beschäftigten mit fester Arbeitszeit in die automatisierte Arbeitszeiterfassung einzubeziehen. In der SKP dagegen bestehen Überlegungen, in die „Grundsätze" entsprechende Ausnahmeklauseln aufzunehmen.

Den vorgesehenen Katalog der zu erfassenden und auszuwertenden Daten habe ich als zu umfangreich bemängelt, weil Geburtsdatum, Personalnummer sowie dienstliche Telefonnummer für die Arbeitszeiterfassung nicht erforderlich sind. Der Senator für Finanzen wird den Datenkatalog entsprechend reduzieren.

Des weiteren verstieß die Absicht, wonach die Daten für Urlaub, Krankheit und Kuren zusammen mit den Arbeitszeitdaten verarbeitet werden und die bisher in der Personalstelle manuell geführten Aufzeichnungen ersetzen sollten, gegen das Zweckbindungsgebot nach § 12 Abs. 1 Bremisches Datenschutzgesetz (BrDSG). Die Datenschutzbeauftragten des Bundes und der Länder haben zu diesem Thema im Jahre 1991 eine Konferenzentschließung gefaßt, wonach automatisierte Systeme zur Verarbeitung von Personaldaten nicht dazu genutzt werden dürfen, zu unterschiedlichen Zwecken (z. B. Urlaubsdatei, Telefondatenerfassung, PC-Betriebsdaten) gespeicherte Angaben zu Persönlichkeitsprofilen der Beschäftigten zu verknüpfen (s. a. 14. Jahresbericht, Ziffer 2.1.1). Der Senator für Finanzen hat die getrennte Führung des Arbeitszeit-Erfassungssystems zugesagt und wird die Dienstvereinbarung entsprechend ändern.

Zur technischen Ausstattung habe ich darauf hingewiesen, daß auf der Code-Karte, mit der jeder Bedienstete Zugriff auf sein individuelles Arbeitszeitkonto haben soll, nur ein minimaler Datensatz gespeichert sein darf: Die Kartennummer ist ausreichend.

Außerdem ist die im Haus des Reichs vorgesehene Hardware für das Arbeitszeiterfassungssystem überdimensioniert. Da die Arbeitszeitkonten in den Personalstellen der einzelnen Dienststellen (senatorische Behörde, Finanzämter etc.) geführt werden, ist eine zentrale behördenübergreifende Speicherung zu vermeiden.

Die Terminals sollten daher mit ausreichender „Intelligenz" ausgerüstet sein, um den zentralen Server zu entlasten bzw. überflüssig zu machen. Der zentrale Server sollte allenfalls als „Vermittlungsrechner" eingesetzt werden, der die von den Zeiterfassungsterminals übergebenen Datensätze direkt an die Personalstellen weiterleitet. Hierfür bedarf es keiner 486DX-Rechnerkapazität. Ein kleinerer Rechner reicht aus, falls nicht ohnehin auf einen zentralen Server ganz verzichtet werden kann (s. o.). Nicht einmal eine Zwischenspeicherung sollte beim zentralen Server erfolgen. Daher sind auch keine Back up- bzw. Streamer-Möglichkeiten vorzusehen. Bei entsprechender Kapazität der Endgeräte ist auch eine unterbrechungsfreie Stromversorgung nicht erforderlich.

Der zentrale Drucker sollte nur dazu dienen, System-Fehlermeldungen auszudrucken. Durch geeignete Maßnahmen ist sicherzustellen, daß die Systemadministration keinen Zugriff auf die Arbeitszeitdaten erhält.

Eine zunächst vorgesehene gleichzeitige Nutzung des zentralen Servers für externe Bürokommunikationsdienste (z. B. elektronische Post, Teletax) ist abzulehnen, da durch den Anschluß an das offene Postnetz die Datensicherheit und der Datenschutz nicht mehr ausreichend gewährleistet werden können (Hackerproblematik etc.).

Bei den dezentralen Geräten ist sicherzustellen, daß die Arbeitszeiterfassung sicher von anderen Anwendungen abgeschottet wird und nur von den zuständigen Beschäftigten aufgerufen werden kann. Dies kann z. B. durch den Einsatz von entsprechend konfigurierter Sicherungssoftware (Safeguard) geschehen.

Der Senator für Finanzen hat erklärt, er werde meine Vorschläge zum Einsatz der Hard- und Software übernehmen, zumal eine Reduzierung der DV-Ausstattung auf das notwendige Maß kostengünstiger sei. Der überarbeitete Musterentwurf soll mir erneut vorgelegt werden.

4.2 Personalplanungs- und -statistiksystem

Die Senatskommission für das Personalwesen (SKP) hat das Konzept **„Personalcomputer-unterstützte Personal- und Stellendateninformationen (PePSI)"** entwickelt mit dem Ziel, diese PC-Anwendung bei allen Personalstellen der bremischen Verwaltung einzuführen. Vorgesehen ist im wesentlichen, Personaldaten

aus den automatisierten Abrechnungsverfahren bzw. Stellenplanverzeichnissen der SKP den Personalstellen mittels eines Abrufverfahrens zur Verfügung zu stellen. Diese Personaldatensysteme sollen durch die in den Personalstellen der Behörden vorhandenen Personaldaten ergänzt werden.

Ziel dieser dezentralen Personalinformationssysteme soll es sein, eine flexible und unabhängige Personal- und Stellenplanung zu ermöglichen. Hierzu ist insbesondere beabsichtigt, die bisher in unterschiedlicher Form vorhandenen Daten (Karteikarten, Geschäftsverteilungspläne, Personalakten und Stellenplan-Listen) zu integrieren. PePSI soll also eine Vielzahl von Personaldaten (z. B. Berufsbezeichnung, Arbeitszeit, Dienstpostenübergabe, Datum der letzten Beförderung/ Höhergruppierung u. a.) enthalten, obwohl viele Daten für die Bearbeitung von Personalangelegenheiten nicht ständig benötigt werden.

Ich habe der SKP dargelegt, daß der Aufbau von dezentralen Personaldatensystemen, die mit den Personaldatenbanken der SKP verbunden sind, nach den derzeit geltenden Bestimmungen nur zulässig ist, soweit dies zur Planung oder Durchführung dienstlicher, organisatorischer, sozialer oder personeller Maßnahmen erforderlich ist und dadurch schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Ein solches Verfahren darf nur eingerichtet werden, soweit dies unter Berücksichtigung des betroffenen Personenkreises und der Aufgaben der beteiligten Stellen angemessen ist.

Im übrigen ist § 14 Bremisches Datenschutzgesetz (BrDSG) beachtlich, wonach die Einrichtung eines **Abrufverfahrens** den Erlaß einer Rechtsverordnung vorschreibt. Hierbei sind Datenempfänger, die Datenart und der Zweck des Abrufs festzulegen.

Soweit die Personalstellen an die SKP-Datenbanken angeschlossen werden und insoweit ein Datenaustausch stattfindet, ist grundsätzlich davon auszugehen, daß sowohl der SKP als auch den jeweiligen Personalstellen die gleichen personenbezogenen Beschäftigtendaten zur Verfügung stehen. Dies ist besonders dann problematisch, wenn unklar bleibt, welche konkreten Aufgaben im Rahmen der Personalwirtschaft und Personalverwaltung der SKP bzw. als Abgrenzung dazu den Personalstellen der einzelnen Dienststellen obliegen. Erst wenn geklärt ist, welche Stellen welche Aufgaben wahrnehmen, können die Beschäftigten erkennen, welche Stellen zu welchem Zweck welche personenbezogenen Daten benötigen.

In diesem Zusammenhang habe ich die SKP aufgefordert, aufgrund der Novellierung des Bremischen Datenschutzgesetzes im Jahre 1987 endlich die „Allgemeinen Verwaltungsvorschriften für die Durchführung des Datenschutzes bei der Verarbeitung personenbezogener Daten von bremischen Bediensteten und Versorgungsempfängern (AVV-BrDSG-Personalwesen)" aus dem Jahre 1982 zu überarbeiten und der neuen Rechtslage anzupassen. Insbesondere ist die Verwaltungsvorschrift dahingehend zu ändern, daß die SKP und die jeweiligen Personalstellen der Behörden nicht mehr als eine einheitliche speichernde Stelle anzusehen sind. Der Austausch von Personaldaten zwischen der SKP und den Personalstellen ist als Übermittlung im Sinne von § 2 Abs. 2 Nr. 4 BrDSG zu qualifizieren mit den Zulässigkeitserfordernissen nach §§ 13, 14 BrDSG.

Die SKP hat Mitte Februar 1993 mitgeteilt, sie werde in Kürze einen Sachstandsbericht vorlegen und darin auch auf meine Rechtsauffassung detailliert eingehen.

4.3 Neues Personalaktenrecht

Am 01. Januar 1993 ist das neue Personalaktenrecht im Beamtenrechtsrahmengesetz (BRRG) in Kraft getreten. Danach gehören alle den Beamten betreffenden Unterlagen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten), zur Personalakte. Darüber hinaus ist festgelegt worden, daß Personalaktendaten ohne Einwilligung des Beamten nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden dürfen.

Des weiteren ist geregelt, daß nicht Bestandteil der Personalakte Unterlagen sind, die besonderen von der Person und dem Dienstverhältnis sachlich zu trennenden Zwecken dienen, z. B. Prüfungs-, Sicherheits- und Kindergeldakten. Kindergeldakten dürfen mit Besoldungs-und Versorgungsakten nur dann verbunden werden, wenn diese von der übrigen Personalakte getrennt sind und durch eine von der Personalverwaltung getrennten Organisationseinheit bearbeitet werden. Insoweit wird dem Sozialgeheimnis Rechnung getragen.

Eine weitere Verbesserung des Datenschutzes ergibt sich aus der strikten Trennung der Beihilfeunterlagen, die stets als Teilakte zu führen und von der übrigen Personalakte getrennt aufzubewahren sind. Beihilfeunterlagen sollen in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden; Zugang sollen nur Beschäftigte dieser Einheit haben.

Darüber hinaus enthält das novellierte BRRG präzise Regelungen zum Akteneinsichtsrecht des Beamten sowie eine Benachrichtigungspflicht bei erstmaliger Speicherung der Daten. Insbesondere ist dem Beamten auf Verlangen ein Ausdruck der zu seiner Person automatisiert gespeicherten Personalaktendaten zu überlassen. Das Einsichtsrecht umfaßt auch andere Akten, die personenbezogene Daten über den Beamten enthalten und für sein Dienstverhältnis verarbeitet oder genutzt werden; dies gilt jedoch nicht für Sicherheitsakten.

Eine weitere Regelung beinhaltet, daß von den Unterlagen über medizinische oder psychologische Untersuchungen und Tests im Rahmen der Personalverwaltung nur die Ergebnisse automatisiert verarbeitet oder genutzt werden, soweit sie die Eignung betreffen und ihre Verarbeitung oder Nutzung dem Schutz des Beamten dient.

Nach Inkrafttreten des BRRG ist der Landesgesetzgeber verpflichtet, das **Bremische Beamtengesetz** dem neuen Rahmenrecht **anzupassen.** Dies bedeutet jedoch nicht, daß sämtliche Rahmenvorschriften wörtlich zu übernehmen sind. Dem Gesetzgeber verbleibt ein Gestaltungsspielraum, insbesondere bei der Festlegung der „Zwecke der Personalverwaltung oder Personalwirtschaft" und der in diesem Rahmen zulässigen Verarbeitung im einzelnen. Die detailliertere Regelung der Bestimmung über den Schutz der Daten im bremischen öffentlichen Dienst (§ 22 BrDSG) bedarf daher keiner Novellierung.

Die Senatskommission für das Personalwesen hat erklärt, in der ersten Hälfte des Jahres 1993 einen Gesetzentwurf vorzulegen und mich frühzeitig zu beteiligen.

4.4 Bewerbungen in der Stadtverwaltung Bremerhaven (s. a. 13. Jahresbericht, Ziffer 2.1.1, Ergebnis)

In meinem 13. Jahresbericht habe ich das Bewerbungsverfahren innerhalb der Stadtverwaltung Bremerhaven beschrieben und kritisiert, daß die Beschäftigten ihre Bewerbungen über den nächsthöheren Vorgesetzten dem jeweiligen Amtsleiter zuzuleiten hatten. Dieser hatte die Bewerbungen an das Personalamt weiterzugeben. Die Eingangsbestätigung des Personalamts ging auf dem gleichen Dienstwege dem Bewerber zu.

Nach Erörterungen im Datenschutzausschuß der Bremischen Bürgerschaft hat der Magistrat beschlossen, daß grundsätzlich die Bewerbungen direkt an das Personalamt bzw. Schulamt zu richten sind, wobei es den Bediensteten freigestellt wird, ob sie den Weg über die Amtsleitung wählen wollen. Die Ausschreibungsrichtlinien sind entsprechend überarbeitet worden, so daß ein datenschutzgeschutzgerechtes Bewerbungsverfahren sichergestellt ist.

4.5 Eigenständiger Beihilfeanspruch für Familienangehörige (s. a. 13. Jahresbericht, Ziffer 2.1.5, Ergebnis)

Dieses Problem habe ich im 13. Jahresbericht dargestellt. Bisher stand ausschließlich dem behilfeberechtigten Angehörigen des öffentlichen Dienstes ein Beihilfeanspruch für seine Familienmitglieder zu; diese hatten keinen eigenständigen Beihilfeanspruch. Daraus ergab sich, daß Familienangehörige des Beihilfeberechtigten gezwungen waren, sämtliche dem Beihilfeantrag beizufügenden Arztunterlagen dem Familienmitglied zu übergeben, dem der Beihilfeanspruch zustand. Diese Verfahrensweise wurde insbesondere von getrennt lebenden Ehegatten sowie erwachsenen Kindern als problematisch empfunden. Obwohl die familiäre Verbundenheit nicht mehr besteht, erfuhr der Beihilfeberechtigte in diesen Fällen z. T. intimste Krankheitsdaten seiner Angehörigen.

Nach Beratungen im Datenschutzausschuß der Bremischen Bürgerschaft ist mit der Senatskommission für das Personalwesen (SKP) vereinbart worden, daß Familienangehörige eines Beihilfeberechtigten **direkt** bei der Beihilfestelle der SKP die Erstattung beihilfefähiger Aufwendungen beantragen können. Nach Gewährung der Beihilfe wird ein Duplikat des Bescheides in einem verschlossenen Umschlag, der nur unter bestimmten Bedingungen geöffnet werden kann, zur Personalakte

des Beihilfeberechtigten genommen. Auf diesem Formular sind neben den Rechnungs- und Beihilfebeträgen lediglich das Rechnungsdatum und die jeweilige Leistungsart angegeben. Dadurch ist nicht ersichtlich, welcher Arzt die Behandlung vorgenommen hat bzw. welches Hilfsmittel geleistet worden ist. Die einzelnen Rechnungsbelege, die der Familienangehörige anläßlich der Antragstellung in einem verschlossenen Umschlag dem Antrag beigefügt hat, erhält er mit dem Beihilfebescheid zurück. Das Duplikat des Bescheides wird nach drei Jahren aus der Beihilfeakte entfernt und vernichtet.

Die SKP beabsichtigt, anläßlich der anstehenden Anpassung der Beihilfevorschriften an das Gesundheitsstrukturgesetz noch in diesem Jahr auf das neue Verfahren hinzuweisen.

5. Inneres

5.1 Polizei

5.1.1 PC-Netz für die Bearbeitung von Anzeigen (s. a. 14. Jahresbericht, Ziffer 2.2.2.1, Ergebnis)

Im Berichtsjahr konnte die Projektphase der ersten Aufbaustufe des Verfahrens „Informations-System-Anzeigen-Dezentral" (ISA-D) abgeschlossen werden. Mit diesem Verfahren sollen alle Polizei-Inspektionen und Reviere (insgesamt 42 Organisationseinheiten) über ein lokales PC-Netz mittels Servers auf die angebundenen Systeme zugreifen können. Hierzu gehören die Polizeisysteme des Bundes (INPOL) und des Landes Bremen (ISA), das Bremer Einwohnermelderegister sowie die Kfz.-Zulassungsdateien des Bundes (ZEVIS) und der Stadt Bremen (FAZID). In der ersten Aufbaustufe werden dem anfragenden Polizeibeamten bestimmte Auskünfte aus den angebundenen Systemen in standardisierten Bildschirm-Masken zur Verfügung gestellt. Für die zweite Aufbaustufe ist im Anschluß geplant, die gesamte Vorgangsbearbeitung soweit wie möglich mit Hilfe des PC's durchzuführen.

ISA-D wurde in einer kriminalpolizeilichen Inspektion und in einem Polizeirevier probeweise eingesetzt. Ich habe mich im Sommer 1992 vor Ort darüber informiert, inwieweit meine datenschutzrechtlichen Anforderungen umgesetzt worden sind. Dabei war festzustellen, daß die in dem unter meiner Mitwirkung erstellten Datenschutzkonzept vorgesehenen technischen Maßnahmen weitgehend getroffen worden sind. Noch nicht realisiert waren allerdings der **Zugriffsschutz** mittels eines Magnetkartenlesers und die **Protokollierung** der Zugriffe auf Bundes- und Landessysteme. Zum Einsatz eines Magnetkartenlesers ist nach Angabe der Polizei ein Programm zum Auslesen fertiggestellt, das aber noch nicht zu Testzwecken ausgeliefert worden sei. Die Protokollierung solle auf einem speziellen Rechner erfolgen, über dessen Beschaffung erst dann entschieden werden könne, wenn Klarheit darüber bestehe, welche Hardware- und Softwarekomponenten für ISA-D zum Einsatz kommen. Zur Beschaffung dieser Komponenten ist ein Ausschreibungsverfahren eingeleitet worden, das voraussichtlich zur Zeit der Abfassung dieses Berichtes abgeschlossen sein wird. Beide Punkte sind Bestandteile dieser Ausschreibung, so daß meinen Anforderungen offenbar Rechnung getragen wird.

5.1.2 Verringerung der bundesweiten Datenspeicherung bei Staatsschutzdelikten

Eine im Jahr 1988 durchgeführte Datenschutzprüfung im Bereich der Inspektion 7 bei der Polizei (KpI-Staatsschutzdelikte) hatte ergeben, daß das Land Bremen das bundesweite Informationssystem APIS (Arbeitsdatei „Personen, Institutionen, Objekte, Sachen") nutzte, um dort alle im Bereich der Inspektion für polizeiliche und strafverfolgende Zwecke anfallenden relevanten Daten einzustellen. Diese Praxis stand nicht im Einklang mit der Errichtungsanordnung und den für die Nutzung von APIS erlassenen Richtlinien. APIS soll nämlich dazu dienen, Verdächtige und Täter bei schweren und überregional begangenen Straftaten zu erfassen, um Schwerpunkte zu bilden. Bei kleineren Delikten hingegen, z. B. der Beschädigung eines Wahlplakats (Sachbeschädigung), sollen Tatverdächtige bzw. Straftäter oder andere in solchen Zusammenhängen beteiligte Personen wie Zeugen, Hinweisgeber etc. nicht in APIS gespeichert werden.

Um eine Trennung zwischen den in APIS zu erfassenden Personen und den nur im Lande Bremen zu speichernden Personen aus dem Bereich des Staatsschutzes zu ermöglichen, hatte ich vorgeschlagen, alle in Bremen relevanten Fälle im Staats-

schutzbereich im bremischen Informationssystem der Polizei ISA (Informationssystem „Anzeigen") zu speichern und nur die schweren oder überregional tätigen Täter in das beim Bundeskriminalamt geführte APIS einzuspeichern.

Mein Lösungsvorschlag, alle bremischen Staatsschutzfälle vollständig in ISA zu führen, hat den Vorteil, daß der Staatsschutz am Verfahren ISA/CANASTA (Zentrales Aktennachweissystem der Staatsanwaltschaft) teilnehmen kann und damit erheblich schneller über den Verfahrensausgang bei der Staatsanwaltschaft informiert ist. Zum anderen können die vom Staatsschutz in ISA gespeicherten Daten am Löschfristenverfahren teilnehmen und einer automatisiert geführten Löschungsprüfung zugeführt werden.

Bei einem Besuch im Dezember 1992 habe ich die Umsetzung meiner Anregungen überprüft. Ich konnte feststellen, daß ein beim Staatsschutz installierter PC online mit dem ISA-Verfahren beim Rechenzentrum der bremischen Verwaltung (RbV) verbunden ist. Im einzelnen erfolgt die Umsetzung der ISA-Anbindung folgendermaßen:

Alle eingeleiteten Ermittlungsverfahren werden bei Eingang in der Staatsschutzabteilung in ISA erfaßt. Vor der Weitergabe an die Staatsanwaltschaft erfolgt vom Staatsschutz eine Ausgangserfassung, d. h. soweit sich aufgrund der Ermittlungen Sachverhalte geändert haben, werden die Daten in ISA entsprechend korrigiert oder ergänzt. Die Staatsschutzfälle erhalten in ISA eine gesonderte Kennung und sind von anderen Polizeidienststellen nicht abrufbar.

Die Erfassung von Staatsschutz-Fällen, die Eingabe von Änderungen sowie die Löschung von einzelnen Fällen erfolgt ausschließlich über den Staatsschutz-PC. Aufgrund noch bestehender Probleme hinsichtlich der Druckersteuerung durch die RbV-Programme wird noch auf ein gesondert ausgewiesenes Terminal mit Druckausgabe in der ISA-Zentrale zurückgegriffen. Ich gehe aber davon aus, daß dieses Problem demnächst beseitigt sein wird.

Im Ergebnis ist also festzustellen, daß mit dem Anschluß der Inspektion 7 (Abteilung Staatsschutz) an das ISA-Verfahren einer meiner wesentlichen Forderungen aus der Prüfung im Jahre 1988 Rechnung getragen wurde. Wegen weiterer, bei der Umsetzung entstandener technischer und verfahrensmäßiger Schwachstellen bin ich mit den beteiligten Stellen im Gespräch.

5.1.3 § 218 StGB: Speicherung betroffener Frauen

Bei Vorliegen des Verdachts auf Verstoß gegen § 218 StGB (Abbruch der Schwangerschaft) werden die betroffenen Frauen im polizeilichen Informationssystem ISA gespeichert. Ich habe gegenüber der Polizei Zweifel geäußert, ob eine solche Verfahrensweise aus ihrer Sicht zur Gefahrenabwehr oder vorbeugenden Straftatenbekämpfung überhaupt notwendig ist. Ich habe darauf hingewiesen, daß die Besonderheit dieses Deliktes darin besteht, daß Schwangerschaftsabbrüche aufgrund einer einmaligen unausweichlichen Konfliktsituation vorgenommen werden und deshalb mit einer Wiederholung nicht zu rechnen ist. Eine Speicherung der Frauen wegen des Tatvorwurfs des Verstoßes gegen § 218 StGB erscheint deshalb aus datenschutzrechtlicher Sicht wenigstens nach Abschluß des staatsanwaltschaftlichen Ermittlungsverfahrens bzw. gerichtlichen Verfahrens nicht mehr erforderlich.

Die Ortspolizeibehörde Bremerhaven hat daraufhin erklärt, sie halte es nicht für erforderlich, die betroffenen Frauen im Kriminalaktennachweis (KAN) zu registrieren. Sie sei 1991 vom Senator für Inneres und Sport angewiesen worden, solche Vorgänge nach Abschluß des staatsanwaltschaftlichen Ermittlungsverfahrens in ISA zu löschen. Dies sei in Bremerhaven umgesetzt worden, so daß keine weiteren Speicherungen vorgenommen und vorhandene Bestände gelöscht wurden.

Auch das Polizeipräsidium Bremen hat sich mir gegenüber entsprechend erklärt. Im Februar 1993 seien über diesen Deliktsbereich in ISA keinerlei Speicherungen mehr vorhanden.

Darüber hinaus hatte ich gebeten zu prüfen, ob auf eine automatisierte Speicherung in ISA nicht generell verzichtet werden kann. Es sollte vielmehr angestrebt werden, die Vorgänge nur noch unmittelbar in den zuständigen Kriminalkommissariaten zu verwalten.

Hierzu hat das Polizeipräsidium Bremen mitgeteilt, daß aus seiner Sicht keine Bedenken gegen die von mir vorgeschlagene Verfahrensweise bestehen, aus

Gründen einer effizienten Vorgangsverwaltung jedoch die Speicherung der Personendaten in ISA zunächst (d. h. bis zum Abschluß des Strafverfahrens) erforderlich sei.

Ich beabsichtige, dem Senator für Inneres und Sport vorzuschlagen, entsprechend der technischen Lösung im Staatsschutzbereich einen abgeschotteten Bereich in ISA für solche Fälle einzurichten. Spätestens mit der Einführung von ISA-D (s. a. o. Ziffer 5.1.1) muß ohne eine solche Lösung grundsätzlich auf eine Speicherung in ISA verzichtet werden.

5.1.4 Multifunktionale PC-Nutzung im Polizeiführungsstab

Mit der Abtrennung des Polizeipräsidiums von dem damaligen Stadt- und Polizeiamt und der Neuorganisation des Polizeiführungsstabes ist eine weitgehende Ausstattung dieses Bereiches mit Personalcomputern verbunden. Der Einsatz von ca. 20 PC ist hierfür beantragt und von mir beratend begleitet worden. Diese werden derzeit noch als isolierte PC eingesetzt. Für einen Teil der beantragten PC besteht aber die Absicht, diese zukünftig zu vernetzen. Neben der Textverarbeitung sollen dabei auch Datenbankanwendungen eingesetzt werden, etwa zur Haushaltsführung, zur Verwaltung von Disziplinarmaßnahmen oder zur Personalplanung, so z. B. zur Personalbedarfsplanung, zur Aufstellung von Einsatzplänen, zur personellen Ausstattung der Polizeireviere und zur Koordinierung von Fortbildungsmaßnahmen.

Betroffen von dieser Datenverarbeitung sind in erster Linie die Polizeibeamten. Zur Wahrung des Datenschutzes bei Dienstverhältnissen hatte ich daher insbesondere darauf zu achten, daß die Umsetzung der beabsichtigten Verarbeitungsziele nicht über das erforderliche Maß hinausgeht und daß die schutzwürdigen Belange der Betroffenen nicht beeinträchtigt werden. Es galt insbesondere zu verhindern, daß Daten, deren Verarbeitung zur Erfüllung bestimmter Aufgaben erforderlich ist, durch Verknüpfung oder den Einsatz von Recherchefunktionen zweckentfremdet beispielsweise zur Leistungs- und Verhaltenskontrolle genutzt werden können. Daher habe ich strenge Regelungen zur Zweckbindung der Datenverarbeitung und zur Löschung der gespeicherten Daten sowie deren Umsetzung durch technische und organisatorische Maßnahmen verlangt.

5.2 Ausländer

5.2.1 Asylbewerber

5.2.1.1 Erkennungsdienstliche Behandlung (s. a. 14. Jahresbericht, Ziffer 2.2.5.3)

Am 30. Juni 1992 wurde das neue Asylverfahrensgesetz (BGBl I S.1126) verkündet, das in seinen wesentlichen Teilen am 01. April 1993 in Kraft tritt. Zu dem Entwurf habe ich bereits in meinem letzten Jahresbericht (Ziffer 2.2.5.4) Stellung genommen. Alle wesentlichen datenschutzrechtlichen Bedenken und Forderungen (s. a. Beschluß der Konferenz der Datenschutzbeauftragten vom 28. 04. 1992, Ziffer 16.2) wurden nicht aufgegriffen. Neben den Datenverarbeitungsvorschriften ohne ausreichende Normenklarheit und Bestimmtheit wurden auch die Regelungen über die erkennungsdienstliche Behandlung aller Asylbewerber — unabhängig von Zweifeln an ihrer Identität — unverändert aufgenommen. Sie bilden nunmehr den rechtlichen Rahmen für die Erweiterung des **Automatisierten Fingerabdrucksystems (AFIS)** der Polizei auch für die Zwecke der Ausländer- und Asylbehörden.

Mit AFIS werden zukünftig alle Asylbewerber im Lande Bremen mit Ausnahme von kleinen Kindern im Polizeipräsidium Bremen und in einer Datei des INPOL erfaßt. Wenn dies auch in einer separaten Datei erfolgen soll, so haben doch alle angeschlossenen Polizeieinrichtungen Zugang auch dann, wenn kein Zusammenhang mit polizeilicher Tätigkeit besteht, sondern sie zu anderen Zwecken erkennungsdienstliche Verfahren aufrufen. Die Ausländerbehörden selbst erhalten paradoxerweise keinen Zugriff auf die von ihnen zu verantwortenden Daten und müssen sich in Fragen der Identitätsprüfung von Asylbewerbern stets der Hilfe der Polizei bedienen.

Wie in diesem System die Prinzipien der Zweckbindung und der Erforderlichkeit bei der Datenübermittlung eingehalten werden können, ist nicht erkennbar. Auch erneuere ich meine Kritik an der Führung einer Informationsdatenbank, die nach polizeilichen Gesichtspunkten angelegt wurde, nach der Rechtslage aber allein

asyl- und ausländerrechtlichen Zwecken dienen soll. Da die erkennungsdienstliche Behandlung von Asylbewerbern nur verhindern soll, daß eine Person sich mit mehreren Namen registrieren läßt, rechtfertigt dies nur eine auf die Ausländerbehörden beschränkte Datei. Eine Speicherung der Identitätsunterlagen hätte daher bei den Ausländerämtern bzw. beim Ausländerzentralregister (AZR) — nach Schaffung einer entsprechenden gesetzlichen Grundlage — erfolgen müssen.

Im ersten Quartal 1993 soll das AFIS im Polizeipräsidium für das Land Bremen installiert werden. Ich werde dann die konkrete Wirkungsweise prüfen und bewerten. Dies gilt auch für andere Datenabgleiche und -flüsse im Zusammenhang mit der Anwendung des neuen Asylverfahrensgesetzes. Aufmerksam beobachten werde ich auch das Projekt **EURODAC**, das der Erfassung und dem Abgleich der Fingerabdrücke von Asylbewerbern im Rahmen der EG dienen soll.

5.2.1.2 Fall: Bonitätseinschätzung an Mietwagenverleiher

Von einem Journalisten wurde ich auf Auskünfte über einen Asylbewerber aus dem Ausländeramt an einen privaten Autovermieter aufmerksam gemacht. Die Aufklärung des Falles gestaltete sich sehr schwierig, weil die Mitarbeiter des Ausländeramtes von den Recherchen der Medien erfahren hatten. Im Ergebnis konnte ich jedenfalls nicht feststellen, daß konkrete Informationen über einen bestimmten Ausländer weitergegeben worden waren. Ein Sachbearbeiter hatte offensichtlich lediglich eine pauschale Einschätzung abgegeben, wonach er generell einem Asylbewerber keinen PKW vermieten würde. Ich habe dem Ausländeramt empfohlen, auch diese Pauschalerklärungen zukünftig zu unterlassen.

Bei der Überprüfung dieses Falles stellte ich einige strukturelle Datensicherungsmängel im internen Dienstbetrieb und bei der Aktenhaltung fest. So kann jeder Mitarbeiter über seinen eigenen Arbeitsbereich hinaus an jede Ausländerakte herankommen, ohne daß darüber ein Nachweis geführt wird. Telefonische Auskünfte werden nicht dokumentiert oder anderweitig nachgewiesen. Auch können zu viele Mitarbeiter das bundesweite Ausländerzentralregister abrufen. Diese Organisationsdefizite sind zum Teil durch Arbeitsüberlastung und zu kurze Einarbeitungs- bzw. Ausbildungszeit der Mitarbeiter bedingt. Der Amtsleiter hat den Vorfall sofort zum Anlaß genommen, eine umfassende Belehrung über das korrekte Informationsverhalten der Mitarbeiter nach außen durchzuführen.

Ich habe zugesagt, an der Lösung der im Ausländeramt bestehenden Datenschutzprobleme mitzuarbeiten.

5.2.2 Automation im Ausländeramt

Vor dem Eindruck der hochschnellenden Asylbewerberzahlen im Lande Bremen hatte der Senat beschlossen, für die Einführung der automatisierten Datenverarbeitung im Ausländeramt des Stadtamtes Bremen erhebliche finanzielle Mittel bereitzustellen. Nachdem daraufhin Ende September 1991 ein Anschluß an das Ausländerzentralregister — ohne entsprechende Rechtsgrundlage (s. a. 14. Jahresbericht, Ziffer 2.2.5.1) — eingerichtet wurde, erhielt das Stadtamt den Auftrag, ein Konzept zu entwickeln, das die Arbeitsverfahren und -abläufe im Ausländeramt sowie die Kommunikation mit anderen öffentlichen Stellen automatisiert unterstützt. Dazu wurden mehrere DV-Verfahren anderer Gebietskörperschaften begutachtet. Diese berücksichtigen jedoch einerseits die datenschutzrechtlichen Vorgaben des Ausländergesetzes und des Bremischen Datenschutzgesetzes nicht ausreichend; denn sie basieren noch auf älteren Anwendungsverfahren, die Datenverarbeitungssegmente enthalten, die durch die Rechtslage nicht mehr erlaubt sind und deshalb erst entsprechend angepaßt werden müßten (wenn eine Anpassung überhaupt möglich ist). Andererseits vollziehen sie die zwischenzeitlich geänderte Aufgabenabgrenzung zwischen dem Bundesamt für die Anerkennung ausländischer Flüchtlinge einschließlich dessen Außenstellen und den übrigen Ausländerbehörden nur unvollständig nach. So enthalten die Anwendungsprogramme insbesondere Module, die auf das Asylverfahren zugeschnitten sind, künftig aber von den Ausländerbehörden nicht mehr benötigt werden.

Ich habe meine Beteiligung an der notwendigen umfassenden Neukonzeption des DV-Verfahrens zugesagt.

5.3 Verfassungsschutz

5.3.1 PC-Netz im Landesamt (s. a. 14. Jahresbericht, Ziffer 2.2.1.3, Ergebnis)

Wie in meinem letzten Tätigkeitsbericht dargestellt, hatte das Landesamt für Verfassungschutz (LfV) geplant, die Terminalanbindung an das bundesweite NADIS-System des Verfassungsschutzes durch ein PC-Netz zu ersetzen. Dieses Netz ist mittlerweile installiert, und ich hatte Gelegenheit, die Installation zu besichtigen.

Im Einsatz sind vier PC, wovon einer die Server-Funktion übernimmt und somit die Verbindung zu dem NADIS-Rechner beim Bundesamt für Verfassungsschutz herstellt. Die anderen PC werden mittels eines Terminal-Emulationsprogramms als NADIS-Stationen eingesetzt und können darüber hinaus als Einzelplatzrechner zur Textverarbeitung und zur Tabellenkalkulation genutzt werden.

Ich hatte daraufhin gefordert, eine Sicherungssoftware derart einzusetzen, daß

- die Bereiche für die Terminal-Emulation und für die PC-spezifischen Anwendungen voneinander getrennt sind;
- die Anwender keinen Zugang zum Betriebssystem erhalten;
- die Diskettenlaufwerke gesperrt werden;
- die Zugangsberechtigung zum Server nur für Systemverwalter eingerichtet wird;
- die NADIS-Anmeldungen und -Abmeldungen landesseitig protokolliert werden.

Mittlerweile hat mir das LfV bestätigt, daß die Sicherungssoftware entsprechend installiert sei. Unter diesen Voraussetzungen bestehen aus technischer und organisatorischer Sicht keine Bedenken gegen den Einsatz des PC-Netzes.

5.3.2 Sicherheitsüberprüfungen

Bereits im Jahr 1988 habe ich den Senator für Inneres darauf hingewiesen, daß das Verfahren der Sicherheitsüberprüfungen einer gesetzlichen Grundlage bedarf (s. a. 11. Jahresbericht, Ziffer 5.2.1.1). Schon damals habe ich auf eine eigene Regelungskompetenz des Landes verwiesen und meine Bereitschaft erklärt, bei der gesetzlichen Ausgestaltung der Sicherheitsüberprüfung mitzuwirken und in einem Kurzaufriß wesentliche Bestandteile einer landesgesetzlichen Regelung benannt.

Bei der Behandlung dieses Themas durch den Datenschutzausschuß der Bremischen Bürgerschaft am 13. Okt. 1989 erklärte ein Vertreter des Senators für Inneres, das Innenressort werde gemeinsam mit der Deputation für Inneres prüfen, ob Bremen eine eigene gesetzliche Regelung erlassen müsse, wenn der Bundesgesetzgeber untätig bleibe. Der Datenschutzausschuß nahm dieses zur Kenntnis und erwartete von dem Senator für Inneres einen Bericht zum Frühjahr 1990; dieser steht noch aus.

Die Konferenz der Datenschutzbeauftragen des Bundes und der Länder hat sich mit dem Problem der Sicherheitsüberprüfungen in ihrem Beschluß zum „Datenschutz im Recht des öffentlichen Dienstes" vom 26./27.Sept. 1991 (s. a. 14. Jahresbericht, Ziffer 6.) erneut befaßt und ebenfalls eindeutige gesetzliche Regelungen gefordert.

Ein solches Gesetz muß — um nur die wichtigsten Gesichtspunkte hervorzuheben — im einzelnen präzisieren, in welchem Umfang die Angaben der überprüften Personen verarbeitet, d. h. insbesondere nachrecherchiert werden. Die Rechte des Betroffenen auf Anhörung, Gegenäußerung und einen schriftlichen Bescheid sind zu gewährleisten. Sicherheitsbereiche müssen auf das unbedingt erforderliche Maß eingeschränkt werden. Sind nicht-öffentliche Stellen betroffen, dürfen ihnen keine Einzelerkenntnisse übermittelt werden.

Mitte Februar 1993 erhielt ich den vom Bundeskabinett kurz zuvor beschlossenen Entwurf eines Sicherheitsüberprüfungsgesetzes. Er betrifft nur das Geheimschutzverfahren für den Bundesbereich und soll offensichtlich in großer Eile verabschiedet werden. Der vorgelegte Text berücksichtigt wesentliche Datenschutzforderungen nicht. In meinen Stellungnahmen gegenüber dem Senator für Inneres und Sport und dem Senator für Justiz und Verfassung habe ich hierauf hingewiesen und darum gebeten, meine Änderungsvorschläge im Bundesrat zu unterstützen.

Nachdem der Bund mit diesem Gesetz nur seinen Verantwortungsbereich regeln will, ist es Sache des Landes Bremen, für seine Bediensteten eigene gesetzliche Regelungen zu schaffen.

5.3.3 Kontrollbefugnis des LfD (s. a. 14. Jahresbericht, Ziffer 2.2.1.1. Ergebnis)

Im Mai 1992 hatte ich mit dem Landesamt für Verfassungsschutz (LfV) einen Prüftermin vereinbart und angekündigt, eine Reihe an mich gerichteter Bürgereingaben zu überprüfen. Am Prüftag gab es Schwierigkeiten im Hinblick auf den Zugang zu den Amtsräumen und zum NADIS-Bildschirm.

Gegenüber dem Senator für Inneres und Sport habe ich daraufhin auf die mir gesetzlich zustehenden Zutritts-, Akteneinsichts- und sonstigen Prüfrechte hingewiesen. So habe ich z. B. gem. § 27 Abs. 3 Nr. 2 Bremisches Datenschutzgesetz (BrDSG) das Recht, das LfV unangemeldet aufzusuchen und die Diensträume zu betreten.

Der Senator für Inneres und Sport hat daraufhin das LfV angewiesen, in jedem Fall das Zutrittsrecht des Landesbeauftragten für den Datenschutz zu allen Dienst- und Geschäftsräumen der Behörde (§ 27 Abs. 3 Satz 2 Nr. 2 BrDSG) und seine übrigen Rechte bei der Einsichtnahme in Unterlagen, Akten, gespeicherte Daten, Datenverarbeitungsprogramme und Programmunterlagen (§ 27 Abs. 3 Satz 2 Nr. 1 BrDSG) zu beachten. Dieser Punkt ist damit für mich erledigt.

Ungeklärt blieb aber noch, ob ich nur im Zuge der Prüfung von Eingaben von Bürgern vom LfV mitgeteilt bekomme, ob zu Personen Datensätze anderer NADIS-Teilnehmer vorliegen und welches Amt jeweils als speichernde Stelle fungiert oder ob mir auch bei Querschnittsprüfungen ein entsprechender vollständiger Einblick auf den NADIS-Bildschirm zu gewähren ist. Die Frage war also, ob der Landesbeauftragte für den Datenschutz bzw. sein bei der Prüfung anwesender Vertreter in jedem Falle Einblick nehmen darf in den NADIS-Terminal, um feststellen zu können, ob Daten zu einer Person auch von anderen Landesämtern oder vom Bundesamt für Verfassungsschutz eingespeichert worden sind.

Da diese Frage zwischen mir und dem Senator für Inneres und Sport kontrovers war, hat der Datenschutzausschuß die Problematik beraten.

Als Ergebnis kann festgehalten werden, daß anerkannt wurde, daß die materielle Prüfbefugnis für die von anderen Verfassungsschutzbehörden eingespeisten Daten dem jeweiligen Landesdatenschutzbeauftragten bzw. dem Bundesdatenschutzbeauftragten obliegt, daß es aber notwendig ist, feststellen zu können, welche anderen Verfassungsschutzbehörden Daten zu der jeweiligen Person eingespeist haben. Für gemeinsame Dateien im Sinne von § 6 Bundesverfassungsschutzgesetz enthält die Gesetzesbegründung zu dieser Vorschrift die Aussage, daß speichernde Stellen hinsichtlich des gesamten Datenbestandes alle (jeweils) beteiligten Verfassungsschutzbehörden sind. Der Abruf von Daten ist nach der Gesetzesbegründung als Nutzung und nicht als Abruf im automatisierten Verfahren zu qualifizieren. Eine Erweiterung der inhaltlichen Kontrollkompetenz der einzelnen für die beteiligten speichernden Stellen zuständigen Datenschutzbeauftragten kann und soll daraus nicht abgeleitet werden, wohl aber das Recht zur Kenntnisnahme.

Das Recht auf informationelle Selbstbestimmung ist umfassend. Die Datenschutzkontrolle, die dieses Recht sicherstellen soll, muß daher bei der Kontrollkompetenz eine Entsprechung finden. Nur bei der Inaugenscheinnahme und Berücksichtigung aller Umstände unter Zuhilfenahme aller Informationen, die auch dem LfV zur Verfügung stehen, läßt sich die Datenverarbeitung des Amtes richtig beurteilen. Deshalb ist ein uneingeschränkter Einblick auf alle in NADIS gespeicherten Daten durch mich unerläßlich. Meine Umfrage in anderen Bundesländern hat ergeben, daß dort in gleicher Weise verfahren wird. Der Senator für Inneres und Sport hat daraufhin anerkannt, daß unabhängig davon, ob einzelne Beschwerden Betroffener vorliegen, mir ein uneingeschränktes Einsichtsrecht in die in NADIS gespeicherten Daten zusteht. Dieses umfassende Einsichtsrecht ist nicht deckungsgleich mit meinem materiellen Prüfungsrecht in bezug auf die Rechtmäßigkeit der gespeicherten Daten. Dieses beschränkt sich auf die vom LfV Bremen in NADIS eingespeicherten Daten.

5.4 Straßenverkehr

5.4.1 Meldung von Drogenkonsumenten an die Führerscheinstelle

Der Senator für Inneres und Sport hatte mir den Entwurf eines Erlasses vorgelegt, wonach anläßlich einer Verkehrskontrolle oder Verkehrserhebung beim Führen eines Kraftfahrzeugs unter offensichtlichem Drogeneinfluß angetroffene Personen zunächst an der Weiterfahrt zu hindern sind. Nach Ansicht der senatorischen Behörde bestehen bei Kraftfahrzeugführern, die Cannabisprodukte und/oder Betäubungsmittel illegal konsumieren, erhebliche Zweifel an der Eignung zum Führen von Kraftfahrzeugen. Die Offensichtlichkeit des Drogeneinflusses könne sich aus Ausfallerscheinungen, z. B. verkehrswidriger Fahrweise, Verwirrtheitszuständen oder physiognomischen Anzeichen wie stecknadelkopfgroßen Pupillen ergeben. Außerdem bestehe erfahrungsgemäß ein enger Zusammenhang zwischen dem Besitz kleiner konsumgerechter Einheiten und deren Konsum. Wegen der mit dem Drogenmißbrauch verbundenen Veränderungen der Persönlichkeit und der Herabsetzung und Verzerrung der Wahrnehmungs- und Reaktionsfähigkeit bestünden besondere Gefahren für die übrigen Verkehrsteilnehmer. Aus diesem Grunde hat die Polizei in diesen Fällen die zuständige Führerscheinstelle zu unterrichten, damit die Verwaltungsbehörde die erforderlichen Maßnahmen (Begutachtung und ggf. Entziehung der Fahrerlaubnis) treffen kann.

Als Rechtsgrundlage kommt § 33 Abs. 1 Satz 1 Bremisches Polizeigesetz (BremPolG) in Frage. Danach darf die Polizei personenbezogene Daten an sonstige öffentliche Stellen übermitteln, wenn dies zur Erfüllung polizeilicher Aufgaben unerläßlich ist. Zu den originären polizeilichen Aufgaben gehört nach § 1 Abs. 1 BremPolG, Gefahren für die öffentliche Sicherheit abzuwehren.

Die Erforderlichkeit einer Meldung von Rauschgiftkonsumenten an die Führerscheinstelle basiert auf dem Gutachten „Krankheit ohne Kraftverkehr" des Gemeinsamen Beirates für Verkehrsmedizin beim Bundesminister für Verkehr und beim Bundesminister für Jugend, Familie und Gesundheit (Heft 67/85 der Schriftenreihe des Bundesministers für Verkehr, S. 19 ff). Danach beeinträchtigt der Konsum von Rauschmitteln die Fahrtauglichkeit in schwerwiegender Weise. Insbesondere für sog. Halluzinogene, zu denen das Haschisch zu rechnen ist, ist zu beachten, daß gefährliche psychische Veränderungen oder Leistungsschwächen nicht nur im akuten Rauschzustand auftreten, sondern auch nach Abklingen der Rauschsymptomatik in der Phase der Nachwirkungen. Speziell bei Haschisch kann es auch bei einmaliger Zufuhr nach einem symptomfreien Intervall von mehreren Tagen zu einem Wiederaufflammen der Rauschsymptome (Echo-Rausch) kommen. Ein unvorhersehbar eintretender Echo-Rausch führt dazu, daß der Eintritt eines die Fahrtauglichkeit ausschließenden Rauschzustandes für den Haschischkonsumenten nicht beherrschbar wird. Diese zeitliche Unbeherrschbarkeit rechtfertigt bei Haschischkonsumenten die Annahme, daß sie zum Führen von Kraftfahrzeugen generell nicht geeignet sind, auch wenn die Einnahme des Rauschmittels jeweils nur zum zeitweisen Ausschluß der Fahrtauglichkeit führt.

Nach diesem Gutachten ergeben sich mithin erhebliche Zweifel an der Fahrtauglichkeit des Haschischkonsumenten, so daß eine Gefahr für andere Verkehrsteilnehmer grundsätzlich zu unterstellen ist. Demzufolge stellt die Meldung von Personen, bei denen im Straßenverkehr Haschischkonsum bzw. -besitz festgestellt worden ist, eine Maßnahme zur Gefahrenabwehr dar, weil nur dadurch der Führerscheinstelle ermöglicht wird, die Fahrtauglichkeit des Drogenkonsumenten festzustellen.

Da mir keine gegenteiligen Erkenntnisse über den Zusammenhang zwischen Drogenkonsum und Fahrtauglichkeit vorliegen, habe ich meine anfänglichen Bedenken gegen die Datenweitergabe an die Führerscheinstelle nicht mehr aufrechterhalten. Der Erlaß ist am 10. Dezember 1992 in Kraft getreten.

5.4.2 Fall: Nebentätigkeits-Kontrolle durch Aufsichtsbehörde

Der Senator für Inneres und Sport hat als Aufsichtsbehörde nach dem Fahrlehrergesetz (FahrlG) eine Fahrschule überprüft und dabei festgestellt, daß ein nebenberuflich tätiger Fahrlehrer hauptberuflich Beamter ist. Aus den Aufzeichnungen der Fahrschule ergaben sich für die Aufsichtsbehörde Zweifel, ob die geleisteten Fahrstunden des nebenberuflichen Fahrlehrers mit seiner Nebentätigkeitsgenehmigung übereinstimmen. Aus diesem Grunde hat sie den Dienstherrn über den eventuellen Verstoß gegen die Nebentätigkeitsverordnung informiert.

Der Senator für Inneres und Sport begründet die Datenweitergabe damit, bei Überschreiten einer Nebentätigkeitsgenehmigung sehe er es im Interesse der Verkehrssicherheit als seine Pflicht an, die Beschäftigungsdienststelle zu informieren. Dies sei erforderlich, da die Aufsichtsbehörde nicht beurteilen könne, ob der Betroffene an seinem Arbeitsplatz so ausgelastet ist, daß die Überschreitung der Nebentätigkeitsgenehmigung dazu führt, daß er zu einer ordnungsgemäßen Fahrausbildung nicht mehr in der Lage ist. Die Beschäftigungsdienststelle habe unter Berücksichtigung der Grundsätze der Verhältnismäßigkeit und nach eigenem Ermessen zu entscheiden, inwieweit sie gegen den Betroffenen vorgeht.

Im übrigen vertritt die Aufsichtsbehörde die Auffassung, eine Nebentätigkeitsgenehmigung beinhalte immer, daß der Betroffene neben seiner hauptberuflichen Tätigkeit nur in einem Zeitrahmen eine andere Tätigkeit zusätzlich ausführen kann, der ausschließt, daß seine hauptberufliche Tätigkeit darunter leidet. Außerdem sei das Erfordernis einer Nebentätigkeitsgenehmigung sinnlos, wenn sie nicht überprüft und das Überprüfungsergebnis nicht mitgeteilt werden dürfe.

Ich habe den Senator für Inneres und Sport darauf hingewiesen, daß die Datenweitergabe durch die Aufsichtsbehörde an den Dienstherrn des nebenberuflich tätigen Fahrlehrers gegen das Zweckbindungsprinzip verstößt. Die Aufsichtsbehörde hat nach § 33 Abs. 2 Satz 2 FahrlG nur die Befugnis, in die vorgeschriebenen Aufzeichnungen Einsicht zu nehmen. § 18 Abs. 2 FahrlG regelt abschließend, welche Aufzeichnungen der Inhaber einer Fahrschule über die Fahrlehrer vorzunehmen hat. Danach ist er verpflichtet, für jeden Fahrlehrer täglich die Anzahl der Fahrstunden und die Gesamtdauer des praktischen Fahrunterrichts in Minuten aufzuzeichnen. Diese Regelung schließt Hinweise auf Nebentätigkeiten der Fahrlehrer aus.

Gleichwohl hat die Aufsichtsbehörde Erkenntnisse darüber erhalten und diese an den Dienstherrn des betroffenen Fahrlehrers wegen eines eventuellen Verstoßes gegen die Nebentätigkeitsverordnung unzulässigerweise weitergegeben, obwohl personenbezogene Daten nach § 12 Abs. 1 Bremisches Datenschutzgesetz (BrDSG) nur für Zwecke verarbeitet werden dürfen, für die sie erstmals gespeichert worden sind. Eine Befugnis zur Durchbrechnung dieses Zweckbindungsprinzips nach § 13 i. V. m. § 12 Abs. 2 und 3 BrDSG bestand nicht. Der Senator für Inneres und Sport hat sich noch nicht dazu geäußert, ob er die Praxis entsprechend meiner rechtlichen Würdigung geändert hat.

5.5 Statistik

5.5.1 Bevölkerungsstatistik (s. a. 12. Jahresbericht, Ziffer 2.2.5.2)

Bereits in meinem 12. Jahresbericht hatte ich mich ausführlich mit der Bevölkerungsstatistik und ihren Datenschutzproblemen beschäftigt. Auslöser damals waren Bemühungen in Bonn, das schon lange nicht mehr datenschutzrechtlichen Anforderungen entsprechende „Gesetz über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes" zu novellieren. Zu einer Novellierung ist es damals (1989/90) nicht gekommen. Dies ist bedauerlich, weil das aus dem Jahre 1980 stammende Gesetz so erhebliche Mängel enthält, daß seine Verfassungsmäßigkeit inzwischen wegen Ablaufs des sogenannten Übergangsbonus in Frage zu stellen ist.

Die datenschutzrechtlichen Mängel des Bevölkerungsstatistikgesetzes beziehen sich im wesentlichen auf folgende Punkte:

Das Gesamtsystem der bevölkerungsstatistischen Datenerhebungen muß hinsichtlich seiner Kohärenz und der Erforderlichkeit einzelner Statistiken oder Statistikteile überdacht werden. Ich habe z. B. Zweifel, ob neben einer funktionierenden, datenschutzkonformen Bevölkerungsstatistik, einem Mikrozensus und der neuen Wohnungsstatistik weiterhin eine allgemeine Volkszählung notwendig ist.

Auch einzelne Erhebungsteile der Bevölkerungsstatistik (z. B. Totgeburten, rechtskräftige Urteile in Ehesachen) und verschiedene Erhebungsmerkmale (z. B. Fragen nach der Religionsgehörigkeit, nach ehelicher/nicht-ehelicher Geburt, nach der Zahl der zuvor lebend oder tot geborenen Kinder) stehen hinsichtlich ihrer Erforderlichkeit und damit ihrer verfassungsrechtlichen Zulässigkeit in Zweifel. Das Bundesverfassungsgericht hat in seiner Volkszählungsentscheidung 1983 erklärt, daß der Gesetzgeber schon bei der Anordnung der Auskunftspflicht prüfen muß, ob diese für den Betroffenen die Gefahr einer sozialen Abstempelung

hervorrufen kann und ob das Ziel der Erhebung nicht auch durch eine anonymisierte Datenerhebung erreicht werden kann.

Verfassungsrechtliche Probleme ergeben sich auch bei den Regelungen zur Auskunftspflicht (ausnahmslos bei allen Daten) und bei der Verflechtung von amtlicher Statistik und Verwaltungsvollzug bei der Erhebung der Daten. Sekundärstatistische Datenerhebungen finden ihre Grenzen im Bestand der Verwaltungsdaten. Daten, die für das Verwaltungshandeln nicht benötigt werden, dürfen von der Verwaltung (z. B. dem Standesbeamten) für Zwecke der Bevölkerungsstatistik nicht bei den Betroffenen oder den Anzeigenden — sogar mit Auskunftspflicht — erhoben werden.

Schließlich ergeben sich für das Statistische Landesamt Bremen Datenschutzprobleme beim Vollzug dieses Gesetzes. Das Statistische Landesamt Bremen ist sowohl Landesamt und als solches mit der Durchführung der Bundesstatistik betraut. Zugleich ist es auch kommunalstatistisches Amt der Stadtgemeinde Bremen. Beide Bereiche sind innerhalb des Statistischen Landesamtes nicht getrennt, mit der Folge, daß der gesamte bevölkerungsstatistische Datenfluß und die aufgrund melderechtlicher Regelungen zufließenden Meldedaten (regelmäßige Bestandsabzüge des bremischen Melderegisters für kommunalstatistische Zwecke) in einem Arbeitsabschnitt des Amtes zusammenfließen. Der Bundesgesetzgeber geht bei seinen Regelungen von einer klaren Trennung zwischen den Ebenen der statistischen Ämter (Bund, Länder, Gemeinden) aus. Anders sind die z. T. differenzierten Regelungen zur Übermittlung von Einzelangaben aus den statistischen Erhebungen an die kommunalstatistischen Ämter oder Stellen nicht zu erklären. Da gerade im kommunalen Bereich die Grenzen statistischer Datennutzung fließend sind und wegen des besonders großen Zusatzwissens und der kleinräumigen Gliederung des Datenmaterials leicht die Grenzen der Deanonymisierung erreicht werden, stellt die Aufhebung des funktionellen Trennungsprinzips im Statistischen Landesamt Bremen ein potentielles Datenschutzrisiko dar.

Obwohl der Senat eine Trennung zwischen Landes- und Kommunalstatistik nicht für erforderlich hält, bleibe ich bei meiner Auffassung, daß sie verfassungsrechtlich geboten ist. Aus der funktionellen Aufgabenbündelung im Statistischen Landesamt resultieren Zweifel an der gesetzeskonformen Vollziehbarkeit des Bevölkerungsstatistikgesetzes in Bremen.

Im Berichtsjahr erhielt ich einen weiteren Referentenentwurf eines „Gesetzes über die Bevölkerungsstatistik" zur Stellungnahme. Dieser Entwurf unterscheidet sich von den Vorläufern aus der letzten Legislaturperiode des Deutschen Bundestages nur wenig. Gegenüber dem geltenden Gesetz präzisiert er zwar das gesamte Erhebungsprogramm und die bei den verschiedenen Erhebungsteilen verlangten Erhebungsmerkmale, ferner die Bestimmungen zur Auskunftspflicht und zur Übermittlung von Daten, beläßt es aber im übrigen beim bisherigen Konzept. In Teilbereichen erfolgt sogar eine Ausweitung der Erhebungsmerkmale. Im Hinblick darauf, daß

— Abstriche am Erhebungsprogramm und an den Erhebungsmerkmalen nicht vorgenommen wurden,

— weiterhin Daten über den Bedarf der Verwaltung hinaus mit Auskunftspflicht erhoben werden sollen und

— Datenschutzprobleme beim Vollzug dieses Gesetzes in Bremen bestehen,

habe ich mich gegenüber dem Senator für Inneres und Sport kritisch zu diesem Gesetzentwurf geäußert. Ich hoffe, daß der Regierungsentwurf die Mängel des Referententextes beseitigt und aus Datenschutzsicht befriedigende Ergebnisse erzielt werden.

5.5.2 Wohnungsstatistik

Im Berichtsjahr hat die Bundesregierung dem Bundesrat erneut den Entwurf eines „Gesetzes über gebäude- und wohnungsstatistische Erhebungen (Wohnungsstatistikgesetz)" zugeleitet. Der Bundesrat hat zu dem Gesetzentwurf Stellung genommen; zusammen mit der Gegenäußerung der Bundesregierung zu dieser Stellungnahme des Bundesrates wurde der Gesetzentwurf Mitte des Jahres dem Bundestag zur Beratung und Beschlußfassung vorgelegt. Im Januar 1993 wurde das Wohnungsstatistikgesetz vom Deutschen Bundestag, im Februar 1993 auch vom Bundesrat beschlossen. Es tritt am Tag nach der Verkündung, die zum Zeitpunkt des Redaktionsschlusses dieses Berichts noch nicht erfolgt ist, in Kraft.

Mit dem Gesetz wird flächendeckend eine Gebäude- und Wohnungszählung in den neuen Bundesländern einschließlich Ostberlin sowie eine Gebäude- und Wohnungsstichprobe (1 %) im gesamten Bundesgebiet angeordnet. Berichtszeitpunkt für die Stichprobenerhebung ist der 30. 09. 1993, für die Zählung in den neuen Bundesländern der 30. 09. 1995. Erhebungseinheiten sind Gebäude mit Wohnraum, bewohnte Unterkünfte und Wohnungen. Bei der Wohnungsstichprobe werden im Vergleich zur Gebäude- und Wohnungszählung sehr viel mehr Angaben, speziell auch zu den Eigentümern und Nutzern der Wohnungen und zu den Haushalten in den Wohnungen, erhoben. Es besteht Auskunftspflicht; lediglich einige wenige Angaben sind freiwillig.

Ich hatte zu dem Gesetzentwurf einige kritische Anmerkungen gemacht. Sie bezogen sich insbesondere auf die Angaben, die von den Haushalten und den einzelnen Haushaltsmitgliedern verlangt werden, und auf die Übermittlung von Einzelangaben aus der Erhebung in den neuen Bundesländern an die statistischen Ämter oder Stellen der dortigen Gemeinden und Gemeindeverbände. Meine Anregungen flossen jedoch nicht mehr in die Beratungen des Bundesrates ein.

5.5.3 Bewährungshilfestatistik/Strafverfolgungsstatistik

Keine gesetzliche Grundlage gibt es bisher für die Führung der Bewährungshilfestatistik. Sie ist eine bundesweit abgestimmte regelmäßige Statistik, bei deren Erstellung von den Justizbehörden Einzelangaben auf Zählkarten erhoben und ohne Namen der Betroffenen an das Statistische Landesamt weitergegeben werden. Die in den Statistischen Landesämtern aufbereiteten Angaben werden an das Statistische Bundesamt weitergeleitet, wo sie zu einem Bundesergebnis zusammengefaßt werden.

In Bremen wird die Bewährungshilfestatistik lediglich aufgrund einer allgemeinen Verfügung des Senators für Justiz und Verfassung durchgeführt. Sie bedarf aber einer gesetzlichen Grundlage, die die Datenerhebung bei den Justizbehörden sowie die nachfolgenden Datenübermittlungs- und aufbereitungsvorgänge umfassend regelt. § 11 Landesstatistikgesetz, der die Befugnis zur Erstellung von Geschäftsstatistiken gibt, reicht für diese regelmäßige Statistik nicht aus, da die Daten nicht im Verwaltungsvollzug und aus dem Verwaltungsdatenbestand erhoben werden.

In den Jahren 1989 und 1990 gab es verschiedene Gesetzentwürfe des Bundesministers der Justiz zu dieser Thematik. Sie wurden aber in der alten Legislaturperiode des Deutschen Bundestages nicht mehr verabschiedet. Diese Gesetzentwürfe bezogen auch weitere im Zusammenhang mit der Strafjustiz stehende Datenerhebungen ein. Der Senator für Justiz und Verfassung ist aufgefordert, im Bundesrat eine Initiative zur baldigen Vorlage eines Gesetzentwurfes zur Strafverfolgungsstatistik zu ergreifen.

5.6 Standesämter

5.6.1 Überholte Dienstanweisung

Die bremischen Standesämter (Bremen-Mitte, BremenNord, Bremerhaven) setzen schon seit längerem DV-Technik ein bei der Erledigung ihrer Aufgaben. Alle drei Standesämter haben sich dabei für das vom Verlag für Standesamtswesen Frankfurt am Main unter Mitwirkung des Bundesverbandes der deutschen Standesbeamten entwickelte und betreute Programmsystem AUTISTA (Automation im Standesamt) entschieden, das inzwischen bei vielen Standesämtern in der Bundesrepublik angewendet wird.

Bei meinen Stellungnahmen zu diesen DV-Anwendungen hatte ich darauf hingewiesen, daß Teile dieses Datenverarbeitungssystems datenschutzrechtlich nicht ausreichend begründet sind, weil sie nicht auf eine Rechtsvorschrift, sondern auf die „Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden" gestützt werden. Diese Dienstanweisung reicht als Zulässigkeitsnorm für die im Personenstandsrecht nicht abgesicherte Datenverarbeitung der Standesämter nicht aus. Der sog. Übergangsbonus für die Anpassung des Personenstandsgesetzes an die Anforderungen des Bundesverfassungsgerichtes in seinem Volkszählungsurteil von 1983 ist — auch nach Auffassung des Bremer Senats — längst abgelaufen. Die Zulässigkeitsnormen des Bremischen Datenschutzgesetzes können hier wegen des auf Bundesebene bestehenden bereichsspezifischen Regelungsbedarfs nicht als Grundlage herangezogen werden.

Die Novellierung des Personenstandsgesetzes — seit Jahren gefordert und immer wieder zugesagt — kommt in Bonn leider nicht voran. Die Novellierungsbemühungen sollen — nach neueren Aussagen des Bundesministeriums des Inneren — in dieser Legislaturperiode nicht fortgeführt werden. Dies ist aus datenschutzrechtlicher Sicht nicht hinnehmbar. Der Senat wird gebeten, über den Bundesrat die Verbesserung und Ergänzung der bereichsspezifischen Datenverarbeitungsregelungen im Personenstandsgesetz einzufordern.

5.6.2 Fall: Namensstreit um „Sascha" und das Briefgeheimnis

Einen erheblichen Verstoß gegen datenschutzrechtliche Vorschriften und gegen innerbehördliche Regelungen zum Umgang mit Poststücken mußte ich bei der Stadtverwaltung Bremerhaven feststellen. Was war passiert? Zunächst hatte sich ein junger Vater, der sich mit dem Standesamt Bremerhaven in einem Rechtsstreit über die Namenseintragung seines Sohnes in das Geburtenbuch befindet, bei mir darüber beschwert, daß Mitarbeiter des Magistrats ihm zwei für ihn bestimmte Briefe vorenthalten und geöffnet hätten. Zur Bekräftigung dieser Aussage legte er die Umschläge der Briefe, einen weiteren Umschlag, mit dem der Magistrat die Briefe an ihn weitergeleitet hatte, sowie als Inhalt der beiden Briefe zwei mit Eingangsstempeln versehene Schreiben vor. Während das eine Schreiben den Eingangsstempel des Standesamtes aufwies, war auf dem anderen neben dem Standesamtsstempel auch der Stempel der Ortspolizeibehörde enthalten. Auf den Umschlägen war zwar der korrekte Name des Petenten angegeben, die Adreßangaben waren jedoch unvollständig bzw. irreführend.

Durch meine Recherchen erfuhr ich, daß beide Briefe in die Poststelle der Ortspolizeibehörde gelangt und von dort — da sie einen Fall betrafen, der dem Mitarbeiter der Poststelle aus den Medien bekannt war — getrennt voneinander an das Standesamt weitergegeben worden waren. Nach den Angaben des Poststellenmitarbeiters wurde nur einer der beiden Briefe geöffnet und mit einem Eingangsstempel versehen. Der zweite Brief sei nicht geöffnet worden, sondern gleich an das Standesamt weitergegeben worden. Nach den Angaben des Standesamtes kamen allerdings beide Briefe geöffnet in der Poststelle des Amtes an. Ich konnte nicht mehr feststellen, wo der zweite Brief tatsächlich geöffnet wurde. Mit der Weiterleitung beider Briefe an das Standesamt wurde gegen die innerbehördlichen Regelungen für den Umgang mit Poststücken verstoßen, mit der Öffnung des zweiten Briefes auch gegen die Bestimmungen des Briefgeheimnisses. Korrekt wäre es gewesen, die Schriftstücke an die Bundespost zurückzugeben, damit diese die Briefe an den eigentlichen Empfänger weiterleiten oder, wenn ihr das nicht möglich ist, an den Absender zurückgeben kann.

Der zweite Brief wurde im Standesamt nicht nur geöffnet und mit einem Eingangsstempel versehen. Er wurde zusätzlich auch kopiert, in den Vorgang des Petenten aufgenommen und an den Senator für Inneres und Sport per Telefax weitergeleitet. Bevor das Schreiben dann gemeinsam mit dem ersten Brief, der mehrere Tage vorher im Standesamt eingetroffen war, an den eigentlichen Empfänger übersandt wurde, wurde in ihm, um darauf besonders hinzuweisen, eine Textpassage gekennzeichnet, die dem Leiter des Standesamtes zur Unterstützung der von ihm vertretenen Rechtsauffassung dient. Das Vorgehen des Standesamtes stellt einen erheblichen Verstoß gegen datenschutzrechtliche Bestimmungen dar. Der Magistrat hat den Verstoß zugegeben. Die Kopien, die sich in der Akte des Standesamtes befanden, wurden vernichtet. Der Senator für Inneres und Sport hat die ihm zugefaxte Kopie zwischenzeitlich mir zugeschickt; ich habe sie inzwischen vernichtet.

5.7 Gewerbe

5.7.1 Fall: Komplette Strafakten beim Stadtamt

Vor Erteilung einer Gewerbeerlaubnis hat die Behörde — soweit es sich nicht um eine nur anmeldepflichtige Gewerbeausübung handelt — die Zuverlässigkeit des Antragstellers zu beurteilen. Als Grundlage benötigt sie dazu neben den Unterlagen über die fachliche Eignung auch ein **polizeiliches Führungszeugnis**, das aus dem Bundeszentralregister erteilt wird. In das Führungszeugnis sind — je nach dem Grad der Zuverlässigkeitsvoraussetzungen, die für die Ausübung des Gewerbes erforderlich sind, und nach dem Zeitablauf einer Eintragung im Register — nur die Daten aufzunehmen, die noch nicht getilgt sind oder für die kein **Verwertungsverbot** besteht. Diese Registerdaten stammen aus den Vorgängen und Urteilen der Gerichte, Staatsanwaltschaften und in bestimmten Fällen auch von Verwaltungsbehörden.

In dem vorliegenden Fall — es ging um die Zulassung als Heilpraktiker — hat das Bundeszentralregister auf Anfrage des Stadtamtes Bremen unter Beachtung der gesetzlichen Tilgungs- und Verwertungssperren und der Zuverlässigkeitsvoraussetzungen ein eintragungsfreies Führungszeugnis erteilt. Das Stadtamt Bremen hat zusätzlich beim Polizeipräsidium Bremen um Mitteilung der Daten gebeten, die der Erteilung einer Gewerbeerlaubnis entgegenstehen könnten. Das Polizeipräsidium verwies auf einen Vorgang bei der Staatsanwaltschaft Bremen. Diese übersandte auf Anforderung des Stadtamtes alle Strafakten des Antragstellers.

Diese Strafakten enthielten nicht nur das Urteil, sondern auch alle Ermittlungsvorgänge mit einer Vielzahl von Angaben, die dem Bundeszentralregister gar nicht mitzuteilen sind bzw. in das Führungszeugnis gerade nicht aufgenommen worden waren, weil das Verwertungsverbot nach § 52 Bundeszentralregistergesetz (BZRG) bei seiner Ausfertigung beachtet worden war. Durch die Mitteilung des Polizeipräsidiums an das Stadtamt und die Weitergabe der kompletten Akten durch die Staatsanwaltschaft wurde das gesetzliche Verwertungsverbot unterlaufen. Der Bürger, der seine berufliche und private Lebensplanung sowie persönliche Rehabilitation darauf abstellt, daß die Daten über seine Verurteilung nach einer bestimmten Frist getilgt sind oder zumindest einem besonderen Verwertungsverbot unterliegen, wird von seiner Vergangenheit eingeholt.

Ich habe die Senatoren für Inneres und Sport sowie für Justiz und Verfassung gebeten, diese Praxis zu ändern. Der Senator für Justiz und Verfassung sieht hierfür derzeit keine Veranlassung. Das Stadtamt meint, es sei nicht nur nicht gehindert, die Strafakten auszuwerten, sondern im Gegenteil dazu verpflichtet, alle Informationen heranzuziehen und im Zulassungsverfahren zum Heilpraktikergewerbe zu nutzen. Diese Auffassung verkennt, daß das Verwertungsverbot im BZRG gerade darauf abzielt, daß bestimmte Daten nicht mehr zur Grundlage von Verwaltungsentscheidungen genommen werden können. Die „Richtlinien über das Straf- und Bußgeldverfahren" — denen ohnehin die erforderliche Rechtsnormqualität fehlt — können die Aktenübersendung durch die Staatsanwaltschaft ebenfalls nicht legitimieren; sie schließen eine Übermittlung aus, wenn eine Rehabilitationsmaßnahme gefährdet wird.

Anderes gilt nur für Daten über noch nicht gerichtlich abgeschlossene, also noch von der Polizei oder der Staatsanwaltschaft bearbeitete Vorgänge. Sie können in die Zuverlässigkeitabwägung für eine Gewerbeerlaubnis einbezogen werden. Nach der Verurteilung gelten dagegen allein die Regelungen des BZRG.

Ich werde die Angelegenheit weiter verfolgen. Dieser Fall belegt erneut, wie wichtig es ist, in die Gewerbeordnung endlich genaue Vorschriften für den Ablauf der Erlaubnisverfahren und die erforderlichen Datenflüsse aufzunehmen (s. o. 14. Jahresbericht, Ziffer 2.8.2).

6. Justiz

6.1 Aufbewahrungsbestimmungen für Schriftgut der Gerichte, der Staatsanwaltschaften und der Justizvollzugsbehörden

Auch die Aufbewahrung von Schriftgut greift in das informationelle Selbstbestimmungsrecht der Bürger ein, die von den erfaßten Informationen betroffen sind. Besondere Bedeutung gewinnen diese Regelungen vor dem Hintergrund, daß zunehmend auch im Bereich der Justiz automatisierte Datenverarbeitungssysteme eingeführt werden. Dabei wird für die Speicherdauer von Informationen in den automatisierten Systemen in der Regel auf die Aufbewahrungsbestimmungen für das Schriftgut verwiesen. Es ist deshalb erforderlich, daß Regelungen in diesem Bereich überprüft und konkretisiert werden.

Damit stellt sich auch die Frage, welche Rechtsqualität entsprechende Regelungen haben sollten. In Übereinstimmung mit anderen Datenschutzbeauftragten wäre es aus meiner Sicht angemessen, solche Bestimmungen auf eine gesetzliche Grundlage zu stellen. Derzeit richtet sich die Dauer der Aufbewahrung von Schriftgut der ordentlichen Gerichtsbarkeit sowie der Staatsanwaltschaften und der Justizvollzugsbehörden nach den zwischenzeitlich mehrfach geänderten Aufbewahrungsbestimmungen, die durch Beschluß der Konferenz der Justizverwaltungen des Bundes und der Länder in Düsseldorf vom 23./24. 11. 1971 festgelegt wurden. Diese Aufbewahrungsbestimmungen sind als Verwaltungsvorschriften anzusehen.

Unabhängig von der Frage der Normqualität ist jedoch zu überprüfen, ob die genannten Aufbewahrungsbestimmungen tatsächlich angemessene Regelungen beinhalten, die als Grundlage der Speicherdauer entsprechender Informationen

auch in automatisierten Systemen dienen können und die dem informationellen Selbstbestimmungsrecht ausreichend Rechnung tragen. Der Gesichtspunkt der Erforderlichkeit ist auch für die Dauer der Speicherung und damit verbunden die potentielle Nutzbarkeit der Daten und Akten zu Lasten der Betroffenen zu beachten.

Ich habe daher beim Senator für Justiz und Verfassung angeregt, die Aufbewahrungsbestimmungen der Justiz für das verwaltete Schriftgut im Lichte des Rechts auf informationelle Selbstbestimmung kritisch zu überprüfen und zu überarbeiten, um in geeigneten Fällen eine Verkürzung der Aufbewahrungsdauer herbeizuführen. Er hat mir daraufhin erklärt, die Landesjustizverwaltung Nordrhein-Westfalen habe die Federführung für die Überarbeitung der bundeseinheitlichen Aufbewahrungsbestimmungen übernommen; über die Ergebnisse wolle er mich unterrichten.

Wenig später hat er mir seine Regelungen zur Aufbewahrung, Aussonderung, Ablieferung und Vernichtung des Schriftguts der Gerichte, der Verwaltungs-, Sozial- und Finanzgerichtsbarkeit zugeleitet. Diese mit mir abgestimmte allgemeine Verfügung sieht Aufbewahrungsfristen von zwei, fünf, zehn und dreißig Jahren vor und ist im Amtsblatt der Freien Hansestadt Bremen vom 19. 01. 1993 veröffentlicht worden. Die zum Teil erfreulich kurzen Aufbewahrungsfristen vereinen dabei datenschutzrechtliche und verwaltungsökonomische Gesichtspunkte. Es bleibt zu hoffen, daß auch die bundeseinheitlich in Absprache befindlichen Aufbewahrungsbestimmungen der anderen Justizbereiche möglichst bald verbessert werden.

6.2 Automation bei der Strafverfolgung: Das SIJUS-Verfahren

Der Senator für Justiz und Verfassung plant eine flächendeckende Einführung der technikunterstützten Informationsverarbeitung bei der Staatsanwaltschaft Bremen. In der Endstufe sollen ca. 120 Arbeitsplätze von dem Verfahren betroffen sein. Die Systementscheidung ist dabei zugunsten einer Anlage der mittleren Datentechnik ausgefallen, da man sich hiervon die höchste Funktionalität verspricht. Der Vergleich der Techniklösungen in anderen Bundesländern hat zu einer Entscheidung für das System SIJUS-Straf geführt, das bereits in den Ländern Baden-Württemberg, Bayern und Niedersachsen eingeführt ist.

SIJUS-Straf soll dazu dienen, alle für die Staatsanwaltschaft anfallenden Verfahrensdaten in einem Datenbank-System bereitzuhalten und zur weiteren Verarbeitung zur Verfügung zu stellen. Es sollen insbesondere folgende Anforderungen erfüllt werden:

- die Aktenverwaltung durch die Geschäftsstelle,
- die Textverarbeitung bei gleichzeitiger Nutzung der in der Datenbank vorhandenen Daten,
- die Übernahme und Verarbeitung der Daten aus dem bremischen Polizei-Informationssystem ISA,
- der Datenaustausch mit anderen Dienststellen, z. B. Bundeszentralregister, Justizvollzugsanstalten, Einwohnermeldeämter,
- die Einbeziehung der Dezernenten und Rechtspfleger in die Technik-Lösung.

Damit stellt SIJUS-Straf eine Ersatz- und Ergänzungslösung zum derzeit bei der Staatsanwaltschaft eingesetzten Verfahren CANASTA dar. Um festzustellen, inwieweit SIJUS-Straf bremischen Standards anzupassen ist, ist eine Testinstallation für die Abteilung 5 der Staatsanwaltschaft — Beschaffungskriminalität und organisierte Kriminalität — errichtet worden. Die Testphase erfolgte zunächst unter Verwendung von Testdaten. In einem zweiten Schritt soll die Verarbeitung von Echtdaten in das Pilotprojekt einbezogen werden. Hierzu bin ich im Rahmen des ADV-Antragsverfahrens um Stellungnahme gebeten worden.

Bestandteil des mir vorgelegten ADV-Antrages war eine **Dienstanweisung**, die den Einsatz von SIJUS-Straf regeln soll. Diese Anweisung enthielt den Ansatz eines Datenschutzkonzeptes, das aber noch wesentliche Punkte offen läßt. Ich habe daher gefordert, daß die konkreten Einsatzgebiete von SIJUS-Straf festzulegen, die Rechtsgrundlagen für die einzelnen Verarbeitungsschritte darzulegen und Maßnahmen zur Sicherstellung einer effizienten Datensicherung zu treffen sind. Im einzelnen sind u. a. folgende **Anforderungen** einzuhalten:

- An das geplante Mehrplatzsystem sollen u. a. PCs mit eigener Rechnerleistung, das heißt nicht nur „dumme" Terminals, angebunden werden. Begründet wird dies damit, daß zusätzlich zu der von SIJUS bereitgestellten Textverarbeitung ein System verwendet werden soll, um die ergonomischen Vorteile einer grafikunterstützten Textverarbeitung nutzen zu können. Diese Lösung bietet gegenüber der in den anderen Bundesländern praktizierten SIJUS-Anwendung (ohne PC-Anbindung) ein größeres Gefährdungspotential. Durch die Möglichkeit, eigene Rechnerleistungen am Arbeitsplatz zu nutzen, wäre ein mißbräuchlicher Einsatz von Programmen und Utilities sowie eine unkontrollierte Nutzung der Daten nicht ausgeschlossen. Falls an dieser Lösung festgehalten werden soll, wären umfassende Maßnahmen zu treffen, dieses Risiko zu minimieren. So wäre eine Sicherheits-Software einzusetzen, die den Zugang zum Betriebssystem sperrt und dem Anwender nur den Zugriff auf Daten und Programme erlaubt, die dieser zur Aufgabenerfüllung benötigt. Außerdem müßte auf die Ausstattung der PCs mit Diskettenlaufwerken verzichtet werden, um das Einspielen fremder Programme und die Kopie von Daten auf Diskette zu verhindern. Diese zusätzlichen Sicherheitsaufwendungen sind in der vorliegenden Fassung der Dienstanweisung nur in allgemeiner Form angesprochen. Ich habe daher ein weitergehendes anwendungsbezogenes Konzept gefordert, gleichzeitig aber angeregt zu überlegen, ob nicht der Verzicht auf die PC-Anbindungen die bessere Lösung ist, da damit der Umfang der Datenverarbeitung von vornherein zentral festgelegt und kontrolliert werden kann.

- In dem dargestellten Anforderungskatalog des Senators für Justiz und Verfassung für die Anwendung von SIJUS-Straf wird u.a. von einem Datenaustausch mit anderen Dienststellen ausgegangen, ohne den Umfang und die Rechtsgrundlagen hierfür anzuführen. Ich habe daher gefordert, die angesprochenen Datenverbindungen zu konkretisieren und darzulegen, aufgrund welcher Rechtsgrundlagen diese erfolgen sollen. So ist z. B. festzulegen, in welcher Form welche Daten an das Bundeszentralregister sowie an das Verkehrszentralregister übermittelt werden sollen.

- Weitere Defizite des mir vorgelegten Datenschutzkonzepts betrafen u.a. den Aufstellungsort und die Zugangssicherung zum Zentralrechner, die Aufbewahrung der Sicherungskopien, den Einsatz der Drucker, die Protokollierung, die Vergabe von aufgabenspezifischen Zugriffsrechten (z. B. differenziert nach einzelnen Geschäftsstellen), die Aufgaben des Systemverwalters, die automatische Umsetzung von Lösch- und Sperrfristen sowie die Wartung.

Mit dem Senator für Justiz und Verfassung ist daher vereinbart worden, daß der Einsatz von PCs innerhalb der Pilotphase auf wenige Anschlüsse beschränkt wird und hierbei eine Sicherungssoftware eingesetzt wird. Während der Pilotphase soll außerdem kein Datenaustausch mit anderen Behörden bzw. Datenverarbeitungssystemen über SIJUS-Straf erfolgen. Außerdem hat der Senator für Justiz und Verfassung seine Dienstanweisung entsprechend meinen Anforderungen ergänzt und präzisiert. Eine gesicherte Rechtsgrundlage für die Vorgangsverwaltung der Strafverfolgungsbehörden insgesamt steht allerdings nach wie vor aus. Die Bundesregierung hat bis heute dem Bundestag den seit Jahren angemahnten und angekündigten Entwurf für ein Strafverfahrensänderungsgesetz (StVÄG) nicht zugeleitet.

7. Bildung und Wissenschaft

7.1 Zweckbindung für Daten der Studenten und des Lehrpersonals — neue Rechtsverordnung

Im letzten Jahr ist das neue Hochschulstatistikgesetz in Kraft getreten. Dieses Gesetz hat im Unterschied zur früheren Rechtslage im Bereich der Studentenstatistik die Umstellung von der Primärerhebung bei den Studenten auf eine Sekundärerhebung bei den Hochschulverwaltungen gebracht. Nicht mehr die Studenten sind gegenüber der Hochschulverwaltung, sondern die Hochschulverwaltungen sind gegenüber dem Statistischen Landesamt auskunftspflichtig. Die Hochschulverwaltungen erfüllen ihre Auskunftspflicht auf der Basis ihrer Verwaltungsdaten. Die für die Aufgabenerfüllung der Hochschulen erforderlichen Daten mußten landesrechtlich bestimmt werden.

Der bremische Gesetzgeber hat im Jahre 1988 das Bremische Hochschulgesetz geändert und einen neuen § 44 a „Datenverarbeitung" in das Gesetz eingefügt. Diese neue Bestimmung ermächtigt den Senator für Bildung und Wissenschaft, durch Rechtsverordnung die von Studienbewerbern, Studenten und Prüfungs-

kandidaten anzugebenden Daten und die Verarbeitungszwecke zu bestimmen. Diese Rechtsverordnung ist 1992 erarbeitet und abgestimmt worden; sie wurde im Dezember 1992 in der zuständigen Deputation beschlossen und im Januar dieses Jahres im Gesetzblatt der Freien Hansestadt Bremen verkündet.

Die Verordnung, die — rückwirkend — zum 01. September 1992 in Kraft getreten ist, präzisiert die anzugebenden Daten der einzelnen Betroffenengruppen und ihre jeweiligen Verwendungszwecke. Aus diesen Verwaltungsdaten dürfen die Hochschulen dann die Angaben für die Hochschulstatistik/Studentenstatistik machen. Ich war bei der Erarbeitung dieser Rechtsverordnung beteiligt; meine Anforderungen wurden im wesentlichen berücksichtigt.

7.2 Vermischung von Landes- und Kommunalaufgaben beim PC-Einsatz

Das Referat 24 in der Abteilung 2 „Schulplanung" des Senators für Bildung und Wissenschaft ist nach der Geschäftsverteilung für die Datenverarbeitung und Statistik zuständig. Nach eigenem Verständnis versteht es sich als Servicereferat für die übrigen Referate (der Abteilung? des Ressorts?), wobei die Servicefunktionen im Bereich Planung und Statistik (z. B. Bereitstellung entsprechender Methoden und Verfahren, Nutzung dieser Methoden und Verfahren zur Bereitstellung von Planungs- und Statistikdaten) und im Bereich der DV-Organisation (Beratung, Entwicklung, Anwendung) liegen. Im Referat 24 werden darüber hinaus auch exekutive Aufgaben (Verwaltungsvollzugsaufgaben) wahrgenommen, z. B. Führung des zentralen Schülerverzeichnisses, Führung einer Schuldatei, regelmäßige Meldung des Lehrerbestandes.

Im Zusammenhang mit einem Antrag zur „Beschaffung eines Servers mit MS-DOS-Arbeitsstationen" für das Referat 24 habe ich mich u. a. mit der Aufgabenstellung dieses Referates und der geplanten Nutzung der Server-Installation beschäftigt. Vor dem Hintergrund der tatsächlichen Gegebenheiten der Geschäftsverteilung für das Referat 24, den bestehenden Verwaltungsvorschriften (ADV-Anweisung, PC-Richtlinien) und datenschutzrechtlichen Anforderungen habe ich mich kritisch zu diesem Vorhaben geäußert.

Bei den **Vollzugsaufgaben,** die das Referat über die Geschäftsverteilung hinaus für die anderen Referate wahrnimmt, wird die Trennung der Kommunalaufgaben (Stadtgemeinde Bremen) von den Aufgaben des Landes Bremen außer acht gelassen, obwohl das Schulverwaltungsgesetz eine solche Trennung vornimmt und das Datenschutzrecht vom Funktionstrennungsprinzip ausgeht.

Bei den **Statistikaufgaben** des Referates wird übersehen, daß das Bundesverfassungsgericht in seinem Urteil zum Volkszählungsgesetz 1983 die Trennung von Statistik und Verwaltungsvollzug verlangt hat (zur Wahrung des Statistikgeheimnisses und des informationellen Selbstbestimmungsrechtes) und daß dem Senator für Bildung und Wissenschaft nur begrenzte, im wesentlichen geschäftsstatistische Befugnisse zustehen (§ 3 Abs. 2 Schulverwaltungsgesetz, § 12 Schuldatenschutzgesetz, § 11 Landesstatistikgesetz). Welche der statistischplanerischen Datenerhebungen und Datenaufbereitungen als Landes- oder welche als Kommunalaufgabe anzusehen sind und welche Geschäftsstatistiken wegen ihrer wiederkehrenden Regelmäßigkeit gem. § 4 Landesstatistikgesetz einer spezifischen Rechtsgrundlage bedürfen, ist noch zu klären.

Bei den **Datenverarbeitungsaufgaben** des Referates wird übersehen, daß es im Datenschutzrecht funktionelle Trennungsprinzipien gibt, die im Regelfall z. B. eine Trennung der Programmerstellung/Programmierung von der Programmanwendung (d. h. Nutzung des PC) erfordert. Die gültige ADV-Anweisung trägt diesem Gesichtspunkt dadurch Rechnung, daß die Programmierung dem Rechenzentrum der bremischen Verwaltung und nicht dem Fachressort bzw. den Fachbereichen zugeordnet ist. Dies gilt nach den für Bremen gültigen PC-Richtlinien ausdrücklich auch für alle Arten von PC-Anwendungsentwicklungen, da die ADV-Anweisung durch die PC-Richtlinien nicht berührt wird.

Das dem Beschaffungsantrag zugrunde gelegte Organisations- und Anwendungskonzept entspricht daher nicht den datenschutzrechtlichen Erfordernissen. Ich habe deshalb empfohlen, den Aufgabenzuschnitt des Referats 24 zu verändern (z. B. durch Herausnahme der exekutiven Aufgaben) und das Serverkonzept hinsichtlich des Anwendungsspektrums und der Aufgabenzuordnungen innerhalb des Ressorts und hinsichtlich der Aufgabenteilung mit dem Rechenzentrum der

bremischen Verwaltung zu überdenken. Der Senator für Bildung und Wissenschaft hat inzwischen erklärt, daß er seinen Antrag überarbeiten und neu stellen will.

7.3 Fall: Ungefragt im Philologen-Jahrbuch

Für die Herausgabe des Philologen-Jahrbuchs Niedersachsen/Bremen werden dem Philologen-Verband Niedersachsen jährlich aktualisierte Listen von den Philologen-Vereinen in Bremen und Bremerhaven mit den Daten von Lehrerinnen und Lehrern übermittelt, die an Schulen in diesen beiden Städten tätig sind. Die Daten der Lehrkräfte werden von Vertrauensleuten des Lehrerverbandes an den einzelnen Schulen erhoben und listenmäßig über einen örtlichen Bearbeiter an die niedersächsische Verbandsstelle weitergegeben. Ein Bremerhavener Lehrer hatte sich bei mir darüber beklagt, daß er — ohne Mitglied zu sein und ohne ausdrückliche Einwilligung — im Philologen-Jahrbuch verzeichnet ist.

Der in Bremerhaven für die Zusammenstellung und Übermittlung der Lehrerdaten verantwortliche Philologe teilte mir dazu mit, daß vor der Weitergabe der Lehrerdaten an die Landesverbandsstelle in den Bremerhavener Schulen ein Aushang erfolgt sei, mit dem auf die bevorstehende Herausgabe des Jahrbuchs und darauf, daß der Veröffentlichung der Daten von dem jeweils Betroffenen widersprochen werden kann, hingewiesen wurde. Der sich beklagende Lehrer hätte sich somit über die Weitergabe seiner Daten informieren und ihr, wenn er dies gewollt hätte, widersprechen können.

Bei der Erhebung und Weitergabe der Daten blieb die bremische Datenschutzrechtslage unberücksichtigt. Die Erhebung und Weitergabe der Beschäftigten-/Lehrerdaten durch Beschäftigte oder Lehrer einer Schule, speziell auch Vertrauensleute eines Lehrerverbandes oder einer Gewerkschaft, zu nicht-dienstlichen Zwecken ist ohne Einwilligung der Betroffenen nicht zulässig. Die Einwilligung der Betroffenen kann nicht durch einen Aushang in der Schule oder eine allgemeine Information über die Möglichkeit des Widerspruchs ersetzt werden.

Ich habe den Bremerhavener Philologen-Verein auf die Mißachtung der datenschutzrechtlichen Vorschriften hingewiesen. Er hat sich daraufhin bereiterklärt, vor der nächsten Ausgabe des Philologen-Jahrbuchs die schriftliche Einwilligung der betroffenen Lehrerinnen und Lehrer einzuholen. Darüber hinaus hat das über den Vorgang in Kenntnis gesetzte Schulamt des Magistrats auf meine Anregung hin die Mitarbeiterinnen und Mitarbeiter an den Schulen nochmals zur Einhaltung der datenschutzrechtlichen Bestimmungen angehalten. Der niedersächsische Datenschutzbeauftragte prüft indes die Datenverarbeitung beim Philologen-Verband Niedersachsen, speziell im Hinblick auf die Herausgabe der Jahrbücher. Das Ergebnis dieser Prüfung steht noch aus.

8. Arbeit und Frauen

8.1 Krankenhausentlassungsberichte an das Versorgungsamt

Das Versorgungsamt hat auf Antrag das Vorliegen und den Grad einer Behinderung festzustellen. Nach § 60 SGB I und ergänzend nach § 12 des Gesetzes über das Verwaltungsverfahren der Kriegsopferversorgung kann das Amt mit Einverständnis des Betroffenen für die Entscheidung erhebliche medizinische Unterlagen von niedergelassenen Ärzten, von Krankenhäusern und anderen Institutionen der Gesundheitsversorgung zur Einsicht beiziehen.

Unabhängig voneinander machten mich ein niedergelassener Arzt und der Medizinische Dienst der Krankenversicherung im Lande Bremen darauf aufmerksam, daß das Versorgungsamt von ihnen Unterlagen über das erforderliche Maß hinaus angefordert habe. Von dem Arzt hatte das Amt Entlassungsberichte angefordert, die Krankenhäuser ihm zum Zwecke der Nachbehandlung seiner Patienten übermittelt hätten und die Daten enthielten, die das Amt für seine Entscheidung nicht benötige. Im anderen Fall wurde berichtet, das Amt fordere regelmäßig alle Unterlagen des Medizinischen Dienstes über einen Versicherten an ohne jede inhaltliche Spezifizierung oder zeitliche Begrenzung. Man sei schon dazu übergegangen, nur die Unterlagen der letzten zwei Jahre zu übersenden; dies habe das Amt nicht moniert.

Auf meinen Hinweis, das Amt sei lediglich befugt, die für seine Entscheidung erheblichen Unterlagen anzufordern, und dies auch nur, soweit der Antragsteller sich damit einverstanden erklärt habe, erwiderte die Versorgungsverwaltung, daran halte man sich seit jeher. Dies sei den vor einigen Jahren mit meiner Dienst-

stelle abgestimmten Vordrucken zu entnehmen, die man noch heute verwende. Im übrigen strebe der Antragsteller regelmäßig eine umfassende Beurteilung seiner Behinderung an, weil er das Ziel verfolge, daß seine Behinderung als möglichst schwer anerkannt werde. Immerhin hat die Versorgungsverwaltung auf meine Vorschläge hin den Vordruck für die Einverständniserklärung nachgebessert:

- Voraussetzung dafür, daß Auskünfte eingeholt und Unterlagen angefordert werden, ist nunmehr sowohl, daß die jeweilige Stelle (Krankenhaus, Arzt usw.) im Antrag benannt ist, als auch, daß die Auskünfte bzw. Unterlagen für die Entscheidung erheblich sind.

- Der Vordruck eröffnet nunmehr dem Antragsteller die Möglichkeit zu vermerken, ob und inwieweit er sein Einverständnis einschränken will.

Dagegen habe ich meinen ursprünglichen Vorschlag, das Amt solle in jedem Einzelfall konkrete Fragen formulieren und um deren Beantwortung bitten, nicht weiter verfolgt, nachdem ich auf eine Umfrage hin erfahren hatte, daß in anderen Bundesländern entsprechende Verfahrensregelungen daran gescheitert seien, daß viele der angesprochenen Ärzte mangels eines als angemessen angesehenen Entgelts ihre Mitarbeit verweigert hätten.

Kurz vor Redaktionsschluß hat mich der Senator für Gesundheit, Jugend und Soziales darauf aufmerksam gemacht, daß das Versorgungsamt in kommunalen Krankenhäusern und insbesondere beim Kinderzentrum des ZKH St.-Jürgen-Str. regelmäßig die gesamten Krankenunterlagen eines Antragstellers anfordere. Ich teile die rechtlichen Bedenken des Gesundheitsressorts dagegen. Zudem widerspräche eine derartige Praxis sowohl dem Vordruck für die Einverständniserklärung als auch den bisherigen Aussagen der Versorgungsverwaltung. Ich werde der Angelegenheit nachgehen.

9. Jugend und Soziales

9.1 Beratungsgeheimnis und wirtschaftliche Hilfen (s. a. 14. Jahresbericht, Ziffer 2.5.2)

— Amt für Soziale Dienste

In jedem meiner vier letzten Jahresberichte hatte ich mich mit dem innerbehördlichen Umgang des Amtes für Soziale Dienste (AfSD) mit Klientendaten auseinandersetzen müssen, die ihm zum Zwecke der Entscheidung über Leistungen der Jugendhilfe von Klienten, Ärzten/Psychologen oder freien Trägern anvertraut bzw. übermittelt werden (s. a. zuletzt 14. Jahresbericht auf S. 36-38 unter Bezugnahme auf die §§ 36, 65 des neuen Kinder- und Jugendhilfegesetzes — KJHG). Es ging im Grunde stets um dasselbe Problem: Der/die zuständige Sozialarbeiter/in erstellt unter Angabe des erzieherischen Bedarfs, der zu gewährenden Art der Hilfe und der notwendigen Leistungen den nach § 36 KJHG gesetzlich gebotenen Hilfeplan. Diesen leitet er nach positivem Votum der Hilfe- oder Fallkonferenz dem Sachgebiet „Wirtschaftliche Hilfen" des Amtes mit der Bitte um Kostenübernahme zu. Regelmäßig wird von dort zusätzlich zum Hilfeplan die Zuleitung sämtlicher Unterlagen verlangt, die zur Vorbereitung der sozialarbeiterischen Entscheidung gedient hatten (ärztliches Gutachten/psychosoziale Diagnose/Entwicklungs- bzw. Verlaufsberichte). Anschließend werden auch diese Unterlagen auf Dauer zu den Akten der „Wirtschaftlichen Jugendhilfe" genommen.

Ich habe dazu stets die Auffassung vertreten, dies sei nicht erforderlich und daher auch nicht rechtmäßig, sondern verletze das **Sozialgeheimnis** der betroffenen Klienten/innen der Jugendhilfe und die **beruflichen Schweigepflichten** von Ärzten/Psychologen, Sozialpädagogen und Sozialarbeitern. Gerade angesichts immer differenzierterer Hilfs- und Förderangebote, der damit verbundenen Tendenz zur Erhebung zusätzlicher Sozialdaten der Klienten sowie zur Einholung von ärztlichen Gutachten und psychosozialen Diagnosen ist in dem arbeitsteilig organisierten AfSD eine abgestufte und auf das erforderliche Maß begrenzte Datenverarbeitung dringend geboten. Die Vorschriften des neuen KJHG bieten sowohl Anlaß als auch Grundlage für die erforderlichen Neuregelungen.

Bereits im September 1990 war die Angelegenheit Gegenstand der Erörterung des Datenschutzausschusses mit dem damaligen Ressort für Jugend und Soziales. Entgegen den dortigen Erklärungen des Ressortvertreters, entgegen dem Beschluß des Ausschusses vom 30. 01. 1991 (Drs. 12/1139 auf S. 3 unten, 4 oben), entgegen der Erklärung des Senats in seiner Stellungnahme zu meinem 13. Jahresbericht

(Drs. 12/1281 vom 02. 07. 1991, S. 10 unten, 11 oben) und entgegen der Ankündigung des Senats in seiner Stellungnahme zu meinem 14. Jahresbericht (Drs. 13/338 vom 22. 09. 1992, S. 8) sind von seiten des Ressorts die entsprechenden Dienstanweisungen des AfSD bis heute nicht erlassen worden. Die Sachbearbeiter/innen der „Wirtschaftlichen Jugendhilfe" im AfSD haben weiterhin alle dem Sozialarbeiter/der Sozialarbeiterin zur Verfügung stehenden Unterlagen angefordert. Ein anderslautender, dem Sozialdatenschutz gerecht werdender Verfahrensvorschlag für den Bereich der integrativen Erziehung behinderter und entwicklungsgestörter Kinder in Kindertagesheimen, den ich zusammen mit dem behördlichen Datenschutzbeauftragten und dem zuständigen Mitglied der Amtsleitung im Januar 1992 vorgelegt hatte, wurde zunächst blockiert. Inzwischen hat die Amtsleitung allerdings diesen Vorschlag erneut aufgegriffen und eine ressortinterne Abstimmung eingeleitet. Auch für andere Bereiche der Jugendhilfe liegen entsprechende Vorschläge vor.

Auf meine wiederholten Schreiben in dieser Sache, zuletzt an die Senatorin persönlich, erhielt ich lange keine inhaltliche Stellungnahme, sondern lediglich Hinweise auf die Belastung des Ressorts und Terminzusagen, welche wiederholt nicht eingehalten wurden. Einmal sollte eine Arbeitsgruppe „bis nach der Sommerpause" 1992 eine Regelung vorlegen (Schreiben des AfSD vom 21. 05. 1992), ein anderes Mal sollte Auftrag dieser Arbeitsgruppe sein, „noch im Laufe dieses Jahres" — d. h. 1992 — für den Leistungsbereich des KJHG Regelungen für den Umgang mit personenbezogenen Daten zu treffen und die bestehenden Dienstanweisungen zu überarbeiten (Stellungnahme des Senats vom 22. 09. 1992 zu meinem 14. Jahresbericht). Schließlich war vom Sommer 1993 die Rede. Inzwischen hat sich der Datenschutzausschuß der Angelegenheit angenommen. Daraufhin legte die Amtsleitung kürzlich den Entwurf einer Dienstanweisung über den Datenschutz in der Sozial- und Jugendhilfe vor, der nach einem ersten Durchblick geeignet scheint, als Grundlage für die erforderliche inhaltliche Abstimmung zu dienen.

— Jugendamt Bremerhaven

Kürzlich hatte mir das Jugendamt Bremerhaven den Entwurf eines Vordrucks für Hilfepläne nach § 36 KJHG zur Prüfung vorgelegt. Auch hier eine ähnliche Problematik: Nicht nur der Hilfeplan, sondern auch psychosoziale Diagnosen und Entwicklungsberichte sollten der Abteilung „Jugendsozialhilfe" des Amtes zugehen. Ich hatte dies kritisch angemerkt und gebeten, den Vordruck in dieser Fassung nicht zu verwenden. Inzwischen hat das Jugendamt erklärt, es werde meine Einwände berücksichtigen.

— Eingliederungshilfe für Erwachsene

Bereits seit 1990 wird im AfSD Bremen im Rahmen des Antragsverfahrens für das Eingliederungsangebot „Betreutes Wohnen" für psychisch Kranke und andere Personengruppen ein mit mir abgestimmtes Verfahren praktiziert. Insoweit ist der von mir für die Jugendhilfe geforderte abgestufte Datenfluß bereits Realität.

Dagegen fordert das Sozialamt Bremerhaven als Voraussetzung für die Kostenübernahme immer noch Eingliederungspläne des Gesundheitsamtes an, deren Inhalt über das für die Entscheidung des Sozialamts erforderliche Maß hinausgeht. Das gleiche gilt für die Berichte, die die Träger an das Sozialamt übermitteln müssen, sei es direkt oder über das Gesundheitsamt. Ich habe den Beteiligten ein Verfahren vorgeschlagen, das dem in Bremen für das „Betreute Wohnen" praktizierten entspricht. Danach würden die Berichte der Träger nur dem Gesundheitsamt zugeleitet und zugleich ihr Inhalt per Formblatt auf das erforderliche Maß begrenzt. Das Gesundheitsamt seinerseits würde dem Sozialamt nur seinen Vorschlag für einen Eingliederungsplan zuleiten, dessen Inhalt gleichfalls auf das erforderliche Maß begrenzt würde. Auf mein Schreiben an das Sozialamt vom August 1992 erhielt ich zwar kurze Zeit später Nachricht, man werde den Vorgang an das Hauptamt abgeben und unaufgefordert auf die Angelegenheit zurückkommen. Trotz meiner Erinnerung vom November 1992 habe ich aber bis heute keine Stellungnahme erhalten.

9.2 Auskunftspflicht aufgrund Unterhaltspflicht

Personen, die einem Sozialhilfeempfänger gegenüber zur Leistung von Unterhalt verpflichtet sind, müssen nach § 116 Bundessozialhilfegesetz (BSHG) dem Träger der Sozialhilfe Auskunft über ihre Einkommens- und Vermögensverhältnisse

geben. Sie erhalten hierzu einen detaillierten Fragebogen zugeschickt. Das Amt für Soziale Dienste Bremen aber fragt den Unterhaltspflichtigen nicht nur nach seinem eigenen Einkommen und Vermögen, sondern auch nach Einkommen und Vermögen seines Ehepartners. Dieser aber ist in der Regel dem Hilfeempfänger gegenüber nicht unterhaltspflichtig und deshalb dem Amt gegenüber nicht zur Auskunft verpflichtet. Das Amt allerdings behauptet in seinen Vordrucken, es bestehe auch insoweit Auskunftspflicht. Dies aber trifft nicht zu. Zulässig wäre die Frage lediglich, wenn die Antwort darauf in das Belieben des Unterhaltspflichtigen gestellt wäre. Dieser kann durchaus ein eigenes Interesse an der Beantwortung haben, weil seine Unterhaltspflicht seinem Ehegatten gegenüber seine Unterhaltspflicht dem Hilfeempfänger gegenüber mindern kann.

Auf meinen Vorschlag, dem Beispiel anderer Bundesländer zu folgen und im Vordruck vorzusehen, daß insoweit die Antwort freiwillig ist, hat das Sozialressort bislang nicht reagiert. Allerdings erfuhr ich von einer Reaktion von anderer Seite: Das Bundesministerium für Familien und Senioren schlug zwischenzeitlich in einem Entwurf für eine Reform des BSHG vor, den § 116 genau um die hier strittige bislang fehlende Auskunftspflicht zu erweitern. Zwar ist der Entwurf inzwischen zurückgezogen worden, sollte die besagte Ergänzung des § 116 BSHG erneut auf den Tisch kommen, wird die Erforderlichkeit dieser Ausweitung kritisch zu hinterfragen sein.

9.3 Seniorenzentraldatei in Bremerhaven

Seit jeher speicherte das Sozialamt Daten der Bremerhavener Bürger im Alter über 63 Jahren in einer manuellen Kartei. Diese wurde erstmals mittels Anfrage bei der Meldebehörde erstellt und auf dem gleichen Wege fortlaufend einmal jährlich durch die Daten der Bürger ergänzt, die im jeweils abgelaufenen Jahr 63 Jahre alt geworden waren. Sterbefälle wurden anhand von Sterbelisten des Standesamtes berücksichtigt. Für die regelmäßige Übermittlung der Meldedaten fehlt die nach § 30 Abs. 4 des Bremischen Meldegesetzes erforderliche Rechtsgrundlage, für die Übermittlung und Nutzung der Sterbelisten eine entsprechende Befugnis im Personenstandsgesetz. Auf meine Intervention hin stellte die Meldebehörde ihre Übermittlung an das Sozialamt ein und verzichtete das Sozialamt auf seine Anfragen beim Standesamt.

Das Sozialamt verfolgte zunächst allerdings seine Planung weiter, die Seniorenkartei künftig auf automatisierter Basis zu betreiben. In diesem Zusammenhang wollte man dem Senator für Inneres und Sport vorschlagen, die Meldedatenübermittlungsverordnung um eine entsprechende Übermittlungsbefugnis der Meldebehörde zu ergänzen. In der Datei sollten alle Bremerhavener Bürger, die älter als 60 Jahre sind, gespeichert werden, ausgenommen diejenigen, die dem ausdrücklich widersprochen hatten. Die Daten sollten genutzt werden, um die Betroffenen über Angebote der Seniorenhilfe zu informieren, die Teilnahme an Ausflugs- und Erholungsfahrten sowie an Gruppenprogrammen zu verwalten und zu überprüfen, ob der Betreffende einen Zuschuß für eine Erholungsfahrt erhalten kann, was alle drei Jahre der Fall ist. Schließlich sollten mit Hilfe der Datei Gesichtspunkte dafür festgestellt werden können, ob sich der einzelne in einer Notlage befinde und ihn deshalb der Besuchsdienst der Seniorenbetreuung aufsuchen und beraten solle. Derartige Gesichtspunkte sollten z. B. sein, daß ein Senior im Alter von 75 Jahren noch an keinem Angebot der Seniorenbetreuung teilgenommen habe, daß er zwar bislang regelmäßig Angebote wahrgenommen habe, nun aber nicht mehr, oder auch der Tod des Ehepartners.

Gegen das Vorhaben, die Daten der älteren Bürger Bremerhavens ohne ihre **Einwilligung** gesondert zu speichern und zu den vorgenannten Zwecken zu nutzen, bestanden grundsätzliche datenschutzrechtliche Bedenken. Es wäre ein Nebenregister zum Melderegister eingerichtet worden, das weder durch das Meldegesetz noch durch das Bundessozialhilfegesetz legitimiert gewesen wäre. Auch § 75 BSHG, der die Altenhilfe regelt, legt lediglich die Aufgaben des Sozialhilfeträgers fest, räumt ihm aber nicht die Befugnis zu einer derart umfassenden Datenspeicherung ein. Überdies ist der Schluß daraus, daß ein älterer Bürger die Angebote der Seniorenbetreuung nicht oder nicht mehr wahrnimmt, darauf, daß er sich in einer Notsituation befinden könne und deshalb geboten sei, daß ihn Mitarbeiter des Sozialamtes aufsuchen, in Frage zu stellen. Der rechtlich unproblematische Weg, uninformierte Senioren anzusprechen und denen unter ihnen zu helfen, die in Not geraten sind, geht nicht über die ausnahmslose Registrierung aller älteren Mitbürger, sondern über zielgruppenspezifische Öffentlichkeitsarbeit und ein Netz von Nachbarschaftshilfen.

Jedoch bestehen keine Bedenken dagegen, daß die Meldebehörde aus Anlaß von Stadtteilfesten die Daten der im Einzugsbereich wohnenden älteren Mitbürger übermittelt, damit sie eingeladen werden können — wohlgemerkt nicht, damit ihre Daten auf Dauer gespeichert werden. Zulässig wäre nach dem Sozialgesetzbuch (SGB) auch eine Speicherung nur zum Zwecke der Entscheidung über einen Antrag und zur Abwicklung der daraufhin gewährten Sozialleistung, etwa einer Erholungsfahrt. Ebensowenig bestehen Bedenken dagegen, daß das Sozialamt die Daten älterer Bürger insoweit speichert, als sie sich ausdrücklich damit einverstanden erklärt haben.

Inzwischen hat der Magistrat meine Bedenken und Hinweise aufgenommen und umgesetzt. Nunmehr sollen nur noch die Daten derjenigen älteren Bürger auf Dauer gespeichert werden, die sich damit ausdrücklich einverstanden erklärt haben. Das Sozialamt hat in Abstimmung mit mir einen Vordruck für die Einverständniserklärung entwickelt. Der Betroffene kann sich darin auch darüber informieren, worin er einwilligt, d. h. es wird im einzelnen aufgeführt, zu welchen Zwecken das Sozialamt die Daten nutzen will. Damit ist ein Weg gefunden worden, der es einerseits dem Sozialamt gestattet, die älteren Bürger Bremerhavens zu erreichen und ihnen entsprechend seinem gesetzlichen Auftrag „die Möglichkeit zu erhalten, am Leben der Gemeinschaft teilzunehmen". Andererseits aber wird respektiert, daß es auch ältere Menschen gibt, die an den Angeboten des Sozialamtes keinen Bedarf und kein Interesse haben.

10. Gesundheit

10.1 Kontrollergebnisse in kommunalen Krankenhäusern

10.1.1 Konsequenzen des Krankenhausdatenschutzgesetzes (KHDSG)

Der Krankenhauspatient befindet sich in einer für ihn oft existentiell bedrohlichen oder als bedrohlich empfundenen Situation. In ihr erwartet er Hilfe von einzelnen Ärzten und Pflegekräften, sieht sich aber zugleich einem für ihn unüberschaubaren Apparat gegenüber. Er hat weder Einfluß noch Überblick, was im einzelnen mit seinen Daten, z. B. medizinischen Befunden, Röntgenaufnahmen, Blutproben, geschieht. Die allgemeinen Regelungen des Bremischen Datenschutzgesetzes (BrDSG) zum Datenschutz bzw. des Straf- und Berufsrechts zur ärztlichen Schweigepflicht werden den besonderen Anforderungen an den Schutz der Patientendaten im Krankenhaus nicht gerecht: Die einen sind auf die Datenverarbeitung in der Verwaltung, die anderen auf den niedergelassenen Arzt zugeschnitten.

Vor diesem Hintergrund ist die Bedeutung des Bremischen Krankenhausdatenschutzgesetzes (KHDSG) zu werten, das im Mai 1989 in Kraft getreten ist (s. a. 11. Jahresbericht, Ziffer 2.1.1). Das Gesetz hat seitdem an Bedeutung noch gewonnen, bedenkt man die beschleunigte Automatisierung der Verarbeitung von Patientendaten in den Krankenhäusern. Sie wird eingesetzt zur Abrechnung mit den Kostenträgern, zur Behandlung, zur Forschung sowie zur Dokumentation und umfaßt zunehmend medizinische Daten. Die Automatisierung wird teils zentral von der Klinikleitung initiiert und gesteuert, teils von Klinikärzten auf eigene Initiative betrieben. Einzelne Klinikärzte verarbeiten Patientendaten auf eigenen PCs (s. a. 11. Jahresbericht, Ziffer 5.6.2) oder auf Geräten und mit Hilfe von Software, die ihnen von Außenstehenden, etwa der Industrie oder von Forschungseinrichtungen zur Verfügung gestellt wurden (s. a. KLIMACS: Medizinische Forschung und AIDS-Bekämpfung, 14. Jahresbericht, Ziffer 2.6.5). In einigen Fällen habe ich den Eindruck gewonnen, als fehle es der Klinikleitung an Überblick über die Datenverarbeitung in den einzelnen Abteilungen. Damit aber fehlt die Grundvoraussetzung dafür, daß die Leitung die ihr nach BrDSG und KHDSG obliegende Verpflichtung erfüllen kann, in ihrem Verantwortungsbereich eine ordnungsgemäße Datenverarbeitung sicherzustellen.

Demgegenüber verpflichtet § 7 BrDSG, der nach § 1 Abs. 4 KHDSG auch für Krankenhäuser gilt, die Krankenhausleitungen dazu, für automatisierte Dateien bzw. für Geräte, mit denen personenbezogene Daten automatisiert verarbeitet werden, in einer Dateibeschreibung bzw. in einem Geräteverzeichnis bestimmte datenschutzrechtlich wichtige Merkmale festzulegen. Diese Festlegungen dienen zugleich

— dazu, der Leitung zu ermöglichen, ihrer Verantwortung gerecht zu werden,

— als Unterlage für die Übersichten zur Datenverarbeitung, die die Leitung nach § 9 KHDSG i. V. m. § 37 Bundesdatenschutzgesetz (BDSG) dem von ihr zu bestel-

lenden betrieblichen Datenschutzbeauftragten zur Verfügung zu stellen hat, und damit als Grundlage für dessen Aufgabenerfüllung,

- als Unterlage für die Anmeldung der Dateien zum von mir geführten Dateienregister (§ 28 BrDSG),
- als Grundlage für meine Überwachung der Datenverarbeitung im Krankenhaus; Dateibeschreibungen, Geräteverzeichnisse und Übersichten sind mir auf Verlangen vorzulegen (§ 27 BrDSG),
- als Grundlage für die kommunale Rechtsaufsicht über die Krankenhäuser nach § 9 der Krankenhausbetriebsgesetze der Stadtgemeinden Bremen und Bremerhaven.

10.1.2 Prüfprogramm

Unabhängig von durch Patientenbeschwerden oder andere Hinweise veranlaßten punktuellen Überprüfungen in einzelnen Krankenhäusern habe ich begonnen, die fünf kommunalen Krankenhäuser im Lande Bremen systematisch auf die Einhaltung des KHDSG und des BrDSG hin zu überprüfen. Dabei nehme ich zum Ausgangspunkt die dargestellten Dokumentationspflichten und die Aufgabenerfüllung durch die betrieblichen Datenschutzbeauftragten. Damit möchte ich zunächst erreichen, daß die Krankenhäuser ihre gesetzlichen Dokumentationspflichten so erfüllen, daß die Verantwortlichen, vor allem die Leitung, die EDV-Leiter und die Datenschutzbeauftragten, ihrer jeweiligen Verantwortung gerecht werden können. Daneben möchte ich die Datenschutzbeauftragten in ihrer Stellung nach § 9 KHDSG i. V. m. § 36 BDSG und bei der Wahrnehmung ihrer Aufgaben nach § 9 KHDSG i. V. m. § 37 BDSG unterstützen. Nach meinen bisherigen Erfahrungen besteht Anlaß, darauf hinzuweisen, daß Datenschutzbeauftragte

- nicht personengleich mit dem EDV-Leiter sein dürfen,
- gegenüber dem EDV-Leiter eine selbständige und unabhängige Stellung haben müssen,
- über genügend Arbeitskapazität für ihre Aufgaben verfügen müssen.

Deshalb bewerte ich es positiv, daß das ZKH Bremen-Ost jetzt als erstes Krankenhaus einen hauptamtlichen Datenschutzbeauftragten — wenn auch nur mit halber Stundenzahl — bestellt hat. Ich bin gern bereit, die anderen Krankenhäuser dabei zu unterstützen, die Krankenkassen davon zu überzeugen, daß im Rahmen des Pflegesatzes auch die Kosten für einen effektiven Patientendatenschutz zu berücksichtigen sind.

Im November 1992 habe ich als erstes das ZKH Rinkenheide in Bremerhaven überprüft. Im ZKH Bremen-Nord habe ich ein ausführliches Vorbereitungsgespräch geführt; ein Prüfbesuch folgt demnächst. Beide Krankenhäuser nahmen meinen Besuch zum Anlaß, ihre EDV-Dokumentation zu vervollständigen, zu systematisieren und zu aktualisieren.

10.1.3 EDV im Zentralkrankenhaus Reinkenheide

Auf der Basis der mir zur Verfügung gestellten Unterlagen überprüfte ich im ZKH Reinkenheide exemplarisch die DV-Organisation in der zentralen Verwaltung einschließlich vier Terminals, die Fernwartung und die Archivierung von Krankenakten. Die dabei festgestellten erheblichen Mängel veranlaßten mich dazu, dem Krankenhaus eine Liste mit den nach § 6 BrDSG gebotenen Vorkehrungen zur Verbesserung der Datensicherheit vorzulegen. Dem Senator für Gesundheit, Jugend und Soziales habe ich die Liste gleichfalls zugeleitet, weil ich sie als Richtschnur für ordnungsgemäße Datenverarbeitung auch in den seiner Aufsicht unterstehenden kommunalen Kliniken der Stadtgemeinde Bremen ansehe. Folgende Punkte sind hervorzuheben:

Datensicherheit in der zentralen EDV:

- Sicherung des EDV-Raumes, so daß nur Wartungs- und Bedienungspersonal der Zugang möglich ist;
- Kontrolle der Operatoraktivitäten durch Protokollierung der Systemaktivitäten und Einführung des „Vier-Augen-Prinzips";
- Einführung der Funktionstrennung zwischen Durchführung und Kontrolle;

— Verbesserung der Paßwortsteuerung durch

- Ausschluß einfacher Kombinationen
- Festlegung einer begrenzten Gültigkeitsdauer
- verschlüsselte Speicherung, d. h. Sicherstellung, daß nur der/die Paßwortinhaber/in Kenntnis haben kann.

Datensicherheit bei den Terminals:

— Verbesserung der Paßwortsteuerung

— Protokollierung des Zugriffs auf Patientendaten

— Einschränkung des Zugriffs durch einzelne Mitarbeiter/innen auf die nur für die jeweilige Aufgabenerfüllung erforderlichen Patientendaten.

Da einige der von mir geforderten Maßnahmen auf der vorhandenen EDV-Anlage nicht zu realisieren sind, gehe ich davon aus, daß sie zumindest bei der geplanten Modernisierung des EDV-Bereiches berücksichtigt werden. Datenschutzsoftware auf den im Krankenhaus vorhandenen Einzelplatz-PCs wurde innerhalb des Prüfungszeitraumes bereits installiert.

Datensicherheit bei Fernwartung:

Die beruflichen Schweigepflichten der Ärzte/Ärztinnen und ihrer Mitarbeiter/innen gelten auch im Krankenhaus. Schon im Hinblick darauf ist es unzulässig, wenn ein Krankenhaus einer Fernwartungsfirma den Zugriff auf personenbezogene Daten seiner Patienten/Patientinnen eröffnet (zur Problematik der Fernwartung allgemein s. o. Ziffer 2.2.2.).

Eine Stellungnahme des ZKH Reinkenheide zu meinen Anforderungen habe ich noch nicht erhalten.

10.1.4 Nachlässigkeit bei externer Wartung (ZKH St.-Jürgen-Straße)

Allerdings gibt es außer der Fernwartung noch andere Wartungsmethoden, die Gefahr für den Patientendatenschutz bedeuten. Dies erfuhr ich, als ich auf einen entsprechenden Hinweis hin mich davon überzeugen wollte, ob bei der automatisierten Speicherung von medizinischen Patientendaten auf einem privateigenen PC eines Chefarztes des ZKH St.-Jürgen-Str. die Datenschutzbestimmungen beachtet wurden. Das Krankenhaus teilte mir mit, daß kurz vor Eingang meines Ankündigungsschreibens die Festplatte mit den Patientendaten bei einer Wartung neu partioniert und formatiert und dabei versehentlich alle Daten auf der Festplatte gelöscht worden seien. Zuvor habe der Chefarzt den PC persönlich — wohlgemerkt mit Festplatte und darauf gespeicherten Patientendaten — zur Wartungsfirma gebracht.

Ich habe darauf aufmerksam gemacht, daß vor der Wartung die Patientendaten hätten auf Diskette übertragen, die personenbezogenen Merkmale auf der Festplatte hätten physikalisch gelöscht und die Diskette im ZKH hätte gesichert aufbewahrt werden müssen. Ich habe um eine entsprechende Unterrichtung der Mitarbeiter/innen gebeten. Das ZKH hat sich hierzu und zu meinen sonstigen Vorschlägen für eine künftige datenschutzgerechte Speicherung der Patientendaten noch nicht geäußert.

10.2 Eckpunkte für ein Gesetz über den öffentlichen Gesundheitsdienst (s. a. 14. Jahresbericht, Ziffer 2.6.6)

Wiederholt habe ich in meinen Jahresberichten auf die Notwendigkeit hingewiesen, Aufgaben und Befugnisse der Gesundheitsämter in einem zeitgemäßen Gesetz zu regeln und damit die bisherige Rechtsgrundlage aus dem Jahre 1934 (!) zu ersetzen. Inhaltliche Anforderungen an die Regelung der Befugnisse zur Datenverarbeitung hatte ich bereits im 12. Bericht (Ziffer 2.7.1.2) formuliert. Kürzlich hat der Senator für Gesundheit, Jugend und Soziales Eckpunkte einer gesetzlichen Regelung in der Deputation für Gesundheit und im Gesundheitsausschuß der Bremerhavener Stadtverordnetenversammlung vorgelegt, die auch Aussagen zum Datenschutz enthalten.

Ich entnehme diesen, daß Einigkeit darin besteht, daß die Garantie eines besonderen Vertrauensschutzes für die Klienten, die die Beratungsangebote der Gesundheitsämter wahrnehmen, und eine enge Zweckbindung bei der Nutzung und

Übermittlung der von den Ämtern erhobenen Daten bzw. der von deren Ärzten und Psychologen erstellten Gutachten und Diagnosen eine wichtige Voraussetzung dafür ist, daß ein öffentlicher Gesundheitsdienst, der sich in erster Linie als Bürgerservice definiert, seine Aufgaben sinnvoll wahrnehmen kann.

In diesem Sinne verstehe ich auch die Verfahrensregelungen, die ich in konkreten Punkten mit dem Gesundheitsamt Bremerhaven und mit dem Hauptgesundheitsamt Bremen vereinbart habe (s. a. 13. Jahresbericht, Ziffer 2.6.2). Allerdings habe ich das Ressort kürzlich erneut darauf hinweisen müssen, daß die Kartei und die Registratur des Amtsärztlichen Dienstes im Hauptgesundheitsamt Bremen datenschutzrechtlichen Anforderungen nicht gerecht werden:

- Ältere Akten enthalten psychosoziale Diagnosen und andere Bestandteile, die nichts mit den Aufgaben des Amtsärztlichen Dienstes zu tun haben, vielmehr ausgesondert und in die Obhut des Sozialpsychiatrischen Dienstes oder anderer Beratungsstellen gegeben werden müssen.

- Es werden Uraltvorgänge aufbewahrt, die längst dem Staatsarchiv hätten angeboten oder vernichtet werden müssen. Jüngst wurde in diesem Zusammenhang die Aktenordnung des Senats von 1958 herangezogen, deren Anpassung an die Löschungsbestimmungen in § 20 Bremisches Datenschutz (BrDSG) überfällig ist.

- Die vom Hauptgesundheitsamt selbst vorgeschlagene Regelung der Neugliederung und Nutzungsbegrenzung seiner eigenen Vorgänge ist noch nicht umgesetzt worden.

Das Hauptgesundheitsamt führt für die Verzögerungen fehlende Personal- und Sachmittel an und verweist auf die ins Auge gefaßte Automatisierung seiner Datenverarbeitung. Auf mein Betreiben hat es jetzt ein Konzept hierfür vorgelegt. Gegenüber der senatorischen Dienststelle dränge ich darauf, daß die Planung vorangetrieben wird. Unabhängig davon hat das Hauptgesundheitsamt zugesagt, schon jetzt technisch mögliche und finanziell neutrale datenschutzrechtlich unabdingbare Änderungen vorzunehmen:

- Wenn aus aktuellem Anlaß eine Karte der amtsärztlichen Kartei gezogen wird, auf der noch unzulässigerweise die Inanspruchnahme eines Beratungsdienstes vermerkt ist, ist sie durch eine neue Akte ohne Quervermerk zu ersetzen (so praktiziert im Gesundheitsamt Bremerhaven).

- Zugleich ist die dazugehörige Akte dem entsprechenden Beratungsdienst zuzuleiten, damit dieser die Vorgänge entnimmt, die in seine Obhut gehören.

Außerdem gehe ich davon aus, daß im Laufe des Geschäftsganges angefallene löschungspflichtige Vorgänge ständig ausgesondert, dem Staatsarchiv angeboten bzw. gelöscht werden.

10.3 Patientendaten in der gesetzlichen Krankenversicherung

10.3.1 Umgehung des unbequemen Gesundheitsreformgesetzes 1989

In meinem 14. Jahresbericht habe ich unter Ziffer 2.6.1 hervorgehoben, daß das Gesundheitsreformgesetz von 1989 (SGB V) die Befugnisse der gesetzlichen Krankenkassen zur Datenerhebung und die Verpflichtung der Erbringer von Leistungen im Gesundheitswesen zur Übermittlung von Patientendaten an die Kassen normenklar und bereichsspezifisch geregelt habe. Zugleich aber habe ich die weit verbreitete Praxis der Krankenkasen kritisiert, bei Ärzten, Krankenhäusern, Trägern von Seniorenheimen und Rettungsdiensten (Leistungsträger) über das durch das Gesetz legitimierte Maß hinaus Versichertendaten zu erheben. In einem der dargestellten Fälle ist inzwischen durch das Gesundheitsstrukturgesetz 1993 (GSG) die erforderliche Rechtsgrundlage geschaffen worden. § 301 Abs. 1 Nr. 3 SGB V verpflichtet seit dem 01. 01. 1993 die Krankenhäuser, den Krankenkassen zwecks Kontrolle der Verweildauer der Patienten die voraussichtliche Dauer der Krankenhausbehandlung sowie, falls diese überschritten wird, auf Verlangen der Krankenkasse die medizinische Begründung zu übermitteln.

Ein anderes der im 14. Jahresbericht dargestellten Probleme — Kontrolle des Verbrauchs medizinischer Hilfsmittel in Altenpflegeeinrichtungen mittels Erhebung der Verbrauchsdaten der Pflegebedürftigen — hat sich nach meiner Intervention dadurch erledigt, daß sich die beteiligten Stellen auf eine pauschalisierte Abrechnung geeinigt haben. Dagegen ist leider noch nicht erkennbar, daß die Kranken-

versicherungen bereit sind, die rechtlich gebotene Trennung zwischen ihrer eigenen Befugnis zur Erhebung von Versichertendaten (§ 284 SGB V) und der Befugnis des Medizinischen Dienstes der Krankenversicherung zur Datenerhebung zwecks Erfüllung von dessen Aufgaben (§§ 175, 176 SGB V) zu beachten. Der Vorschlag des Bundesministers für Gesundheit, im Rahmen des geplanten 2. Gesetzes zur Änderung des SGB eine entsprechende Klarstellung in § 276 SGB V einzufügen, ist noch nicht in das Gesetzgebungsverfahren gelangt. Vor allem aber hat sich gezeigt, daß es weiterhin verbreitete Praxis der Spitzenverbände im Gesundheitswesen ist, auf Bundesebene zu vereinbaren, daß die Leistungserbringer an die Krankenversicherungen wesentlich mehr Daten übermitteln müssen als das SGB V zuläßt.

— Erstes Beispiel: Der Abrechnungsschein für den ärztlichen Notfalldienst

Der Chefarzt einer chirurgischen Klinik in Bremen leitete mir den Abrechnungsschein für die ambulante Notfallbehandlung im Krankenhaus zu. Es handelt sich dabei um einen vierteiligen inhaltsidentischen Durchschreibesatz. Das Original ist für die Kassenärztliche Vereinigung zur Abrechnung mit der Krankenkasse bestimmt, ein Durchdruck soll an den weiterbehandelnden Arzt gehen und zwei Durchdrucke sollen im Krankenhaus verbleiben. Anders als auf normalen Krankenscheinen muß der Notfallarzt auf diesen Vordrucken nicht nur die erbrachten ärztlichen Leistungen und Diagnosen eintragen, sondern auch Angaben zum Unfallhergang und zur Therapie machen. Wie auch die Krankenhausgesellschaft der Freien Hansestadt Bremen in einem Rundschreiben an ihre Mitglieder einräumte, sollen diese zusätzlichen Angaben den weiterbehandelnden Arzt informieren und der Dokumentation des Krankenhauses dienen.

Die AOK Bremen/Bremerhaven dagegen erklärte mir, sie benötige sämtliche Angaben, um die ihr gesetzlich übertragenen Aufgaben zu erfüllen und berief sich auf den zwischen der Kassenärztlichen Bundesvereinigung und den Bundesverbänden der Krankenkassen vereinbarten „Bundesmantelvertrag Ärzte" sowie dessen Anlage 2, die sogenannte Vordruckvereinbarung. Zwar entspricht das Abrechnungsformular diesen Vereinbarungen; davon konnte ich mich überzeugen, nachdem mir die AOK auf Anforderung die Vereinbarungen zur Verfügung gestellt hatte. Die Vereinbarungen verstoßen aber ihrerseits gegen gesetzliche Regelungen. Zwar beauftragt das SGB V die Spitzenverbände der Kassen und der Leistungserbringer damit, Form und Inhalt von Abrechnungsunterlagen zu vereinbaren (§§ 295 Abs. 3, 301 Abs. 3 SGB V), jedoch dürfen die Vordrucke nicht vorsehen, daß deren Empfänger mehr Informationen über die Patienten erhalten als gesetzlich vorgesehen. Genau dies aber ist Inhalt der getroffenen Vereinbarungen. Ich habe den Eindruck, daß die Vereinbarung gesetzeswidriger Übermittlungen von Patientendaten in diesem Fall weniger auf Absicht als auf bürokratischer Gedankenlosigkeit beruht. Vielleicht hat man nur vergessen, die Durchdrucke so zu variieren, daß jedem der Empfänger nur die Daten übermittelt werden, die er jeweils benötigt. Dies berechtigt zu der Hoffnung, daß in naher Zukunft Abhilfe geschaffen wird.

— Zweites Beispiel: Meldung und Speicherung der Daten von Methadonsubstituierten Drogenabhängigen

In der Stadtgemeinde Bremen verabreichen inzwischen ca. 50 niedergelassene Ärzte Methadon an Drogenabhängige. Grundlage ist eine im Jahre 1990 vom Senator für Gesundheit, der Ärztekammer und der Kassenärztlichen Vereinigung Bremen gemeinsam abgegebene Empfehlung. In meinem 14. Jahresbericht hatte ich unter Ziffer 2.6.3 auf die sich daraus ergebenden datenschutzrechtlichen Probleme hingewiesen. Unter bestimmten Umständen werden nunmehr die Kosten von den gesetzlichen Krankenkassen übernommen. Die Voraussetzungen hierfür regeln Empfehlungen, die die Bundesausschüsse der Ärzte und der Krankenkassen auf der Grundlage von § 135 Abs. 1 SGB V zur Methadon-Substitionsbehandlung als neue Nr. 2 der Richtlinien über die Einführung neuer Untersuchungs- und Behandlungsmethoden abgegeben haben. In diesen sogenannten **NUB-Richtlinien** wird u. a. zur Voraussetzung der Kassenfinanzierung gemacht, daß der substituierende Arzt Beginn und Ende der Substitution unverzüglich sowohl der Kassenärztlichen Vereinigung als auch der Krankenkasse seines Patienten anzeigt.

Diese Datenübermittlungen finden im SGB V keine Grundlage. Meiner entsprechenden Kritik ist entgegengehalten worden, die Ärzte seien nach § 295 SGB V

ohnehin verpflichtet, die Krankenscheine ihrer Patienten — also auch der Methadon-Substituierten - bei der Kassenärztlichen Vereinigung einzureichen, und diese leite die Unterlagen später an die jeweilige Krankenkasse weiter. Die NUB-Richtlinie verlange also nur eine zeitliche Vorverlegung der Datenübermittlung. Dabei wird aber verkannt, daß, anders als es das Gesetz vorsieht,

- zusätzliche detaillierte Daten über psychosoziale Betreuung übermittelt werden sollen, in bestimmten als strittig gekennzeichneten Fällen auch der Therapieplan,
- die Kassenärztliche Vereinigung die ihr eingereichten Meldungen auf Dauer speichert (und auch auswertet), wohingegen sie die Krankenscheine mit ihren Abrechnungsunterlagen an die Kassen weiterleitet, also von den anderen Versicherten auf Dauer keine personenbezogenen Unterlagen zurückbehält,
- die Kassen ohne die Meldung der substituierenden Ärzte die Daten von Methadonsubstituierten Versicherten lediglich zusammen mit allen anderen eingereichten Krankenscheinen, also praktisch nicht getrennt auswertbar, erhielten.

Dies alles ist um so bedenklicher, als weder Kassenärztliche Vereinigung noch Kassen in Bremen bisher verbindlich erklärt haben, wozu sie die Daten der Methadon-Substituierten verwenden und wie sie die Einhaltung der von ihnen selbst definierten Zweckbestimmung gewährleisten wollen. Vielmehr berufen sie sich lediglich auf die NUB-Richtlinie. Diese aber — und hier sehe ich eine Parallele zum vorgenannten Beispiel — vermag über das gesetzliche Maß hinaus eine Verarbeitung von Versichertendaten durch Kassenärztliche Vereinigung und Kassen nicht zu rechtfertigen, zumal in § 135 SGB V, der als Rechtsgrundlage für die NUB-Richtlinie herangezogen wird, zwar von anderen Regelungsinhalten derartiger Richtlinien, nicht aber von der Einräumung von Befugnissen zur Datenverarbeitung die Rede ist.

Der Gesetzgeber hat in dem zum 01. 01. 1993 in Kraft getretenen Gesundheitsstrukturgesetz (GSG, s. a. Ziffer 10.3.2) die §§ 295, 301 SGB V um zusätzliche Datenarten ergänzt, die die Ärzte bzw. Krankenhäuser den Kassenärztlichen Vereinigungen bzw. Krankenkassen zu Abrechnungszwecken übermitteln müssen. Dabei hat der Gesetzgeber weitgehend die Forderungen der Kostenträger übernommen. Dies alles wäre nicht der Mühe wert gewesen, wenn letztere selbst einverständlich bestimmen könnten, in welchem Umfang ihnen die Leistungserbringer Versichertendaten übermitteln müssen.

Dem kann nicht entgegengehalten werden, meine datenschutzrechtlichen Bedenken gefährdeten das Methadon-Programm. Vielmehr haben die Gegner des Methadon-Programms die kritisierte Datenverarbeitung mit dem Ziel von dessen Einschränkung erzwungen. Demnach ist ein sachgerechtes Verfahren sehr wohl ohne die zusätzliche Datenverarbeitung denkbar. Ich befürchte, daß hier an einer Gruppe von Versicherten, die in besonderem Maße gesellschaftlich stigmatisiert sind, erstmals eine isolierte Datenverarbeitung erprobt wird, die eine versichertenbezogene Auswertung ihrer medizinischen Daten geradezu herausfordert. Die daran beteiligten Stellen lassen es in einem bedauerlichen Maße an der gebotenen Sensibilität fehlen.

10.3.2 Auswirkungen des Gesundheitsstrukturgesetzes (GSG '93)

Das GSG 93 ist in seinen Neuregelungen zur Datenverarbeitung im Gesundheitswesen geprägt von dem Bestreben, die Automatisierung der Datenverarbeitung zu forcieren. Dies gipfelt in der Androhung finanzieller Sanktionen, falls die Leistungserbringer nicht bis zum 01. 01. 1995 die Abrechnungsdaten automationsgerecht übermitteln, § 303 Abs. 3 SGB V. Der damit verbundenen und auch von mir während des Gesetzgebungsverfahrens beschworenen Gefahr, daß die Automatisierung der Verarbeitung von Versichertendaten es den Kassen ermöglichen werde, über das bisher mögliche und rechtlich legitimierte Maß hinaus Abrechnungsdaten versichertenbezogen zu verknüpfen und — etwa zum Zwecke der Beratung, Überwachung oder Risikominimierung — in Gestalt von Leistungskonten und Gesundheitsprofilen der einzelnen Versicherten auszuwerten, hat das GSG 93 in seiner in Kraft getretenen Fassung Rechnung getragen. So ist im letztmöglichen Augenblick die Regelung des § 305 SGB V über den Anspruch der Versicherten an die Krankenkassen auf Auskunft über in Anspruch genommene Leistungen und deren Kosten mit dem erklärten Ziel verändert worden, eine auf die

einzelnen Versicherten bezogene Speicherung und Auswertung von medizinischen Daten auszuschließen. Dem selben Ziel dient die Klarstellung in § 295 Abs. 2 SGB V, wonach künftig die Kassenärztlichen Vereinigungen den Kassen die Abrechnungsdaten zwar fallbezogen, aber ausdrücklich nicht versichertenbezogen übermitteln sollen.

Ich begrüße, daß der Bundesbeauftragte für den Datenschutz — u. a. auf meine Anregung hin — hier erfolgreich interveniert hat. Damit ist klargestellt, daß der Gesetzgeber die Kassen zwar instandsetzen will, die Leistungserbringer zu überprüfen, nicht aber dazu, die einzelnen Versicherten zu überprüfen. Vor allem auch deshalb gilt es, der verbreiteten Praxis, über das gesetzliche Maß hinaus und sogar gegen den ausdrücklichen Gesetzeswortlaut Versichertendaten zu erheben und auszuwerten, einen Riegel vorzuschieben. Ich habe deshalb den Bundesbeauftragten für den Datenschutz und die anderen Datenschutzbeauftragten wegen einer gemeinsamen Initiative angeschrieben. Ich hoffe, daß der Senat und insbesondere die Senatorin für Arbeit und Frauen, in deren Aufgabenbereich die Rechtsaufsicht über die Krankenkassen und die Kassenärztlichen Vereinigungen fällt, mich dabei unterstützen.

10.3.3 Abrechnung mit Chipkarten

Selbst bei einem Erfolg dieser Bemühungen sehe ich weiterhin die von mir unter Ziffer 2.6.2 meines 14. Jahresberichts dargestellte Gefahr, daß die Krankenversichertenkarte, die nunmehr zum 01. 01. 1995 flächendeckend — und zwar nicht mehr bloß als Magnetstreifenkarte, sondern als Chipkarte — eingeführt werden und die Krankenscheine ersetzen soll, zu einer ausufernden, nicht mehr kontrollierbaren Speicherung und Auswertung von Gesundheitsdaten der Krankenversicherten durch öffentliche und nicht-öffentliche Stellen führen könnte. Zwar hat das GSG 93 an dem Verbot des § 291 SGB V festgehalten, auf der Krankenversichertenkarte medizinische Daten der Versicherten zu speichern. Jedoch ist auffällig, mit welchen Argumenten die für die Entwicklung der Krankenversichertenkarte Verantwortlichen die Entscheidung für den „als Durchbruch einer innovativen Technik" gefeierten Einsatz der Chipkartentechnik begründen. Da ist die Rede von dem Potential der Anwendung für die Chipkartentechnik im Gesundheitswesen oder davon, über die Förderung der DV-Anwendung in den Arztpraxen einen Kreislauf des Datenaustausches in Gang zu setzen. Als Anwendungsbeispiele werden der medizinische Notfallausweis, der Impfpaß, der Röntgenausweis, der „Medical Record" für Risikopatienten und das elektronische Rezept genannt. Die Kassenärztliche Bundesvereinigung hat Anfang 1992 in dankenswerter Deutlichkeit erklärt, man präferiere die Chipkarte auch deshalb, weil sie die Erweiterung des Datenbestandes auf medizinische Daten eröffne, sollte dies eines Tages legal möglich sein.

Es ist nicht meine Aufgabe und auch nicht mein Bestreben, alle aufgeführten Beispiele der Speicherung medizinischer Daten auf Chipkarten abzulehnen. Ich will aber doch deutlich machen, daß alle diese Anwendungsmöglichkeiten vom geltenden Recht nicht gedeckt sind — und dies mit guten Gründen. Die Speicherung medizinischer Daten auf Chipkarten wirft eine Fülle ungelöster datenschutzrechtlicher Fragen auf. Solange diese nicht zufriedenstellend beantwortet sind, ist es zum Schutz der ärztlichen Schweigepflicht und des informationellen Selbstbestimmungsrechts der Versicherten geboten, das Verbot aufrecht zu erhalten. Ein unkontrollierter Zugang zu den auf Chipkarte gespeicherten Gesundheitsdaten könnte insbesondere unverantwortbare Nachteile für Sozialstatus, Berufsaussichten und Versicherungsschutz der Angehörigen von gesundheitlichen Risikogruppen mit sich bringen.

Würden mit Hilfe der Chipkartentechnik schließlich auch Ergebnisse von Genomanalysen gespeichert und zugänglich gemacht (s. a. 11. Jahresbericht, Ziffer 2.4 und 12. Jahresbericht, Ziffer 2.7.3), so täte sich vollends die „schrecklich schöne medizinisch/datentechnische Wunderwelt des gläsernen Patienten" auf. Dies sollte man nicht als unrealistische, technikferne Horrorvision abtun: Die Erfahrung zeigt, daß das technisch Machbare nach praktischer Umsetzung drängt. Der entsprechende Druck auf den Gesetzgeber wird nicht mehr lange auf sich warten lassen. Es gilt, die Entwicklung wachsam zu begleiten und die nötigen Diskussionen in der demokratischen Öffentlichkeit anzuregen.

10.4 Verkauf von Arztpraxen: Einwilligung der Patienten (s. a. 14. Jahresbericht, Ziffer 3.6, Ergebnis)

In der langjährigen Diskussion darüber, ob Ärzte ihre Patientenkartei zusammen mit ihrer Praxis verkaufen dürfen, ohne die einzelnen Patienten zuvor um ihr Ein-

verständnis gebeten zu haben, hat der Bundesgerichtshof (NJW 92, 737) jetzt entschieden, daß ein Arzt, der zuvor nicht die Einwilligung der Patienten eingeholt habe, damit das informationelle Selbstbestimmungsrecht der Patienten und die ärztliche Schweigepflicht verletze.

Die Ärztekammer und die Zahnärztekammer Bremen haben ihre Mitglieder über die Entscheidung unterrichtet. Ich habe dennoch den Senator für Gesundheit, Jugend und Soziales gebeten, im Wege der Rechtsaufsicht über die Kammern tätig zu werden, da die bloße Unterrichtung allein nicht ausreiche, um die langjährig eingefahrene rechtswidrige Praxis grundlegend zu ändern, zumal dies mit ökonomischen Nachteilen (Kaufpreisverlust, Kosten für das Anschreiben der Patienten etc.) verbunden sein könne. Der Senator für Gesundheit, Jugend und Soziales teilt meine Auffassung, daß die Berufsordnung für Ärzte eine Regelung treffen müsse und beabsichtigt, in den Entwurf eines Änderungsgesetzes zum Heilberufsgesetz eine entsprechende Verpflichtung aufzunehmen. Entsprechende Erörterungen werden auch in anderen Bundesländern geführt. Die dort gemachten Erfahrungen veranlassen mich zu den Hinweisen, daß

- sichergestellt sein muß, daß der die Praxis übernehmende Arzt ohne Einwilligung des jeweiligen Patienten keinen Zugriff auf dessen Daten haben darf, d. h., daß ein vertragliches Verbot nicht ausreicht,
- die Einwilligung nur dann wirksam ist, wenn sie sich konkret auf den Verkauf an einen namentlich genannten Käufer bezieht, d. h., daß ein vorsorglich für den Fall einer späteren Veräußerung an einen nicht genannten Arzt unterschriebenes Formular nicht ausreicht.

Anders lautende Regelungen oder Vordrucke würden den Verdacht erregen, als wolle man mit ihnen der höchstrichterlichen Entscheidung zwar formell Genüge tun, sie in Wirklichkeit aber zu unterlaufen versuchen.

11. Umweltschutz und Stadtentwicklung

11.1 Einsichtsrecht in Umweltakten: Entwurf eines Umweltinformationsgesetzes

Der Rat der Europäischen Gemeinschaften (EG) hat am 07. Juni 1990 eine Richtlinie über den freien Zugang zu Informationen über die Umwelt beschlossen. Danach soll in der EG allen natürlichen und juristischen Personen der freie Zugang zu den bei Behörden in Schrift, Bild, Ton oder DV-Form verfügbaren Informationen über den Zustand der Umwelt, Tätigkeiten oder Maßnahmen, die diesen Zustand negativ beeinflussen oder negativ beeinflussen können, sowie über Tätigkeiten oder Maßnahmen zum Schutz der Umwelt gewährleistet werden. In bestimmten, genau bezeichneten Fällen kann gerechtfertigt sein, erbetene umweltbezogene Informationen zu verweigern. Insbesondere können die Mitgliedstaaten vorsehen, daß ein Antrag auf Zugang zu einer derartigen Information abgelehnt wird, wenn u. a. die Vertraulichkeit personenbezogener Daten bzw. Akten berührt ist. Die Mitgliedstaaten waren verpflichtet, bis spätestens zum 31. Dezember 1992 die erforderlichen Rechts- und Verwaltungsvorschriften zu erlassen, um dieser Richtlinie nachzukommen.

Der Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit hat den Landesregierungen Ende 1991 sowie im Sommer 1992 Arbeitsentwürfe zu einem Umweltinformationsgesetz zugesandt. Ein neuer Entwurf liegt seit Dezember 1992 vor. Ich habe gegenüber dem Senator für Umweltschutz und Stadtentwicklung Stellung genommen.

Zu begrüßen ist, daß — ausgehend von der EG-Richtlinie — mit dem Entwurf das seit Jahren diskutierte Zugangsrecht des Bürgers zu Verwaltungsinformationen im Umweltbereich gewährleistet werden soll, weil die Herstellung von Öffentlichkeit Voraussetzung für die Ausübung demokratischer Kontroll-, Beteiligungs- und Mitwirkungsbefugnisse ist. Das mit dem Gesetz verfolgte Ziel der Erhöhung der Transparenz der Verwaltung auf dem Gebiet des Umweltschutzes steht dem Datenschutz nicht entgegen; vielmehr ist die Informationsfreiheit ein notwendiges Korrelat zum Datenschutz.

Der Gesetzentwurf regelt das Informationszugangsrecht nicht nur gegenüber den Behörden des Bundes, sondern auch gegenüber denen der Länder, Gemeinden und Gemeindeverbände. Dem Bund obliegt jedoch lediglich, materiellrechtliche Regelungen im Umweltrecht zu schaffen, soweit seine Kompetenz gegeben ist. Er verfügt beim Informationszugangsrecht in den Ländern und Kommunen weder

über eine ausschließliche noch über eine konkurrierende Regelungskompetenz, so daß es den Ländern obliegt, im Rahmen ihrer Gesetzgebungskompetenz nach Art. 70 Grundgesetz (GG) den Verpflichtungen der EG-Richtlinie nachzukommen. Der bremische Gesetzgeber ist also gehalten, eigenständige Regelungen zu schaffen.

Grundsätzlich muß der Antragsteller wählen können, ob ihm Auskunft erteilt oder ob ihm Informationsträger zur Verfügung zu stellen sind. Diese Wahlmöglichkeit wird jedoch faktisch negiert, wenn — wie im Bundesentwurf vorgesehen — der Anspruch auf die Auskunftserteilung beschränkt ist, wenn z. B. die Auskunft auch ohne den Informationsträger verständlich wäre. Hierüber entscheidet die Verwaltungsbehörde. Die Wahlmöglichkeit kann ebenfalls aufgehoben werden, wenn die Behörde eine Akteneinsicht ablehnt mit der Begründung, eine Aussonderung schutzwürdiger Daten sei mit einem unvertretbaren Aufwand verbunden, ohne daß der Bürger dies überprüfen kann. Außerdem ist anzunehmen, daß die dann zu erfolgende Auskunftserteilung wegen möglicher Nachfragen des Bürgers noch aufwendiger wird. Klarzustellen ist im übrigen, daß das „Zurverfügungstellen von Informationen" — so die EG-Richtlinie — das klassische Akteneinsichtsrecht beinhaltet.

Die den Mitgliedstaaten nach der EG-Richtlinie überlassene Entscheidungsbefugnis, ob und inwieweit der Informationszugang unter bestimmten Voraussetzungen ausgeschlossen bzw. beschränkt werden kann, legt der Referentenentwurf äußerst extensiv aus.

Das Informationszugangsrecht wird nach dem Gesetzentwurf generell verwehrt, soweit dadurch Betriebs- und Geschäftsgeheimnisse zugänglich gemacht werden. Dies geht jedoch zu weit: Das Betriebs- und Geschäftsgeheimnis sollte im Sinne von § 22 Abs. 2 und 3 Chemikaliengesetz (ChemG) definiert werden. Danach unterliegen Angaben nur dann einem Betriebs- und Geschäftsgeheimnis, wenn der Betroffene begründet darlegt, daß ihre Verbreitung ihm betrieblich oder geschäftlich schaden könnte. Darüber hinaus empfiehlt es sich festzulegen, daß ein wichtiges Betriebs- oder Geschäftsgeheimnis nicht gegeben ist, wenn durch die Offenbarung kein oder nur ein unwesentlicher wirtschaftlicher Schaden entsteht. Das Informationszugangsrecht wäre demnach nur insoweit eingeschränkt, als dadurch ein Betriebs- oder Geschäftsgeheimnis offenbart wird und schutzwürdige Belange des Betroffenen überwiegen. Außerdem halte ich es für erforderlich, die Voraussetzungen festzulegen, unter denen eine Offenbarung von Betriebs- oder Geschäftsgeheimnissen schutzwürdigen Belangen des Betroffenen nicht entgegenstehen.

Der Referentenentwurf schränkt den Informationszugangsanspruch auch ein, soweit durch das Bekanntwerden der Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Eine Offenbarung ist nur dann vorgesehen, wenn der Zugang zu Informationen über die Umwelt unvermeidbar mit der Offenbarung des Namens, des Berufs, der Branchen- oder Geschäftsbezeichnung des Verursachers einer Umweltbeeinträchtigung verbunden ist, es sei denn, daß schutzwürdige Interessen des Verursachers überwiegen.

Auch diese Regelung halte ich unter Berücksichtigung des durch die EG-Richtlinie den Mitgliedstaaten überlassenen Gestaltungsspielraums für zu restriktiv. Der Katalog der personenbezogenen Daten, die keine schutzwürdigen Belange der Verursacher tangieren, kann ohne weiteres ausgeweitet werden. Schutzwürdige Belange des Betroffenen stehen einer Offenbarung insbesondere dann nicht entgegen, wenn sich aus einer Umweltakte die Tatsache ergibt, daß der Betroffene als Gutachter, Sachverständiger oder in vergleichbarer Weise eine Stellungnahme abgegeben hat.

Die vorgesehene Ablehnung der Offenbarung von Unterlagen, die von einem Dritten übermittelt worden sind, der dazu nicht verpflichtet war, nutzt den Gestaltungsspielraum der EG-Richtlinie ebenfalls nicht aus. Um dem Zugangsrecht Rechnung zu tragen, wäre es z. B. möglich, Informationen, die ein Dritter an die Behörde weitergegeben hat, ohne dessen personenbezogene Daten zu offenbaren.

Nach dem Referentenentwurf können für alle Amtshandlungen nach diesem Gesetz Gebühren und Auslagen erhoben werden. Dagegen erlaubt die EG-Richtlinie nur, angemessene Gebühren ausschließlich für die Gewährung der Informationen zu erheben. Ich halte eine entsprechende Änderung des Entwurfs für erfor-

derlich und rege an, auch bei der Gewährung des Informationszugangs auf die Erhebung von Gebühren und Auslagen zu verzichten.

Die EG-Richtlinie schreibt nicht vor, nach welchen zeitlichen Abständen die Öffentlichkeit regelmäßig über den Zustand der Umwelt informiert werden soll. Der im Referentenentwurf vorgesehene vierjährige Abstand reicht nicht aus, den Zielen der EG-Richtlinie Rechnung zu tragen. Ein jährlicher oder Zweijahresbericht erscheint mir angemessen.

Des weiteren halte ich es zur Wahrnehmung des Informationszugangsrechts für geboten, die Öffentlichkeit regelmäßig auch darüber zu unterrichten, bei welchen Behörden Informationen über die Umwelt bereitliegen.

Insgesamt bleibt festzustellen, daß der Gesetzentwurf viel zu spät erarbeitet worden ist, zumal der Fristablauf spätestens Mitte 1990 bekannt war. Außerdem ist der Entwurf in wesentlichen Punkten viel zu restriktiv und wird den Intentionen der EG-Richtlinie nicht gerecht.

Am 31. Dezember 1992 ist die Frist abgelaufen, bis zu der die Mitgliedstaaten verpflichtet waren, entsprechende gesetzliche Regelungen zu erlassen. Die EG-Richlinie gilt nunmehr unmittelbar, d. h. sie ist in der bremischen Verwaltung umzusetzen. Aus diesem Grunde hat der Senator für Umweltschutz und Stadtentwicklung einen Erlaß für alle seiner Aufsicht unterstehenden Umweltbehörden herausgegeben, der die praktische Umsetzung der EG-Richtlinie gewährleisten soll. Dieser Erlaß sieht im wesentlichen vor, bei der Bearbeitung von Anträgen auf Zugang zu Informationen über die Umwelt pauschal die Vorschriften des Verwaltungsverfahrens- und des Datenschutzrechts zu beachten, unabhängig davon, ob schutzwürdige Belange der Betroffenen tangiert sind oder nicht.

Ich habe daher angeregt, diesen Erlaß insoweit zu ergänzen, als ein Auskunftsanspruch nicht ausgeschlossen ist, wenn der Zugang zu Informationen über die Umwelt unvermeidbar mit der Offenbarung des Namens, des Berufs, der Branchen- oder Berufsbezeichnung des Verursachers verbunden ist, es sei denn, daß besonders schutzwürdige Belange des Betroffenen überwiegen. Außerdem sollte deutlich erkennbar sein, daß der Informationszugang nach Wahl des Antragstellers entweder durch Auskunft aus oder Einsicht in Umweltakten oder andere Datenträger zu gewähren ist. Weil nicht nur die Behörden des Umweltressorts über Umweltinformationen verfügen, sollte der zu überarbeitende Erlaß als Senatsbeschluß für alle Teile der bremischen Verwaltung, bei denen sich unter den Anwendungsbereich der Richtlinie fallende Unterlagen befinden, verbindlich angeordnet werden.

Der Senator für Umweltschutz und Stadtwentwicklung ist nicht bereit, den bereits herausgegebenen Erlaß zu ändern, weil damit zu rechnen sei, daß das neue Umweltinformationsgesetz ohnehin im Laufe des Jahres in Kraft treten wird. Im übrigen habe er seinen Erlaß den anderen Ressorts zugesandt und anheimgestellt, entsprechende Regelungen zu treffen. Im Erlaß selbst sind auch die anderen senatorischen Behörden angesprochen.

Der Senat muß prüfen, welche gesetzlichen Vorschriften im Bereich der Landeskompetenz zu erlassen sind, wie dies in Einzelbereichen, z. B. für die Einsicht in das Wasserbuch nach dem Bremischen Wassergesetz, bereits geschehen ist. Ich werde die Praxis genau verfolgen und darauf achten, daß dieses neue Instrument der Bürgerinformation und -partizipation nicht durch bürokratische Hemmnisse entwertet wird.

11.2 Die „codierte Mülltonne"

Die Umweltbehörde plant eine individuelle Müllgebührenabrechnung, die abhängig von der Häufigkeit der Entleerung der Mülltonne sein soll. Danach sollen alle Mülltonnen mit einem haushaltsbezogenen Code versehen werden, der bei Müllentleerungen mit Hilfe eines Scanners abgelesen wird. Insoweit soll die sich auf dem Müllfahrzeug befindliche Datenverarbeitungsanlage speichern, an welchem Tage und zu welcher Uhrzeit welche „codierte Mülltonne" entleert worden ist. Diese Daten sollen mit Hilfe des individuellen Codes mit den Adreßdaten der Gebührenpflichtigen zum Zwecke der Müllgebührenabrechnung verknüpft werden.

Zu diesem Zweck hat bereits im vergangenen Jahr ein Versuch in Bremen-Horn stattgefunden. Ich habe anläßlich dieser Probephase gegenüber dem Senator für Umweltschutz und Stadtentwicklung dargelegt, daß bei einer späteren haushalts-

bezogenen Speicherung dieser Daten der in § 19 Abs. 3 des Ortsgesetzes über die Abfallbeseitigung in der Stadtgemeinde Bremen abschließende Datenkatalog entsprechend ergänzt werden muß. In den Datenkatalog muß aufgenommen werden, an welchem Tage und — soweit dies erforderlich ist — zu welcher Uhrzeit die Entleerung vorgenommen worden ist.

Anfang Februar 1993 hat der Senator für Umweltschutz und Stadtentwicklung den angekündigten Novellierungsentwurf vorgelegt. In einem neuen § 27 sollen die Datenverarbeitungsregelungen geschaffen werden. Allerdings regelt dieser Entwurf in § 27 Abs. 3 Nr. 4 lediglich, die Abfuhr- und Entleerungshäufigkeit zu speichern. Ich habe darauf gedrängt, auch den Tag der Entleerung in den Datenkatalog aufzunehmen. Soweit begründet dargelegt wird, daß auch die Speicherung der Uhrzeit erforderlich ist, wäre der Datenkatalog entsprechend zu ergänzen. Der Senator für Umweltschutz und Stadtentwicklung hat zugesagt, meine Vorschläge zu berücksichtigen.

11.3 Datenschutz im Naturschutzgesetz

Der Senator für Umweltschutz und Stadtentwicklung hat mir den Entwurf einer Änderung des Bremischen Naturschutzgesetzes vorgelegt. Wesentlicher Teil dieser Änderungen ist die Schaffung bereichsspezifischer Datenverarbeitungsregelungen.

Der Entwurf ist für den Bürger wichtig, weil er nunmehr normenklare Regelungen über die Erhebung personenbezogener Daten derjenigen enthält, die bei der Aufstellung von Landschaftsprogrammen und Landschaftsplänen Bedenken und Anregungen vorgebracht haben. Des weiteren legt der Entwurf Auskunftspflichten von Eigentümern und sonstigen Nutzungsberechtigten von Grundstücken fest, die z. B. im Geltungsbereich eines Landschaftsplanes liegen. Darüber hinaus enthält der Entwurf die Befugnis, personenbezogene Daten aus dem Liegenschaftskataster zu erheben.

Während die Art der Datenerhebung normenklar festgelegt worden ist, habe ich empfohlen, die Zweckbestimmungen eindeutig im Gesetz zu definieren. Es reicht nicht aus, wenn lediglich in der Begründung zu dem Entwurf aufgeführt wird, daß die Daten zur Ermittlung entschädigungsrechtlicher Auswirkungen, landschaftsplanerischer Festsetzungen und Unterschutzstellungen sowie im Rahmen der Beteiligungsverfahren verarbeitet werden dürfen. Außerdem halte ich es für erforderlich festzulegen, daß die Daten der Verursacher von beantragten oder angezeigten Eingriffen in Natur und Landschaft zur Durchführung der jeweiligen Antrags- oder Anzeigeverfahren verarbeitet werden dürfen.

Eine Datenübermittlung an andere öffentliche Stellen will der Entwurf „zur rechtmäßigen Aufgabenerfüllung der empfangenden Stelle" erlauben, soweit diese Stellen in den Verfahren zur Aufstellung von Landschaftsprogrammen und Landschaftsplänen zu beteiligen sind. Dies soll auch gelten, wenn Teile von Natur und Landschaft durch Rechtsverordnung z. B. zum Naturschutzgebiet, Landschaftsschutzgebiet, Naturdenkmal oder geschützten Landschaftsbestand erklärt werden sollen.

Aus dieser Datenübermittlungsregelung läßt sich jedoch nicht präzise erkennen, welchen öffentlichen Stellen im Rahmen der Verfahren die genannten personenbezogenen Daten übermittelt werden dürfen. Ich halte es daher für erforderlich, die für die jeweiligen Verfahren als Adressaten in Frage kommenden öffentlichen Stellen im einzelnen zu benennen.

Des weiteren enthält der Entwurf eine Regelung, wonach die oberste Naturschutzbehörde ermächtigt wird, durch Rechtsverordnung im Einvernehmen mit dem Senator für Inneres und dem Landesbeauftragten für den Datenschutz zu bestimmen, welche sonstigen Daten erhoben und weiterverarbeitet werden dürfen. Hierzu habe ich darauf verwiesen, daß es mir nur obliegt, Empfehlungen zur Verbesserung des Datenschutzes zu geben sowie insbesondere den Senat und die einzelnen Senatoren in Fragen des Datenschutzes zu beraten. Diese Aufgabendefinition schließt ein formelles Einvernehmen aus, so daß ich empfohlen habe, sie durch ein Anhörungsrecht des Landesbeauftragten für den Datenschutz zu ersetzen. Die senatorische Behörde hat den Gesetzentwurf erneut überarbeitet und dabei meine Anregungen im wesentlichen berücksichtigt.

11.4 Einwenderdaten in Bebauungsplänen (s. a. 13. Jahresbericht, Ziffer 2.8.4, Ergebnis)

In meinem 13. Jahresbericht habe ich darüber berichtet, daß auf die namentliche Nennung von Einwendern in als Bürgerschaftsdrucksache veröffentlichten Mitteilungen des Senats an die Bremische Bürgerschaft aufgrund eines Urteils des Bundesverfassungsgerichts vom 24. Juli 1990 — 1 BvR 1244/87 — verzichtet werden muß. Nach diesem Urteil unterliegen die Daten einer besonderen Zweckbindung, die ein Einwendungsführer der Planfeststellungsbehörde preisgibt, um ihr eine sachgerechte Beurteilung der geltend gemachten Einwendung zu ermöglichen. Das Gericht hatte seinerzeit festgestellt, daß das Zweckbindungsprinzip durch eine **öffentliche Bekanntmachung** der nichtanonymisierten Daten unterlaufen und damit in das Persönlichkeitsrecht der Betroffenen eingegriffen werde.

Nach Erörterungen im Datenschutzausschuß der Bremischen Bürgerschaft hat der Senator für Umweltschutz und Stadtentwicklung im Einvernehmen mit der Bürgerschaftsverwaltung und mir festgelegt, die eingegangenen Bedenken und Anregungen einschließlich der hierzu abgegebenen Stellungnahmen nicht mehr als integrierten Bestandteil des Berichtes für die Deputation für Stadtentwicklung zu behandeln, sondern diese in einer **gesonderten Anlage** des Berichtes aufzuführen. Die Bürgerschaftsverwaltung wird gebeten sicherzustellen, daß künftig die vom Senat an die Stadtbürgerschaft weitergeleiteten Mitteilungen des Senats einschließlich des Berichtes der Deputation für Stadtentwicklung mit Anlage (Bedenken und Anregungen, soweit welche eingegangen sind) nur noch ohne die Anlage (Bedenken und Anregungen mit dazu abgegebenen Stellungnahmen einschließlich der Stellungnahme des zuständigen Beirates) in die entsprechende offizielle Bürgerschaftsdrucksache (gelbe Farbe) aufgenommen werden.

Die Bürgerschaftsverwaltung will weiterhin veranlassen, daß diese Anlage (in einem anderen Farbton) aus datenschutzrechtlichen Gründen nur den Stadtbürgerschaftsmitgliedern ausgehändigt wird. Diese Aushändigung muß vor Beschlußfassung über die Bauleitplanung in der Stadtbürgerschaft erfolgen, damit gewährleistet bleibt, daß die Mitglieder der Stadtbürgerschaft die Möglichkeit haben, die eingegangenen Bedenken und Anregungen einschließlich dazu ergangener Stellungnahmen in ihre Entscheidungsfindung einzubeziehen. Die Bürgerschaftsverwaltung hat gegenüber dem Datenschutzausschuß erklärt, daß sie mit diesem Verfahren einverstanden ist. Die neue Handhabung gilt (nur) für neu eingeleitete Planverfahren.

12. Wirtschaft, Mittelstand und Technologie

12.1 Wählerverzeichnis als Mitgliederverzeichnis der Arbeitnehmerkammern (s. a. 10. Jahresbericht, Ziffer 5.12.2)

In meinem 10. Jahresbericht habe ich auf die fehlenden rechtlichen Voraussetzungen für die Übermittlung von Arbeitnehmerdaten durch die Arbeitgeber an die mit der Durchführung der Kammerwahlen beauftragten Wahlvorstände hingewiesen. Es war zwar in der Wahlordnung eine entsprechende Regelung enthalten, allerdings fehlte dafür die gesetzliche Grundlage.

Das geänderte Arbeitnehmerkammergesetz vom 15. Dez. 1992 (Brem.GBl.S.670) ist am 1. Januar 1993 in Kraft getreten. Der Senator für Wirtschaft, Mittelstand und Technologie hat mich an den vorbereitenden Arbeiten zum Entwurf dieses Gesetzes beteiligt. Nach ausführlichen Gesprächen mit der senatorischen Behörde und den Kammern waren normenklare Formulierungen für die Datenverarbeitung der Arbeitnehmerkammern und der Wahlvorstände sowie die Nutzung der Mitgliederverzeichnisse eingearbeitet worden. Im Gesetzgebungsverfahren ist leider die entsprechende Vorschrift unberücksichtigt geblieben, obwohl der zuständige Senator und die Kammern ausführlich dargelegt haben, daß die Kammern ohne die Mitgliederverzeichnisse ihre gesetzlichen Aufgaben nicht erfüllen können.

Ich werde die Nutzung der Wählerdaten als Mitgliederdatei der Kammern ohne entsprechende gesetzliche Ermächtigung nur noch für die bevorstehende Wahl hinnehmen. Diese Festlegung ist in § 44 der Wahlordnung vom 12. Febr. 1993 (Brem.GBl.S.48) ausdrücklich statuiert. Soll die bisherige Praxis beibehalten werden, erwarte ich, daß der Senator für Wirtschaft, Mittelstand und Technologie — wie zugesagt — unverzüglich nach der Wahl eine Revision des Gesetzes initiiert. Dabei ist präzise festzulegen, welche Daten aus den Wählerverzeichnissen an die Kammern für die Mitgliederlisten übermittelt werden dürfen.

13. Finanzen

13.1 Die Landeshauptkasse als Sammelstelle für Belege

Die Landeshaushaltsordnung (LHO) regelt die Haushaltsaufstellung, den Haushaltsvollzug, die Rechnungslegung sowie die Rechnungsprüfung in der Freien Hansestadt Bremen. Da diese Regelungen z. T. generalklauselartig formuliert sind, ist der Senator für Finanzen befugt (z. T. im Benehmen mit dem Rechnungshof), Verwaltungsvorschriften zu erlassen. Die Verwaltungsvorschriften zu einigen Paragraphen sind sehr umfangreich und detailliert ausformuliert.

Im Mai 1990 hat der damalige Landesbeauftragte für den Datenschutz die Verwaltungsvorschriften zu § 70 LHO auf ihre Vereinbarkeit mit dem Bremischen Datenschutzgesetz hin untersucht und daraufhin für den Haushaltsvollzug seiner Behörde verfügt, den Kassenanordnungen keine Einzelbelege mehr beizufügen. § 70 LHO bestimmt lediglich, daß die Zahlungen von Kassen und Zahlstellen nur auf Grund schriftlicher Anordnung des zuständigen Senators oder der von ihm ermächtigten Dienststelle angenommen oder geleistet werden dürfen und daß der Senator für Finanzen Ausnahmen zulassen kann.

Die zugehörigen Verwaltungsvorschriften gehen darüber hinaus und verlangen, daß allen Kassenanordnungen die jeweiligen Belege (sog. **begründende Unterlagen)** beizufügen sind. Aus ihnen sollen der Zweck und der Anlaß der Einzahlung oder Auszahlung so deutlich erkennbar sein, daß die ihr zugrundeliegenden Verwaltungsmaßnahmen zweifelsfrei ersichtlich sind, und dies, obwohl diese Informationen auch in der Kassenanordnung selbst anzugeben sind. Ausnahmen von der Beifügungspflicht läßt die Verwaltungsvorschrift nur nach Bestimmung des Senators für Finanzen im Einvernehmen mit dem Rechungshof zu.

Ich sehe in dieser Praxis einen Verstoß gegen das Gebot der Erforderlichkeit bei der Datenübermittlung. Mit den vorgeschriebenen Anlagen wird an die Kassen — insbesondere an die Landeshauptkasse — über die Angaben in der Kassenanordnung hinaus eine Vielzahl von auch personenbezogenen Daten übermittelt, die diese selbst für ihre Aufgabenerfüllung, d. h. die Annahme oder Auszahlung eines Betrages und dessen Buchung, nicht benötigen, etwa Informationen über die Abwicklung einer Dienstreise (einschl. der Angaben über Hotel, evtl. Ferngespräche, Benutzung der Minibar), die Gewährung von Beihilfen und Zuschüssen (einschl. der Angaben über die Prüfung der Bedürftigkeit), die Abrechnung von Dienstunfällen usw. Nach meiner Ansicht reicht die ausgefüllte Kassenanordnung völlig aus. Die Belege werden ausschließlich deshalb mitgeschickt, um die Prüfung durch den Rechnungshof zu erleichtern. Dieser Zweck reicht jedoch nicht aus, um die Übermittlung von teilweise sogar sensiblen Daten an die Kasse zu legitimieren.

Ich habe den Senator für Finanzen gebeten, die Verwaltungsvorschriften in diesem Punkt zu korrigieren. Er will jedoch zunächst mit den übrigen Länderfinanzverwaltungen dieses Problem erörtern. Im übrigen hat er auf das zukünftige automatisierte Mittelbewirtschaftungsverfahren (s. u. Ziffer 13.2) verwiesen, das ohnehin auf die Beifügung der begründenden Unterlagen verzichtet.

Ich bin der Auffassung, daß Länderabsprachen und die beabsichtigte Einführung eines neuen EDV-gestützten Haushaltsverfahrens eine Verzögerung der Problemlösung nicht rechtfertigen und die derzeitige Praxis sofort eingestellt werden sollte. Die Rechnungsprüfung wird dadurch nicht behindert. Nach der gegebenen Rechtslage sind die Behörden und Dienststellen selbst und nicht Dritte, wie etwa die Landeshauptkasse, verpflichtet, auf Anforderung des Rechnungshofs die Unterlagen für ihren Verantwortungsbereich prüfungsfähig zur Einsicht vorzulegen.

13.2 Datensicherung beim neuen Haushalts- und Mittelbewirtschaftungssystem

Im Rahmen einer Neugestaltung des bremischen Haushalts-, Kassen- und Rechnungswesens (HKR), die eine Optimierung dieser Verfahren in einem Gesamtverfahren für das „integrierte bremische Finanzwesen" vorsieht, wird das Softwareprodukt „Mittelbewirtschaftungssystem (MBS-PC)" eingesetzt. Die vorliegende aktuelle Version bietet Unterstützung bei der Führung der Haushaltsüberwachungslisten, der Mittelbewirtschaftung und beim Druck von Kassenanordnungen. Der ADV-Ausschuß hat im August 1992 auf Antrag des Senators für Finanzen der Zulassung des Produktes zugestimmt. In meiner Stellungnahme zum MBS-Verfahren habe ich auf folgende, auch für andere PC-Anwendungen exemplarische Probleme hingewiesen:

— Paßwortorganisation

Die softwareimmanente Paßwortorganisation entspricht nicht den Anforderungen des § 6 Abs. 2 Bremisches Datenschutzgesetz (BrDSG), insbesondere nicht den Vorschriften über Zugriffs-, Übermittlungs- und Eingabekontrolle. Die Paßwortvergabe erfolgt zwar zweistufig für den „privilegierten Sachbearbeiter" und den normalen Anwender, trennt aber die Systemverwaltungs- nicht eindeutig von den Anwenderfunktionen. Der **„privilegierte Sachbearbeiter"** ist jederzeit in der Lage, alle Benutzernummern, -Namen und -Paßwörter zu bearbeiten. Er kann sogar mit der Kennung eines anderen Benutzers Daten eingeben oder verändern. Er hat demzufolge über jedes Paßwort Zugang zum System, wobei seine eigenen Aktivitäten keiner Kontrolle unterliegen, da eine Protokollierung nicht vorgesehen ist. Eine vom Senator für Finanzen vorgeschlagene, nicht näher ausgeführte organisatorische Sicherstellung, daß Änderungen an Nummer, Name und Paßwort nur zusammen mit dem Benutzer vorgenommen werden, kann die erforderliche technische Lösung nicht ersetzen.

— Auswertung von Dateien

Die Daten werden auf den Orginaldateien zwar grundsätzlich verschlüsselt; diese Verschlüsselung läßt sich aber durch den Sachbearbeiter aufheben. Daher sind mit Standardprogrammen die Daten für beliebige Zwecke auswertbar. Der Senator für Finanzen schlägt die Sperrung des entsprechenden Moduls vor. Bis zum Redaktionsschluß hatte ich keine Bestätigung, daß ein entsprechender Auftrag an die Softwarefirma ergangen ist.

— Individuelle Auswertungen

Buchungen können über ein Zusatzfeld mit frei gestaltbaren individuellen Verschlüsselungen und Indizes versehen werden. Auch dies ermöglicht unkontrollierbare individuelle Auswertungen. Auch hier will der Senator für Finanzen statt mit technischen lediglich mit organisatorischen Maßnahmen die mögliche rechtswidrige Nutzung verhindern.

— Löschung

Nicht mehr benötigte personenbezogene Daten können nur durch Aufruf eines speziellen Moduls physikalisch gelöscht werden. Das hat zur Folge, daß sie bis dahin wieder lesbar gemacht und damit weiter genutzt werden können. Wird die Information nicht endgültig zum Verschwinden gebracht, sondern nur ihre Verwertbarkeit eingeschränkt, liegt zwar eine Sperrung, aber keine Löschung i. S. v. § 2 Abs. 2 Nr. 6 BrDSG vor. Anders ausgedrückt: Nach § 20 Abs. 3 BrDSG erforderliche Löschungen können in den meisten Fällen mit den in Standard-Software enthaltenen normalen „Löschfunktionen" nicht getätigt werden. § 20 Abs. 3 BrDSG setzt voraus, daß die Löschung nicht mehr rückgängig gemacht werden kann. Auch diese Sicherungslücke will der Finanzsenator nur organisatorisch schließen.

— Leistungskontrolle

Bei jeder Buchung wird die Sachbearbeiternummer festgehalten, die auch für Leistungs- und Verhaltenskontrollen ausgewertet werden kann.

Das Mittelbewirtschaftungsprogramm wird derzeit auf PCs eingesetzt, ohne daß ein ausreichendes Datenschutzkonzept vorliegt. Eine bereits angekündigte, mir aber noch nicht vorliegende neue MBS-Version, die auch für den Einsatz im Netzwerk konzipiert ist, soll nach Informationen der Entwicklungsfirma eine gestaffelte Vergabe von Zugriffsrechten ermöglichen und damit die gravierenden Mängel der Paßwortorganisation beheben. Auch die anderen Schwachstellen sollten bei der Weiterentwicklung des Produktes ausgeräumt werden. Technische Lösungen müssen dabei klaren Vorrang vor organisatorischen Vorkehrungen haben.

13.3 Fall: „Informantengeheimnis" bei der Steuererklärung von Journalisten

Ein Journalist wurde vom Finanzamt aufgefordert, bei seinen Betriebsausgaben bzw. Werbungskosten nicht nur die aufwendungsrelevanten Daten wie z.B. Wegstrecke, Kosten für Bewirtung usw., sondern auch Namen und Anschrift des Informanten oder Auftraggebers offenzulegen. Auf seine Einwände hin erklärte die Steuerbehörde, diese Daten seien durch das Steuergeheimnis ausreichend geschützt.

Ich habe das Finanzamt auf den hohen Rang der **Pressefreiheit** nach Art. 5 des Grundgesetzes hingewiesen. In einer Reihe von Rechtsgebieten ist die **journalistisch-redaktionelle Tätigkeit** gegenüber staatlicher Kontrolle auch ausdrücklich privilegiert, sogar im Strafverfahren durch ein Zeugnisverweigerungsrecht (vgl. auch das „Medienprivileg" im Datenschutzrecht, § 41 Bundesdatenschutzgesetz — BDSG). Die Medien könnten ihre Aufgabe nicht erfüllen, wenn sie ihren Hinweisgebern und Gesprächspartnern keinen absoluten Vertrauensschutz gewähren könnten. Die Steuerverwaltung akzeptierte schließlich, daß Journalisten im Rahmen redaktioneller Tätigkeit — also nicht z.B. bei Arbeiten als Werbephotograph oder -texter — die Personalien ihrer Kontaktpartner in ihren Steuererklärungen nicht offenbaren müssen. Es genügt, wenn auf den Artikel oder den Auftrag der Redaktion verwiesen und der Name der Straße ohne Hausnummer angegeben wird. Bei kürzeren Straßen braucht auch nur das nähere Stadtgebiet beschrieben zu werden, um eine Identifizierung zu vermeiden.

13.4 Datenflüsse nach dem „Zinsabschlaggesetz"

Zahlreiche Bürger haben sich bei mir erkundigt, welche Daten zwischen den Kreditinstituten und den Steuerbehörden bei der Anwendung des sogenannten „Zinsabschlaggesetzes" fließen.

Der **Freistellungsauftrag**, der bis zu einer bestimmten Höhe den Vorsteuerabzug (30 % Zinssteuer vor der Auszahlung durch die Bank oder Sparkasse) von Guthabenzinsen unterbindet, ist gegenüber dem Kreditinstitut in einer Summe oder, wenn bei mehreren Geldinstituten Guthaben bestehen, in entsprechenden Teilbeträgen abzugeben. Der Kunde selbst kann über die Verteilung des Freibetrages entscheiden. Dieser Freistellungauftrag verbleibt bei der jeweiligen Bank oder Sparkasse. Nur auf besondere Anforderung und, wie es in der Begründung zum Gesetzestext lautet, „in ausgewählten Fällen" ist das Bundesamt für Finanzen ermächtigt, sich die Daten über die Freistellungsaufträge melden zu lassen. Wenn sich dabei Überschreitungen ergeben, wird das zuständige Finanzamt mit den weiteren Ermittlungen beauftragt. Ansonsten erfolgen keine Datenübermittlungen an die Steuerbehörden.

Auch bei der Zahlung der Zinssteuer teilt das Kreditinstitut dem Finanzamt keine personenbezogenen Daten mit. Die Überweisung erfolgt pauschal und damit anonym. Der Steuerbürger erhält von seinem Geldinstitut eine Bescheinigung über den für ihn abgeführten Steuerbetrag. Die Kreditinstitute sind allerdings auf Grund einer Anweisung des Bundesministeriums für Finanzen gehalten, den Namen, die Anschrift und die Unterschrift des **Ehepartners** bei den Freistellungsaufträgen auch in den Fällen anzugeben, in denen dieser nicht Vertragspartner der kontoführenden Bank oder Sparkasse ist. Ich halte diese Datenerhebung zumindest bei getrennter Veranlagung der Ehepartner für durch das „Zinsabschlaggesetz" nicht ausreichend begründbar. Eine endgültige und bundeseinheitliche Regelung dieser Frage steht noch aus.

14. Nicht-öffentlicher Bereich

14.1 Zugriffsprobleme bei Dialogsystemen

Bei den Stadtwerken Bremen fand im Berichtsjahr eine anlaßbezogene Datenschutzprüfung statt, die sich speziell auf den Dialogteil des soz. Kundeninformationssystems der Stadtwerke bezog. Mit Hilfe dieses Dialogsystems können von den berechtigten Mitarbeitern der Stadtwerke über Terminals Bildschirmmasken aufgerufen, Daten gelesen und eventuell geändert werden. Zugleich ist es möglich, Bildschirminhalte über Hardcopygeräte in Papierform auszugeben. Das Prüfverfahren ist noch nicht abgeschlossen.

Im Hinblick darauf, daß derartige Dialogsysteme weit verbreitet sind, möchte ich schon in diesem Bericht auf folgende **Anforderungen** hinweisen:

— Protokollierung der Systembenutzung

Zur ordnungsgemäßen Anwendung von DV-Programmen, mit denen personenbezogene Daten verarbeitet werden (§ 37 Abs. 1 Satz 3 Nr. 1 Bundesdatenschutzgesetz — BDSG), gehört auch, angemessene technisch-organisatorische Schutzmaßnahmen (§ 9 BDSG nebst Anlage) vorzusehen und ihre Beachtung „sicherzustellen". Zum „Stand der Technik", insbesondere bei Dialoganwendungen, gehört eine möglichst umfassende, differenzierte und wirksame Protokollierung

der Systembenutzung, speziell auch der Benutzer-, Zugriffs- und Eingabeaktivitäten. Über Details der Protokollierung wie z. B. Art, Inhalt, Umfang und Aufbewahrungsdauer sagt das BDSG nichts. Die speichernden Stellen müssen diese Details selbst aufgrund der Abwägung zwischen Aufwand und Schutzzweck (§ 9 Satz 2 BDSG) festlegen. Hinsichtlich der Nutzung der Protokolldaten schreibt das BDSG in § 31 eine strikte Zweckbindung vor; die Daten dürfen nur zur Datenschutzkontrolle, zur Datensicherung und zur Sicherstellung eines ordnungsgemäßen DV- bzw. Rechenzentrumsbetriebes genutzt werden. Die Protokolle sollten möglichst zeitnah, und ggf. stichprobenweise, z. B. durch den betrieblichen Datenschutzbeauftragten, überprüft werden und können nach Ablauf einer gewissen Aufbewahrungsfrist zur Vernichtung bzw. Löschung freigegeben werden. Die Aufbewahrungsdauer kann nach Art und Verwendungszweck des einzelnen Protokolls unterschiedlich geregelt werden; ein Minimum von drei Monaten sollte jedoch nicht unterschritten werden. Innerhalb des durch § 9 BDSG gesetzten Rahmens können die Einzelheiten der Protokollierung durch Betriebsvereinbarung festgelegt werden.

— Protokollierung bei automatisierten Abrufverfahren

Für automatisierte Abrufverfahren, bei denen Daten von dritten Stellen online abgerufen oder bei ihnen eingesehen werden können, sieht das BDSG in § 10 Abs. 4 Satz 3 vor, „zumindest durch geeignete **Stichprobenverfahren**" eine Übermittlungskontrolle zu gewährleisten. Ähnliches gilt nach § 10 Abs. 4 Satz 4 BDSG auch für die Übermittlung eines Gesamtdatenbestandes im Rahmen eines Stapelübertragungs-, Stapelfernverarbeitungs- oder Datenträgeraustauschverfahrens. Die Protokollierungspflicht des § 10 Abs. 4 Satz 3 und 4 BDSG dient dazu, einzelne Datenabrufe bzw. automatisierte Datenübermittlungsvorgänge auf ihre Zulässigkeit hin überprüfen zu können.

Die technische Ausgestaltung des Stichprobenverfahrens ist der speichernden Stelle überlassen. Die Größe der Stichprobe ist im Gesetz ebenfalls nicht festgelegt. Sie muß jedoch so groß bemessen sein, daß nachträgliche Überprüfungen der Zulässigkeit einzelner Datenabrufe oder Datenbestandsübermittlungen tatsächlich möglich sind. Das Verfahren sollte deshalb so gestaltet werden, daß alle Abrufer (Terminals, User) und möglichst auch alle sensiblen Abrufe/Zugriffe einbezogen sind und dazu jeweils eine signifikante Zufallsstichprobe gezogen wird. Stichproben im Promillebereich halte ich nicht für signifikant. Inhaltlich sind mindestens zu protokollieren: Datum, Uhrzeit, Empfänger/Abrufer (Terminal, User), Transaktion/Bildschirmmaske sowie Datensätze, auf die zugegriffen wurde.

Bei Abruf oder Übermittlung eines Gesamtdatenbestandes (s. o.) bezieht sich die Protokollierungspflicht global auf diesen Bestand, nicht auf die einzelnen Daten. Hier könnten anstelle eines speziellen Stichprobenverfahrens die üblichen Job-Account-und Sys-Log-Verfahren benutzt werden, die die einzelnen Vorgänge jeweils protokollmäßig festhalten.

Auch diese Protokolldaten sollten möglichst zeitnah überprüft werden; sie unterliegen ebenfalls einer strikten Zweckbindung. Die Aufbewahrungsdauer sollte in diesem Fall wenigstens ein Jahr betragen.

— Beschränkung der Zugriffsberechtigung

Zur Verringerung unberechtigter Zugriffe durch prinzipiell befugte Personen, etwa aus Neugier oder privaten Interessen, empfiehlt es sich, neben einer Protokollierung der Zugriffsaktivitäten und deren möglichst zeitnaher Überprüfung auch den Kreis der Personen, denen der Umgang mit den jeweiligen Datensätzen nach der innerbetrieblichen Aufgabenverteilung erlaubt ist, zu beschränken. Der mögliche Konflikt zwischen Kundenfreundlichkeit und Datenschutz darf nicht einseitig zu Lasten des Datenschutzes gelöst werden. Die heutigen (Groß-) Rechnersysteme bieten neben hardwaremäßigen Mitteln auch softwaremäßige Möglichkeiten für eine differenzierte, funktionsbezogene Beschränkung bzw. Kontrolle des Zugriffs auf Daten und Programme. Von diesen Möglichkeiten sollte in jedem Fall Gebrauch gemacht werden. Bei offenen oder halboffenen Auskunfts- oder Informationssystemen kommt der Zugriffs- und Benutzungskontrolle auch wegen der Gefahr einer „Verseuchung" mit Programmviren erhöhte Bedeutung zu.

14.2 Fall: Unberechtigte Schufa-Abfrage

Ein Petent beschwerte sich bei mir darüber, daß die Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) Bremen eine falsche bzw. unvollständige Angabe

gespeichert und einer Bank, mit der er keinerlei Verbindung habe, eine Kreditauskunft erteilt habe. Meine Prüfung dieser Beschwerde bei der Schufa Bremen hat ergeben, daß die monierte Datenspeicherung unvollständig und somit unrichtig war; die gespeicherten Daten wurden berichtigt. Die Berechtigung der erteilten Kreditauskunft konnte seitens der Schufa Bremen nicht dargelegt werden; ein Angestellter der anfragenden Bank hatte ohne dienstliche Veranlassung, d. h. ohne berechtigtes Interesse, mißbräuchlich (für private Zwecke) die Kreditanfrage gestellt und Auskunft erhalten; die Datenübermittlung durch die Schufa Bremen war also unzulässig.

Der Petent hat wegen dieser unzulässigen Datenübermittlung Strafantrag gegen Verantwortliche der Schufa gem. § 43 Bundesdatenschutzgesetz (BDSG) gestellt. Die Staatsanwaltschaft Bremen hat das Verfahren eingestellt; im Widerspruchsverfahren des Betroffenen gegen die Einstellungsverfügung hat die Generalstaatsanwaltschaft Bremen eine Stellungnahme von mir zu einzelnen Datenschutzfragen erbeten.

Dieser Vorgang gibt zu folgenden datenschutzrechtlichen Erwägungen Anlaß:

— Glaubhafte Darlegung des berechtigten Interesses

Das BDSG verlangt in § 29 Abs. 2 Nr. 1 a, daß sich die Auskunftei vor einer Datenübermittlung das berechtigte Interesse an der Kenntnis der Daten glaubhaft darlegen läßt. Außerdem verlangt das Gesetz eine Prüfung, ob Grund zu der Annahme besteht, der Betroffene habe ein schutzwürdiges Interesse am Ausschluß der Datenübermittlung. Der Gesetzgeber verpflichtet hier die Auskunfteien nicht nur dazu, sich das berechtigte Interesse an der Kenntnis der Daten — wenn auch nicht in allen Einzelheiten durch Urkunden belegt — darlegen zu lassen, sondern auch dazu, in jedem Fall zu prüfen, ob schutzwürdige Interessen des Betroffenen vorliegen können. Die vom Gesetzgeber verlangte Interessenabwägung im Einzelfall wird von den Auskunfteien — auch der Schufa — in aller Regel nicht praktiziert. Sie begreifen sich als Auskunftssysteme und verlassen sich im übrigen auf die Korrektheit und Glaubwürdigkeit ihrer Anfrager (Kunden). Dies ist jedoch nicht immer gewährleistet, wie der geschilderte Fall zeigt. Die Darlegung des berechtigten Interesses erfolgt in der Praxis so, daß auf dem Anfrageformular oder per Telefon, Telex, Telefax o. ä. typisierte Anfragegründe angegeben werden, die von den Auskunfteien gem. der Verpflichtung in § 29 Abs. 2 Satz 3 BDSG gespeichert bzw. aktenmäßig festgehalten werden. Weitere Darlegungen seitens des Anfragers werden im Regelfall zum Nachweis des berechtigten Interesses nicht verlangt.

Die obersten Datenschutzaufsichtsbehörden haben im Jahre 1979 kurz nach Inkrafttreten des BDSG eine **stichprobenweise Überprüfung** des dargelegten berechtigten Interesses durch die Auskunfteien als ausreichend akzeptiert. Maßgeblich dafür war damals der Hinweis der Auskunfteien auf die große Zahl ihrer Mitteilungen (Datenübermittlungen) und auf Praktikabilitätsprobleme bei den verschiedenen Anfrageformen (schriftlich, telefonisch, per Telex oder Telefax, automatisiert). Für die Schufa-Gesellschaften waren damals zehn Überprüfungen pro Geschäftsstelle und Monat verabredet. Dazu sollten dann noch die Überprüfungen kommen, die ggf. aufgrund von Anlaßkontrollen der Aufsichtsbehörden notwendig werden sollten.

Die Erfahrungen mit der stichprobenweisen Überprüfung des berechtigten Interesses durch die Auskunfteien — auch die Schufa — sind nicht positiv. Die Stichprobe ist angesichts der massenhaften Auskunftserteilungen (Datenübermittlungen viel zu klein, um Mißbräuche und unbefugte Mitteilungen aufzudecken. Außerdem ist das schematische und formularmäßig ablaufende Prüfverfahren ohne nähere Verifizierung der tatsächlichen Anfragegründe — sofern sie überhaupt erfolgt — nicht ausreichend, um das, was der Gesetzgeber erreichen will, zu erreichen. Die obersten Datenschutzaufsichtsbehörden diskutieren seit längerem mit den Auskunfteien über Veränderungen des Verfahrens (z. B. deutliche Anhebung der Zahl der Überprüfungen; zusätzliche Angaben und Unterlagen zum Anfragegrund). Diese Diskussion muß so bald wie möglich zum Abschluß kommen.

— Aufbewahrungsdauer der Aufzeichnungen zum Nachweis des berechtigten Interesses

Das BDSG sagt zur Aufbewahrungsdauer dieser Aufzeichnungen, die von den Auskunfteien gem. § 29 Abs. 2 Satz 3 BDSG oder bei automatisierten Abrufverfah-

ren beim Datenempfänger anzufertigen sind, nichts. Die obersten Datenschutzaufsichtsbehörden haben sich aus Praktikabilitätsgründen auf eine Aufbewahrungsfrist von einem Jahr verständigt. In der Kommentarliteratur zum BDSG wird die Auffassung vertreten, daß diese Frist länger sein müsse. Unter Hinweis auf die Möglichkeit späterer Datenschutzkontrollen, die Beweisregelung in § 8 BDSG und die in § 35 Abs. 2 Nr. 4 BDSG genannte 5-Jahresfrist wird eine längere, z. T. sogar eine 5-jährige Aufbewahrungsdauer gefordert. Ich vertrete die Auffassung, daß die Ein-Jahres-Frist allenfalls als Minimum anzusehen ist; eine längere Frist würde den Intentionen des Gesetzgebers eher entsprechen. Die Aufzeichnungen selbst bzw. die Protokolldaten müssen revisionsfest auswertbar und sicher aufbewahrt werden und dürfen gem. § 31 BDSG nur zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlage verwendet werden. Diese Verpflichtung trifft die Auskunfteien und bei automatisierten Abrufverfahren die Empfänger der Daten.

— Sorgfaltspflichten des Anfragers

Die Strafandrohung des § 43 Abs. 2 Nr. 1 BDSG und die vertraglichen Regelungen zwischen den Auskunfteien und ihren Kunden bedingen auch für die Anfrager besondere Sorgfaltspflichten. So müssen z. B. die Anschlußkunden der Schufa sicherstellen, daß nur befugte und auf das Datengeheimnis verpflichtete Mitarbeiter die Anfragecodes kennen und benutzen dürfen. Für andere Auskunfteien gilt dies analog für die verwendeten „Anfrageschecks". Die Codes selbst müssen regelmäßig verändert werden. Neben einem Kundencode muß auch ein individueller Mitarbeitercode vorhanden sein. Zwischen Anfrageinhalt und Anfragegrund muß ein Zusammenhang herstellbar sein, weil andernfalls die Berechtigung der Anfrage bzw. Datenübermittlung nicht belegbar ist. Auf die zweckgebundene Verwendung der erhaltenen Informationen ist hier nur zusätzlich hinzuweisen.

14.3 Aufbau eines Mietkatasters

Eine Vermieterorganisation beabsichtigt den Aufbau einer **Vergleichsmietendatei,** die u. a. die Angaben Straße, Hausnummer und Höhe der Miete des jeweiligen Mietobjekts enthalten soll. Aus diesem automatisiert geführten Mietkataster sollen Auskünfte an interessierte Vermieter und Mieter, Gerichte und Einrichtungen der öffentlichen Hand im Bereich der Wohnungswirtschaft erteilt werden.

Ich habe die Organisation darauf hingewiesen, daß Vermieter mit der Weitergabe solcher Informationen aus ihren Dateien an die das Mietkataster führende Einrichtung personenbezogene Daten der Mieter übermitteln, obwohl hierfür die Voraussetzungen des § 28 Bundesdatenschutzgesetz (BDSG) nicht vorliegen.

Insbesondere besteht ein Grund zu der Annahme, daß die betroffenen Mieter ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung an das Mietkataster haben. Für den Fall, daß ihre Wohnung als Vergleichsobjekt im Rahmen eines Mieterhöhungsverlangens benannt wird, sind sie nicht in der Lage, sich vor unverhältnismäßigen Belästigungen, weil andere Mieter oder Vermieter ihre Wohnung besichtigen möchten, zu schützen.

Diese Auffassung wird von den meisten Aufsichtsbehörden in den anderen Bundesländern geteilt. Zwar wird ein berechtigtes Interesse der Vermieter an der Übermittlung von Daten über Vergleichswohnungen anzunehmen sein, weil § 2 Abs. 2 Satz 4 des Gesetzes zur Regelung der Miethöhe (MHG) deren Benennung ausdrücklich als eine von mehreren Möglichkeiten zur Begründung von Mieterhöhungsverlangen zuläßt und es Vermietern erfahrungsgemäß gelegentlich Schwierigkeiten bereitet, geeignete Vergleichswohnungen namhaft zu machen.

Im Hinblick auf Mietwohnungen sind aber auch die Belange der Mieter zu berücksichtigen, für die die eigene Wohnung zum Kernbereich ihrer Privatsphäre gehört. Sie müssen fürchten, daß ihre Wohnungen aufgrund der durch die automatisierte Verarbeitung eröffneten schnellen und leichten Verfügbarkeit der Informationen deutlich häufiger als bisher zur Begründung von Mieterhöhungsverlangen herangezogen werden.

Damit besteht eine erhöhte Wahrscheinlichkeit, daß bei Mietern Nachforschungen über ihre Wohnungen angestellt werden. Außerdem enthält das Mietkataster Angaben, die Rückschlüsse auf Einkommenslage und sonstige Lebensumstände der Wohnungsinhaber ermöglichen.

Mehrere Aufsichtsbehörden kommen nach Abwägung der Interessen zum Ergebnis, daß die Übermittlung der Daten von Vergleichswohungen durch die Ver-

mieter nur zulässig ist, wenn die Betroffenen nicht widersprochen haben. Nach meiner Auffassung genügt die Widerspruchsmöglichkeit nicht; vielmehr bedarf es einer **Einwilligung des Mieters** nach § 4 Abs. 2 BDSG, in der Regel also schriftlich. Ich habe daher folgendes Verfahren vorgeschlagen:

Soweit die Einwilligung der Mieter nicht vorliegt, sind die Vermieter darauf hinzuweisen, daß insoweit die Angaben „Straße und Hausnummer" nicht gemeldet werden dürfen. Hierzu ist es erforderlich, den von der Vermieterorganisation verwendeten „Erhebungsbogen zur Ermittlung von Vergleichsmieten für frei finanzierte Wohnungen/Einfamilienhäuser im Stadtgebiet Bremen" entsprechend umzugestalten, damit die Vermieter bei Fehlen der Einwilligung lediglich die Angaben eintragen, die keinen Personenbezug ermöglichen.

Hat ein Vermieter anläßlich einer beabsichtigten Mieterhöhung Vergleichsdaten erhalten, die den Mieter nicht identifizieren, kann er sich an den Vermieter der angegebenen Wohnung wenden. Dieser kann dann nur mit i. d. R. schriftlicher Einwilligung des Betroffenen Straße und Hausnummer offenlegen. Eine Stellungnahme der Vermieterorganisation liegt noch nicht vor.

14.4 Arbeitnehmerdatenschutz

14.4.1 Fall: Führungszeugnisse im laufenden Arbeitsverhältnis

Mehrere Beschäftigte eines Unternehmens wandten sich dagegen, daß ihr Arbeitgeber sie ohne konkreten Anlaß aufgefordert hat, polizeiliche Führungszeugnisse vorzulegen.

Das Verlangen nach Beibringung eines polizeilichen Führungszeugnisses beinhaltet insbesondere die Frage nach Vorstrafen. Hierzu hat das Bundesarbeitsgericht in mehreren Urteilen entschieden, daß nur Fragen nach für das jeweilige Arbeitsverhältnis einschlägigen Vorstrafen wahrheitsgemäß beantwortet werden müssen. Je nach Art des zu besetzenden Arbeitsplatzes darf z. B. entweder nur nach Vorstrafen auf vermögensrechtlichem Gebiet (so etwa beim Bankkassierer) oder nach verkehrsrechtlichen Strafen (beim Kraftfahrer) gefragt werden. Das polizeiliche Führungszeugnis enthält sämtliche Straftaten, für die der Betroffene in den letzten fünf Jahren rechtskräftig verurteilt worden ist, geht also über den Rahmen des **Fragerechts des Arbeitgebers** in der Regel hinaus.

Ausnahmen im Einzelfall sind möglich, etwa wenn der betroffene Arbeitnehmer einen sicherheitsrelevanten Arbeitsplatz einnehmen soll, für den die bisherige völlige Straffreiheit wesentliche Voraussetzung ist. Außerhalb des Bewerbungsverfahrens, also im laufenden Arbeitsverhältnis, sind kaum einschlägige Fälle denkbar. In Betracht kommt z. B. die Situation, daß ein Arbeitnehmer innerhalb des Unternehmens auf eine der Sicherheitsüberprüfung unterliegende Funktion umgesetzt werden soll. Den anfragenden Mitarbeitern habe ich geraten, die Aufforderung des Arbeitgebers abzulehnen.

14.4.2 Unzulässige Rubriken im Bewerbungsfragebogen

Ein großes Bremer Unternehmen hat von Bewerbern Personalfragebogen ausfüllen lassen, die eine Vielzahl von unzulässigen Angaben enthalten. Dieser Fall ist exemplarisch für die vielfach anzutreffende, häufig aber auch nur auf Nachlässigkeit beruhende **„Datensammelwut" im Personalwesen der Privatwirtschaft.**

Nach § 28 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG) müssen Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden. Ihre Speicherung ist u. a. zulässig im Rahmen der Zweckbestimmung des Arbeitsverhältnisses. Unabhängig davon hat das Bundesarbeitsgericht in ständiger Rechtsprechung eine Beschränkung des **Fragerechts des Arbeitgebers** aus dem geschützten allgemeinen Persönlichkeitsrechts des Arbeitnehmers abgeleitet. Bei der Erhebung von Arbeitnehmerdaten sind die Grenzen dieses Fragerechts strikt einzuhalten. Hieraus folgt, daß nur solche Fragen gestellt werden dürfen, die mit dem Arbeitsplatz oder der zu leistenden Arbeit im Zusammenhang stehen (s. o. Ziffer 14.4.1).

Insbesondere der Geburtsname des Ehegatten hat mit der Zweckbestimmung des zu begründenden Arbeitsverhältnisses nichts zu tun und muß daher entfallen. Die Daten Religion, Kinder, Krankenkasse und erhaltener Urlaub sind erst dann erforderlich, wenn die Einstellung tatsächlich erfolgt. Die Angabe des Arbeitsamtes sowie der dort geführten Stammnummer ist im Bewerbungsverfahren ebenfalls nicht notwendig.

Fragen nach dem **Gesundheitszustand** bzw. nach bestehenden Krankheiten sind nur zulässig, soweit sie auf eine mögliche Beeinträchtigung der konkret zu verrichtenden Arbeit bezogen sind oder eine Gefährdung der zukünftigen Kollegen oder Kunden in Betracht kommt. Die entsprechende Rubrik im Fragebogen muß daher in diesem Sinne einschränkend formuliert werden.

Mit Urteil vom 08. November 1990 hat der Europäische Gerichtshof entschieden, daß ein Arbeitgeber unmittelbar gegen das Diskriminierungsverbot verstößt, wenn er eine von ihm für geeignet befundene Bewerberin wegen deren Schwangerschaft ablehnt. Inzwischen hat sich das Bundesarbeitsgericht dieser Auffassung mit Urteil vom 15. 12. 1992 (Az.: 2 AZR 227/92) angeschlossen. Daraus ergibt sich, daß die Frage nach einer **Schwangerschaft** grundsätzlich unzulässig ist.

Die Verwendung der **Rentenversicherungsnummer** unterliegt nach § 18 f Sozialgesetzbuch IV (SGB IV) der strikten Zweckbindung. Der Arbeitgeber darf sie nur erheben, speichern oder verwenden, soweit dies für die Erfüllung einer gesetzlichen Aufgabe der in dieser Rechtsvorschrift genannten Stellen erforderlich ist. Dies ist aber erst nach Eingehen des Arbeitsverhältnisses der Fall. Im Bewerbungsfragebogen ist dieses Datum daher zu streichen.

Die Frage nach erfolgten Pfändungen kann nur dann — bezogen auf den zu besetzenden Arbeitsplatz — von Bedeutung sein, wenn Bewerber besondere Vertrauensstellungen einnehmen sollen (z. B. Buchhaltung oder Kasse).

Auch die Frage nach Verwandten im Betrieb oder in der gleichen Branche läßt keinen Bezug zu einem konkreten Arbeitsplatz erkennen.

Ich habe das Unternehmen gebeten, den Personalfragebogen entsprechend zu ändern. Es hat dies zugesagt und wird mir nach Abstimmung mit dem Betriebsrat den überarbeiteten Vordruck zuleiten.

14.4.3 Noch immer kein Arbeitnehmerdatenschutzgesetz

Bereits seit 1984 bemängeln die Datenschutzbeauftragten des Bundes und der Länder das Fehlen eines bereichsspezifischen Arbeitnehmerdatenschutzes. Zwar hat der Bundestag bereits 1985 die Notwendigkeit gesetzlicher Regelungen unterstrichen, allerdings ist bis heute nichts passiert. Lediglich für den Beamtenbereich gibt es neue Sonderregelungen im Beamtenrechtsrahmengesetz (BRRG) (s. a. Ziffer 4.3 dieses Berichts). Aufgrund dieser Untätigkeit haben die Datenschutzbeauftragten des Bundes und der Länder am 23./24. März 1992 eine Entschließung zum Arbeitnehmerdatenschutz verabschiedet (s. u. Ziffer 16.1). Ich habe diese Entschließung dem Senator für Arbeit und Frauen mit der Bitte zugeleitet, sich auf Bundesebene für spezielle gesetzliche Regelungen in diesem Bereich einzusetzen.

Der Senator für Arbeit und Frauen unterstützt die Entschließung von der Sache her. Allerdings erscheint es ihm zur Zeit nicht zweckmäßig, selbst entsprechende Initiativen im Bundesrat zu ergreifen. Art. 30 Abs. 1 Nr. 1 des Einigungsvertrages verpflichte den gesamtdeutschen Gesetzgeber ohnehin, das Arbeitsvertragsrecht möglichst bald einheitlich neu zu kodifizieren. Hierzu sei bereits ein Diskussionsentwurf vorgelegt worden, der auch Vorschriften über den Arbeitnehmerdatenschutz enthalte.

Am 26. Juni 1992 hat die Bundesregierung auf eine Kleine Anfrage der SPD geantwortet, sie teile die Auffassung der Datenschutzbeauftragten und halte es für geboten, daß der Schutz von Arbeitnehmerdaten bereichsspezifisch geregelt wird. Sie werde den Beschluß des Ausschusses für Arbeit und Sozialordnung des Deutschen Bundestages vom 13. November 1991 berücksichtigen, nach dem ein Gesetzentwurf noch in dieser Legislaturperiode vorgelegt werden soll.

Außerdem hat der Bundesrat am 25. September 1992 die Schaffung eines Arbeitsschutzgesetzbuches in der Bundesrepublik Deutschland gefordert. In dieser Entschließung werden Rechtsgrundlagen für eine den Prinzipien des Datenschutzes verpflichtete epidemiologische Forschung über arbeitsbedingte Gesundheitsrisiken gefordert. Außerdem müsse den Behörden und der Wissenschaft die Möglichkeit der Datendokumentation und -auswertung eingeräumt werden.

Schließlich hat der Innenausschuß des Deutschen Bundestages am 21. Dezember 1992 die Bundesregierung noch einmal aufgefordert, einen Gesetzentwurf zum Arbeitnehmerdatenschutz so rechtzeitig vorzulegen, daß er noch in dieser Legislaturperiode verabschiedet werden könne. In diesem Zusammenhang hat die

Bundesregierung erklärt, der Bundesminister für Arbeit und Sozialordnung habe die dazu erforderlichen umfangreichen Vorarbeiten (!) aufgenommen.

Eine weitere Verzögerung ist nicht mehr vertretbar.

15. Register der nach dem Bundesdatenschutzgesetz meldepflichtigen Stellen

In dem bei mir geführten Register der meldepflichtigen Stellen, sind derzeit gem. § 32 Bundesdatenschutzgesetz (BDSG) insgesamt 87 Unternehmen registriert, von denen 72 aus der Stadt Bremen und 15 aus Bremerhaven stammen. Unterteilt nach Art der meldepflichtigen Tätigkeit und regionaler Ansiedlung im Lande Bremen ergibt sich folgendes Bild:

Art der Tätigkeit	insgesamt	Bremen	Bremerhaven
Speicherung personenbezogener Daten zum Zwecke der Übermittlung	8	5	3
Speicherung personenbezogener Daten zum Zwecke der anonymisierten Übermittlung	—	—	—
Verarbeitung oder Nutzung personenbezogener Daten im Auftrag als Dienstleistungsunternehmen	79	67	12

Zu den insgesamt acht Unternehmen, die Daten zum Zwecke der Übermittlung speichern, gehören fünf Kredit- und Handelsauskunfteien und drei Adreßhandelsunternehmen. Unter den 79 Unternehmen, die Daten im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen, befinden sich drei Datenlöschungs- und -vernichtungsbetriebe. Die anderen Firmen betreiben in der Mehrzahl automatisierte Datenverarbeitung für Dritte (z. B. Service-Rechenzentren).

Die Umstellungs- und Aktualisierungsarbeiten, die 1991 nicht beendet werden konnten, wurden im Berichtsjahr abgeschlossen. In mehreren Fällen wurden Verwarnungen wegen des Verstoßes gegen die Meldepflicht ausgsprochen, in einem Fall aus dem gleichen Grund ein Bußgeldverfahren eingeleitet. Darüber hinaus habe ich eine Vielzahl von Unternehmen, die bislang nicht zum Register gemeldet waren, angeschrieben und um Prüfung der Meldepflicht und ggf. Anmeldung gebeten.

16. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

16.1 Entschließung zum Arbeitnehmerdatenschutz vom 23./24. März 1992

I.

Im Rahmen des Arbeitsverhältnisses werden personenbezogene Daten aus ganz unterschiedlichen Lebensbereichen des Arbeitnehmers erhoben und gespeichert. Diese Daten verwendet der Arbeitgeber nicht nur für eigene Zwecke. Aus dem Arbeitsverhältnis ergeben sich auch Auskunfts-, Bescheinigungs- und Meldepflichten, die der Arbeitgeber gegenüber öffentlichen Stellen zu erfüllen hat. Durch die Möglichkeit, im Arbeitsverhältnis anfallende personenbezogene Daten miteinander zu verknüpfen und sie — losgelöst vom Erhebungszweck — für andere Verwendungen zu nutzen, entstehen Gefahren für das Persönlichkeitsrecht des Arbeitnehmers. Mit der Intensität der Datenverarbeitung, insbesondere durch Personalinformationssysteme und digitale Telekommunikationsanlagen, nehmen die Kontroll- und Überwachungsmöglichkeiten des Arbeitgebers zu.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb bereits seit 1984 bereichsspezifische und präzise gesetzliche Bestimmungen zum Arbeitnehmerdatenschutz. Bundestag, Bundesrat und Bundesregierung haben ebenfalls eine Regelungsnotwendigkeit bejaht; gleichwohl stehen bundesgesetzliche Regelungen über den allgemeinen Arbeitnehmerdatenschutz immer noch aus.

Die Notwendigkeit zur gesetzlichen Regelung besteht unabhängig davon, ob Arbeitnehmerdaten in automatisierten Dateien, in Akten oder in sonstigen Unterlagen verarbeitet werden. Der erhöhten Gefährdung durch die automatisierte Datenverarbeitung ist durch spezifische Schutzvorschriften Rechnung zu tragen.

Angesichts der besonderen Abhängigkeit des Arbeitnehmers im Arbeitsverhältnis und während der Phase einer Bewerbung um einen Arbeitsplatz ist durch Gesetz zu untersagen, daß Rechte, die dem Arbeitnehmer nach einschlägigen Datenschutzvorschriften zustehen, durch Rechtsgeschäft, Tarifvertrag und Dienst- oder Betriebsvereinbarung ausgeschlossen werden. Außerdem ist durch Gesetz festzulegen, daß eine Einwilligung des Arbeitnehmers oder Bewerbers nur dann als Grundlage einer Datenerhebung, -verarbeitung oder -nutzung in Frage kommt, wenn die Freiwilligkeit der Einwilligung sichergestellt ist, also die Einwilligung ohne Furcht vor Nachteilen verweigert werden kann. Deshalb dürfen allein aufgrund einer Einwilligung z. B. keine Gesundheitszeugnisse, Ergebnisse von Genomanalysen u. ä. angefordert werden, wenn sie den Rahmen des Fragerechts des Arbeitgebers überschreiten.

II.

Die gesetzliche Ausgestaltung des Arbeitnehmerdatenschutzes muß insbesondere folgende Grundsätze beachten:

1. Die Datenerhebung muß grundsätzlich beim Arbeitnehmer erfolgen.
2. Der Arbeitgeber darf Daten des Arbeitnehmers — auch durch Befragen des Arbeitnehmers oder Bewerbers — nur erheben, verarbeiten oder nutzen, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses erforderlich oder sonst gesetzlich vorgesehen ist. Dabei ist der Grundsatz der Zweckbindung zu beachten. Auch ist zwischen der Bewerbungs- und Einstellungsphase zu unterscheiden.
3. Der Arbeitgeber darf Daten, die er aufgrund gesetzlicher Vorgaben für andere Stellen (z. B. Sozialversicherungsträger) erheben muß, nur für diesen Zweck verwenden.
4. Eine Datenauswertung und -verknüpfung, die zur Herstellung eines umfassenden Persönlichkeitsprofils des Arbeitnehmers führen kann, ist unzulässig.
5. Beurteilungen und Personalauswahlentscheidungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.
6. Notwendige Datenübermittlungen zwischen Arzt und Arbeitgeber sind eindeutig zu regeln. Dem Arbeitgeber darf grundsätzlich nur das Ergebnis der ärztlichen Untersuchung zugänglich gemacht werden. Darüber hinaus dürfen ihm — soweit erforderlich — nur tätigkeitsbezogene Risikofaktoren mitgeteilt werden. Medizinische und psychologische Befunde sind getrennt von den üblichen Personalunterlagen aufzubewahren. Die Ergebnisse medizinischer oder psychologischer Untersuchungen und Tests des Beschäftigten dürfen automatisiert nur verarbeitet werden, wenn dies dem Schutz des Beschäftigten dient.
7. Dem Arbeitnehmer sind umfassende Auskunfts- und Einsichtsrechte in die Unterlagen einzuräumen, die sein Arbeitsverhältnis betreffen. Diese Rechte müssen sich auch auf Herkunft, Verarbeitungszwecke und Empfänger der Daten sowie die Art und Weise ihrer Auswertung erstrecken.
8. Dem Personal-/Betriebsrat muß ein Mitbestimmungsrecht bei der Einführung, Anwendung und der wesentlichen Änderung von automatisierten Dateien mit personenbezogenen Daten der Arbeitnehmer für Zwecke der Personalverwaltung zustehen. Das gilt auch bei sonstigen technischen Einrichtungen, mit denen das Verhalten und die Leistung der Beschäftigten überwacht werden kann.
9. Gesetzlich festzulegen ist, welche Daten der Arbeitnehmervertretung für ihre Aufgabenerfüllung zugänglich sein müssen und wie der Datenschutz bei der Verarbeitung von Arbeitnehmerdaten im Bereich der Arbeitnehmervertretung gewährleistet wird. Regelungsbedürftig ist auch das Verhältnis zwischen dem Personal-/Betriebsrat und dem behördlichen/betrieblichen Datenschutzbeauftragten.
10. Die Befugnis des Personal-/Betriebsrats, sich unmittelbar an die Datenschutzkontrollinstanzen zu wenden, ist gesetzlich klarzustellen.
11. Arbeitnehmerdaten dürfen nur dann ins Ausland übermittelt werden, wenn dort ein dem deutschen Recht vergleichbarer Datenschutzstandard gewährleistet ist oder wenn der Betroffene nach den oben genannten Grundsätzen (vgl. Abschn. I Abs. 4) eingewilligt hat.

16.2 Entschließung zur Neuregelung des Asylverfahrens vom 28. April 1992

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält Änderungen des Gesetzentwurfs zur Neuregelung des Asylverfahrens für erforderlich, insbesondere der geplanten Regelungen

1. über die erkennungsdienstliche Behandlung von Asylbewerbern zur Sicherung der Identität (§ 16 Abs. 1) und
2. über die Nutzung der dabei gewonnenen erkennungsdienstlichen Unterlagen zur Strafverfolgung und zur Gefahrenabwehr (§ 16 Abs. 5).

Zu 1:

Nach dem geltenden Recht sind Lichtbilder und Fingerabdrucke bei Asylbewerbern nur dann zu fertigen, wenn deren Identität nicht eindeutig bekannt ist. Demgegenüber sieht der Gesetzentwurf zur Neuregelung des Asylverfahrens vor, daß von sämtlichen Asylbewerbern — bis auf wenige Ausnahmen — Lichtbilder und Fingerabdrucke zu fertigen sind. Dies ist mit dem Verfassungsgrundsatz der Verhältnismäßigkeit nicht vereinbar:

Der Staat hat selbstverständlich das Recht zu wissen, mit wem er es zu tun hat. Jeder — gleichgültig ob Deutscher oder Ausländer — muß sich deshalb durch Dokumente ausweisen können; nur wenn Zweifel an der Identität bestehen, kommen erkennungsdienstliche Maßnahmen in Betracht. Dieser Grundsatz unserer Rechtsordnung muß auch im Rahmen der Neuregelung des Asylverfahrens beachtet werden. Nur wenn feststeht, daß die Identität eines hohen Anteils der Asylbewerber — also nicht bloß diejenige einzelner oder bestimmter Gruppen — zweifelhaft ist, wäre eine erkennungsdienstliche Behandlung aller Asylbewerber gerechtfertigt. Gerade dies aber ist bisher nicht hinreichend belegt: In der amtlichen Begründung des Gesetzentwurfs ist allein davon die Rede, daß nach Feststellung niederländischer Behörden 20 % der Asylbewerber unter falschem Namen einen weiteren Asylantrag stellen. Aussagekräftige Angaben, in welchem Umfang in der Bundesrepublik Deutschland Asylbewerber unter Täuschung über ihre Identität gleich bei der ersten Antragstellung oder nach dessen Ablehnung erneut versuchen, Asyl zu erhalten, fehlen bislang.

Zu 2:

Bei der zentralen Auswertung der Fingerabdrücke von Asylbewerbern durch das Bundeskriminalamt muß — ungeachtet dessen, ob das Bundeskriminalamt dabei in eigener Zuständigkeit oder für das Bundesamt für die Anerkennung ausländischer Flüchtlinge tätig wird — unbedingt folgendes sichergestellt sein:

— Fingerabdrücke von Asylbewerbern, die unter Beachtung des zu Nr. 1 Gesagten gefertigt wurden, dürfen nur gespeichert werden, soweit dies zur Sicherung der Identität unbedingt erforderlich ist. Dazu reicht die bisher vom Bundeskriminalamt angewandte Methode der sog. Kurzsatzverformelung der Fingerabdrucke aus. Gerade aber dabei soll es nicht bleiben:

  Mit der bevorstehenden Einführung von AFIS — einem neuen automatisierten Fingerabdruckverfahren — sollen künftig auch die Fingerabdrucke von Asylbewerbern, die allein zur Feststellung deren Identität gefertigt wurden, genauso erfaßt und ausgewertet werden wie die Fingerabdrucke mutmaßlicher oder tatsächlicher Straftäter. Asylbewerber würden damit von vornherein wie Straftäter behandelt. Eine solche Verfahrensweise wird dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot nicht gerecht. Zudem unterläuft sie die in § 16 Abs. 4 des Gesetzentwurfs vorgesehene Trennung der erkennungsdienstlichen Unterlagen von Asylbewerbern und Straftätern. Um die gebotene Differenzierung sicherzustellen, sollte — über das Trennungsgebot des § 16 Abs. 4 hinaus — die Verformelung auf den Abdruck eines Fingers des Asylbewerbers beschränkt werden, da dies zur eindeutigen Feststellung seiner Identität genügt.

— Die Datenschutzbeauftragten verkennen nicht, daß es unter Umständen im überwiegenden Allgemeininteresse notwendig sein kann, im Rahmen asylrechtlicher Identitätsfeststellung gefertigte Fingerabdrucke für Zwecke der Strafverfolgung zu nutzen. Weil eine solche Verwendung einen neuen und zudem erheblichen Eingriff in das Grundrecht auf Datenschutz darstellt, darf sie nicht — wie es der Gesetzentwurf aber vorsieht — praktisch voraussetzungslos erfolgen. Notwendig ist vielmehr, die Voraussetzungen in einem

abschließenden Straftatenkatalog aufzuführen; darin könnten auch die in der amtlichen Begründung des Gesetzentwurfs erwähnten Fälle des Sozialhilfebetrugs enthalten sein.

- Ein entsprechender Maßstab ist an die Regelung anzulegen, wann zur Identitätssicherung gefertigte Fingerabdrucke von Asylbewerbern zur polizeilichen Gefahrenabwehr genutzt werden dürfen. Eine solche Nutzung sollte nur zugelassen werden, soweit dies zur Abwehr einer gegenwärtigen erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist.

16.3 Entschließung zum Grundrecht auf Datenschutz vom 28. April 1992

1. Seit dem Volkszählungsurteil des Bundesverfassungsgerichts im Jahre 1983 ist allgemein anerkannt, daß die Grundrechte auch die Befugnis des einzelnen umfassen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden. Die Datenschutzbeauftragten treten dafür ein, dieses Recht ausdrücklich im Grundgesetz zu verankern. Damit würde

- für die Bürger deutlicher erkennbar, daß unsere Verfassung ihr Recht auf Datenschutz in gleicher Weise garantiert wie die traditionellen Grundrechte,
- der wachsenden Bedeutung des Datenschutzes für das Funktionieren der freiheitlichen Demokratie Rechnung getragen und auf die negativen Erfahrungen der DDR-Geschichte reagiert,
- der Grundrechtskatalog dem technologischen Wandel angepaßt und
- die Konsequenz aus den positiven Erfahrungen gezogen, die in mehreren Ländern des Bundes und im Ausland mit ähnlichen Verfassungsbestimmungen gemacht wurden.

Die Konferenz begrüßt deshalb die Vorstellungen, die in der Verfassungskommission des Bundesrates entwickelt worden sind.

Die Datenschutzbeauftragten empfehlen der Gemeinsamen Verfassungskommission des Bundestages und Bundesrates im Zusammenhang mit Art. 1 und Art. 2 GG den nachfolgenden Text zur Beratung:

> „Jeder hat das Recht, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen. Dazu gehört das Recht auf Auskunft und Einsicht in amtliche Unterlagen. Dieses Recht darf nur durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden, soweit überwiegende Interessen der Allgemeinheit es erfordern."

2. Darüber hinaus empfiehlt die Konferenz, die unabhängige Datenschutzkontrolle, die für die Verwirklichung des Grundrechts auf Datenschutz im Alltag von entscheidender Bedeutung ist, in der Verfassung zu verankern.

3. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es zusätzlich für erforderlich, in die Verfassungsdiskussion folgende Punkte miteinzubeziehen, die sich aus der Entwicklung der Informationstechnik ergeben:

- Stärkung der Grundrechte aus Art. 10 und 13 im Hinblick auf neue Überwachungstechniken
- Recht auf Zugang zu den Daten der Verwaltung (Aktenöffentlichkeit, Informationsfreiheit)
- Instrumente zur Technikfolgenabschätzung.

16.4 Entschließung zum „Lauschangriff" vom 1./2. Oktober 1992

Die Datenschutzbeauftragten des Bundes und der Länder erklären (bei Gegenstimme des LfD Bayern):

Nachdem erst vor kurzem mit dem Gesetz zur Bekämpfung der organisierten Kriminalität die Befugnisse der Strafverfolgungsbehörden erheblich erweitert worden sind und obwohl über den Erfolg dieser Maßnahmen noch keine Erfahrungen gesammelt werden konnten, wird gegenwärtig parteiübergreifend vielfach die Forderung erhoben, der Polizei in bestimmten Fällen das heimliche Abhören und Herstellen von Bild- und Tonaufzeichnungen in und aus Wohnungen (sog. „Lauschangriff") zu ermöglichen.

1. Das Grundgesetz gewährt jedem einen unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen ist. Dem einzelnen muß um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein „Innenraum" verbleiben, in dem er „sich selbst besitzt" und „in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt" (BVerfGE 27,1 ff.). Jedem muß ein privates Refugium, ein persönlicher Bereich bleiben, der obrigkeitlicher Ausforschung — insbesondere heimlicher — entzogen ist. Dies gilt gegenüber Maßnahmen der Strafverfolgung vor allem deshalb, weil davon auch unverdächtige oder unschuldige Bürger betroffen sind. Auch strafprozessuale Maßnahmen dürfen nicht den Wesensgehalt eines Grundrechts, insbesondere das Menschenbild des Grundgesetzes verletzen.

2. Die Datenschutzbeauftragten nehmen die Gefahren, die das organisierte Verbrechen für die Opfer und auch für die Demokratie und den Rechtsstaat heraufbeschwört, sehr ernst. Sie sind allerdings der Meinung, daß eine angemessene Abwägung zwischen der Verfolgung der organisierten Kriminalität und dem Schutz der Persönlichkeitsrechte der Bürger geboten und möglich ist und es eine Wahrheitserforschung um jeden Preis auch künftig im Strafprozeßrecht nicht geben darf. Daraus folgt, daß der Lauschangriff auf Privatwohnungen für Zwecke der Strafverfolgung auch in Zukunft nicht erlaubt werden darf.

3. Eine andere Frage ist, ob und unter welchen Voraussetzungen der Gesetzgeber für Räume, die allgemein zugänglich sind oder beruflichen oder geschäftlichen Tätigkeiten dienen (z. B. Hinterzimmer von Gaststätten, Spielcasinos, Saunaclubs, Bordelle), einen Lauschangriff zulassen kann. Hierfür sind Mindestvoraussetzungen ein eng begrenzter abschließender Straftatenkatalog, die Verwendung der gewonnenen Erkenntnisse ausschließlich zur Verfolgung dieser Straftaten, ein strikter Richtervorbehalt sowie die Wahrung besonderer Amts- und Berufsgeheimnisse.

16.5 Entschließung zum Gesundheitsstrukturgesetz 1993 vom 1./2. Oktober 1992

Die Bundesregierung will mit dem Gesundheits-Strukturgesetz dem Kostenanstieg in der gesetzlichen Krankenversicherung entgegenwirken. Dieses begrüßenswerte Ziel soll nach dem vorgelegten Gesetzentwurf u. a. auch durch eine verstärkte automatisierte Datenverarbeitung erreicht werden. Die damit verbundenen Eingriffe in die Persönlichkeitsrechte der Versicherten und in die sie schützende ärztliche Schweigepflicht müssen auf das unbedingt Notwendige beschränkt werden. Die Datenschutzkonferenz hält vor allem folgende Verbesserungen des Gesetzentwurfs für notwendig:

— Der Gesetzentwurf sieht vor, daß die Krankenhäuser den Krankenkassen mehr Versichertendaten zur Verfügung stellen müssen als bisher. Es sollte deshalb eingehend geprüft werden, ob die Krankenkassen tatsächlich alle geforderten Angaben benötigen; die Aufgabenteilung zwischen Krankenkassen und Medizinischem Dienst muß aufrechterhalten bleiben.

— Für das Modellvorhaben zur Überprüfung des Krankenhausaufenthalts müssen die Erhebung, Verwendung und Löschung von Versichertendaten durch den Medizinischen Dienst präziser als bisher vorgesehen geregelt werden.

— Beim Einzug der Vergütung der Krankenhausärzte für Wahlleistungen durch Krankenhäuser sollte die Einschaltung privater Abrechnungsstellen ohne Einwilligung der Patienten nicht zugelassen werden, da dabei Abrechnungsdaten an Dritte offenbart werden. Die Daten sind gegen unbefugte Offenbarung und Beschlagnahme rechtlich besser geschützt, wenn sie — auch zur Abrechnung — im Krankenhaus verbleiben. Die Krankenhäuser sind zudem selbst in der Lage, die Vergütung einzuziehen.

— Für die neu vorgesehenen Patienten-Erhebungsbogen zur Ermittlung des Bedarfs an Pflegepersonal im Krankenhaus sollte eine strikte Zweckbindung sowie eine frühestmögliche Löschungs- oder Anonymisierungspflicht festgelegt werden. Eine Überlassung der Patienten-Erhebungsbogen in der im Gesetzentwurf vorgesehenen Fassung an die Krankenkassen ist abzulehnen.

16.6 Entschließung zum Datenschutz bei internen Telekommunikationsanlagen vom 1./2. Oktober 1992

Der zunehmende Einsatz von digitalen Telekommunikationsanlagen (TK-Anlagen) in Wirtschaft und Verwaltung birgt Datenschutzrisiken in sich, denen durch

eine datenschutzfreundliche Ausgestaltung der Technik und durch geeignete bereichsspezifische Regelungen entgegengewirkt werden muß. Telefongespräche stehen — auch wenn sie von einem Dienstapparat aus geführt werden — unter dem Schutz des Grundgesetzes. Dies hat das Bundesverfassungsgericht in seiner neueren Rechtsprechung hervorgehoben.

Der Schutz des Fernmeldegeheimnisses und des nichtöffentlich gesprochenen Wortes ist gerade bei Arbeitnehmern bedeutsam, da diese sich in einem besonderen Abhängigkeitsverhältnis befinden; aber auch das informationelle Selbstbestimmungsrecht Dritter, die anrufen oder angerufen werden, muß gewahrt werden.

Entsprechende bundesrechtliche Regelungen für interne TK-Anlagen sind überfällig, da in diesen Anlagen — insbesondere wenn sie digital an das öffentliche ISDN angeschlossen sind — umfangreiche Sammlungen sensibler personenbezogener Daten entstehen können, die sich auch zur Verhaltens- und Leistungskontrolle eignen und zudem Hinweise auf das Kommunikationsverhalten aller Gesprächsteilnehmer geben.

Die Regelungen sollten verbindliche Vorgaben für die technische Ausgestaltung von TK-Anlagen geben und den Umfang der zulässigen Datenverarbeitung festlegen:

- Es müssen die technischen Voraussetzungen gewährleistet sein, daß Anrufer und Angerufene die Rufnummernanzeige fallweise abschalten können.
- Die automatisische Speicherung der Rufnummern von externen Anrufern nach Beendigung des Telefongesprächs ist auszuschließen, es sei denn, eine sachliche Notwendigkeit besteht hierfür (z. B. bei Feuerwehr und Rettungsdiensten).
- Die Weiterleitung eines Anrufs an einen anderen als den gewählten Anschluß sollte dem Anrufer so rechtzeitig signalisiert werden, daß dieser den Verbindungsaufbau abbrechen kann.
- Das Mithören und Mitsprechen weiterer Personen bei bestehenden Verbindungen sollte nur nach eindeutiger und rechtzeitiger Ankündigung möglich sein.
- Verbindungsdaten einschließlich der angerufenen Telefonnummern sollten nach Beendigung der Gespräche nur insoweit gespeichert werden, als dies für Abrechnungszwecke und zulässige Kontrollzwecke erforderlich ist. Die Nummern der Gesprächspartner von Arbeitnehmervertretungen, internen Beratungseinrichtungen und sonstigen auf Vertraulichkeit angewiesenen Stellen dürfen nicht registriert werden.
- Die TK-Anlagen müssen durch geeignete techische Maßnahmen gegen unberechtigte Veränderungen der Systemkonfiguration und unberechtigte Zugriffe auf Verbindungs- und Inhaltsdaten geschützt werden.

Da TK-Anlagen geeignet sind, das Verhalten und die Leistung der Arbeitnehmer zu kontrollieren, und sie überdies häufig die Arbeitsplatzgestaltung beeinflussen, löst ihre Einführung in Betrieben und Behörden Mitbestimmungsrechte der Betriebsräte und überwiegend auch der Personalräte aus. Sie dürfen daher nur betrieben werden, wenn unter Beteiligung der Arbeitnehmervertretungen verbindlich festgelegt wurde, welche Leistungsmerkmale aktiviert und unter welchen Bedingungen sie genutzt werden, welche Daten gespeichert, wie und vom wem sie ausgewertet werden. Die Nutzer der TK-Anlage sind über den Umfang der Datenverarbeitung umfassend zu unterrichten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, daß umgehend datenschutzrechtliche Regelungen für den Einsatz und die Nutzung von internen TK-Anlagen mit einer bereichsspezifischen Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten geschaffen werden.

Druck: Anker-Druck Bremen