BREMISCHE BÜRGERSCHAFT
Landtag
12. Wahlperiode

Drucksache 12/163

Zehnter Jahresbericht des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag), dem Präsidenten des Senats den 10. Bericht über das Ergebnis meiner Tätigkeit im Jahre 1987 zum 31. März 1988 (§ 33 Abs. 1 Bremischen Datenschutzgesetz).

Dr. Alfred Büllesbach, Landesbeauftragter für den Datenschutz

Inhaltsübersicht

FFD 121 163

FFD 12/163

FFD 121/163

FFD 12/163

1. Vorbemerkungen

1.1 10 Jahre Datenschutz in Bremen

Am 1. Januar 1978 trat das Bremische Datenschutzgesetz in Kraft. Ich lege nunmehr den 10. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Bremen vor. Die ersten fünf Jahresberichte wurden von Herrn Schepp, meinem Amtsvorgänger, vorgelegt. Für die Jahresberichte 6. bis 10. trage ich die Verantwortung. Ingesamt zehn Jahre Datenschutz in einer landes- und bundespolitisch interessanten Phase, in der es darum ging, in der Öffentlichkeit, bei der Verwaltung, in der Wirtschaft, in der Gesetzgebung und nicht zuletzt auch in der Justiz den Datenschutzgedan-

ken zu verankern. Wer die letzten zehn Jahre Datenschutzgeschichte mitverfolgt hat, wird sich erinnern, daß dies gelegentlich nicht ohne scharfe Auseinandersetzungen geschah. Die Diskussion um die Durchsetzung des Datenschutzes bei der Polizei und bei den anderen Sicherheitsbehörden war nie sehr leicht. Der Durchbruch des Datenschutzprinzipes gelang nicht zuletzt dadurch, daß das Bundesverfassungsgericht mit seinem Volkszählungsurteil 1983 das Recht auf informationelle Selbstbestimmung prägte, nach dem jedermann das Recht hat, selbst zu bestimmen, wer was wann und bei welcher Gelegenheit über ihn weiß. In dieses Recht darf nur durch den Gesetzgeber und nur unter bestimmten Voraussetzungen eingegriffen werden. Dieses Urteil war sowohl wegweisend für die weitere Entwicklung des Rechtes als auch eine Antwort auf die Entwicklung zur sogenannten Informationsgesellschaft, wie sie gegenwärtig diskutiert wird. Zwischenzeitlich ist das Recht auf informationelle Selbstbestimmung auf viele Bereiche ausgedehnt worden, so z. B. in der Diskussion um Arbeitnehmerdatenschutz, um Datenschutz im Gesundheitswesen, Datenschutz im Bereich der Polizei und der Strafverfolgungsbehörden, der Verfassungsschutzämter, der Statistikämter etc. Mehr und mehr wird den Handelnden bewußt, daß Datenschutz vom Bürger verlangt wird und Mißachtungen der Grundsätze des Datenschutzes nicht mehr als Kavaliersdelikte hingenommen werden. Datenschutz ist inzwischen auch unter dem Aspekt der Sozialverträglichkeit im engeren Sinne der Datenschutzverträglichkeit bei der Gestaltung von Bürokommunikationssystemen, ja insgesamt bei der Anwendung von Informations- und Kommunikationstechnik thematisiert.

Je breiter moderne Informations- und Kommuniktionstechniken eingesetzt werden und je intensiver die Erfahrungen im Umgang mit diesen Rechnern werden, desto deutlicher ist die datenschutzrechtliche Sensibilisierung. Menschen, die früher mit dem Datenschutzthema nichts verbinden konnten, erkennen plötzlich, nachdem sie selbst sich mit Personal- oder Home-Computern befaßten, welche Möglichkeiten der Zugriffe, der Auswertungen, der variablen Verknüpfung mit personenbezogenen Daten entstehen können und wie durch solche Manipulationen elementar in grundrechtlich geschützte Positionen eines Menschen eingegriffen werden kann. Es steht — und dies machte ich in den letzten Jahresberichten mehrfach deutlich — die Autonomie des einzelnen Menschen und dessen Freiheit, sich autonom entscheiden zu können, zur Diskussion. Das Risiko ist, daß diese Veränderungen schleichend stattfinden, und nicht wie im Umweltschutz durch absterbende Bäume, tote Vögel oder sterbende Fische drastisch wahrnehmbar sind. Der Verlust an Autonomie und Freiheit, den es zu verhindern gilt, wird meist erst wahrgenommen, wenn er bereits eine gewisse Intensität eingenommen hat. Um diese schleichende Tendenz zur Überwachung menschlicher Arbeits- und Geschehensabläufe entgegenzuwirken, ist der Datenschutz angetreten. Er sichert somit elementare Grundrechtspositionen eines jeden Bürgers in einem demokratischen Staat. Gemeinwesen — und dies hat das Bundesverfassungsgericht klargestellt — ist angewiesen auf die bewußte Wahrnehmung von Rechten durch ihre Bürger, die dies in der Teilnahme an Diskussionsprozessen, Versammlungen etc. dokumentieren. Die allzeitige Erfassung und Speicherung der verschiedensten Bürgeraktivitäten und Arbeitsabläufe registriert nicht nur die Bürger, sondern beraubt sie auch ihrer unmittelbaren Freiheit. Für die gesellschaftliche Entwicklung ist bereits das Gefühl der umfangreichen Speicherung und der damit vermeintlich verbundenen Freiheitsbedrohung höchst gefährlich.

Die Bedeutung, die der Datenschutz deshalb für die gesellschaftliche Entwicklung im Rahmen der Entwicklung zur Informationsgesellschaft hat, liegt nicht mehr und nicht weniger in der Sicherung menschlicher Autonomie und Freiheit und — wie das Bundesverfassungsgericht es hergeleitet hat — in dem Schutz der freien Persönlichkeitsentfaltung und der Menschenwürde.

Die fortschreitende Technisierung von immer mehr sozialen Vorgängen und damit deren Einbettung in technisch-strukturierte Organisationssysteme verbunden mit umfangreichen Vernetzungsstrukturen erzeugt beim Bürger mehr und mehr auch das Gefühl einer Überorganisation. Wenn sich dieser vorläufig noch anfängliche Eindruck einer Überorganisation verdichtet und zu dem Gefühl einer Überinstitutionalisierung von menschlichen Verhaltensweisen führt, ist nicht nur das Recht auf informationelle Selbstbestimmung tangiert, sondern die Frage der Beteiligungsrechte und der Wahrnehmung von Freiheitsrechten der Bürger in einer demokratischen Gesellschaft schlechthin. Es darf in einer demokratischen Gesellschaft nie dazu kommen, daß die Entscheidungen durch noch so effizient und optimal durchstrukturierte Techniksysteme und Kommunikationssysteme fallen, der Bürger hingegen nicht mehr benötigt wird. Aktive Demokratie setzt den seine Rechte

aktiv wahrnehmenden Bürger voraus. Dies gilt es bei der Installation von regionalen und internationalen Kommunikationssystemen stets zu berücksichtigen.

Die Diskussion um die Risikogesellschaft, die auch in dem Bereich der Informations- und Kommunikationstechnik und deren Wirkungen diskutiert wird, mündet schließlich auch hier in die Feststellung, daß wir alle lernen müssen, unser Wissen zu beherrschen und nicht durch wissenchaftlich-technisches Wissen und deren Umsetzung beherrscht, ja in der Freiheit beraubt werden. Fast biblisch läßt sich sagen, was nützt es dem Menschen, umfangreiche Techniksysteme eingesetzt zu haben, wenn er als Mensch in seiner Freiheit hierunter leidet, ja bedroht wird. Diese Anlehnung an eine Bibelstelle verweist aber auch zugleich auf die umfangreiche Herausforderung nicht nur unter dem Aspekt der datenschutzrechtlichen Gestaltung, sondern auch der Werte, die einer technischen Einführungs- und Konzeptionsentscheidung zugrundeliegen.

Die Diskussion um die Herausforderung an die Gesellschaft wird inzwischen in politischen Parteien, gesellschaftspolitisch interessierten Gruppen, privaten Diskussionszirkeln und nicht zuletzt in kirchlichen Gesprächskreisen geführt, so daß ein begrüßenswerter Ansatz zur demokratischen Gestaltung der Technik gefunden werden könnte.

10 Jahre Datenschutz verweist natürlich auch darauf, daß Gesetzesnovellierungen in den letzten 10 Jahren vorgenommen wurden. Im Jahre 1987 sei besonders erwähnt die Novelle zum Bremischen Datenschutzgesetz und die Verabschiedung des Gesetzes über den Datenschutz in den Schulen.

10 Jahre Datenschutz wirft allerdings auch die Frage nach der Perspektive des Datenschutzes auf. Die technische Entwicklung mit immer neuen Möglichkeiten auf der einen Seite verweist auf der anderen Seite auf die Frage nach neuen Konzepten der Technikgestaltung. Es ist überfällig die Diskussion darüber zu eröffnen, wie das Datenschutzkonzept künftig aussehen kann. Es zeigt sich immer deutlicher, daß das gegenwärtige Datenschutzkonzept in sich unvollständig und brüchig ist. Die hohe Komplexität der technischen Entwicklung und die hieraus resultierenden Gefährdungen für die Persönlichkeitsrechte lassen die Fragen nach den verschiedenen Informationsflüssen, nach dem Bedürfnis bestimmter Informationen, nach der Verteilung bestimmter Informationen, nach deren Schutzintensität etc. erneut stellen. Es ist empfehlenswert, einem einschlägig vorgebildeten Team von verschiedenen Fachleuten und Wissenschaftlern den Auftrag zu erteilen, ein Konzept, z. B. Datenschutz 2000, vorzulegen. Dies ist selbstverständlich keine Bremer Angelegenheit allein, sondern eine Angelegenheit aller Länder und des Bundes.

1.2 Personalsituation

Der Datenschutzausschuß und der Haushaltsausschuß der Bremischen Bürgerschaft befaßten sich mit dem von mir vorgelegten Personalentwicklungskonzept 1995 und legten eine stufenweise Realisierung dieses Konzeptes fest. Die erste Stufe der Realisierung ist im Haushalt 1987 und durch das Haushaltsgesetz 1988 realisiert worden. Ich darf der Bremischen Bürgerschaft und den Mitgliedern der Ausschüsse hierfür meinen besonderen Dank für die Sache „Datenschutz" aussprechen. Die Diskussion um die Sozialverträglichkeit und die Gestaltung der Informations- und Kommunikationstechnik belegt inzwischen, wie wichtig das von mir vertretene Prinzip der datenschutzverträglichen Technikgestaltung von allen politischen Kräften eingeschätzt wird. Ich gehe deshalb auch zukünftig davon aus, daß die nächsten Stufen des Personalentwicklungsplans zügig realisiert werden.

2. Übergreifende Probleme der Rechts-, Informationstechnik- und Technologieentwicklung

2.1 Rechtsentwicklung

— Land Bremen —

2.1.1 Novelle Bremisches Datenschutzgesetz

Das Bremische Datenschutzgesetz (BrDSG) verdrängt für den Bereich der bremischen Behörden und sonstigen öffentlichen bremischen Stellen das Bundesdatenschutzgesetz (BDSG). Im Rahmen der konkurrierenden Gesetzgebung hat der Landesgesetzgeber den in § 7 Abs. 2 BDSG geregelten Vorbehalt für landesrechtliche Datenschutzgesetze ausgefüllt.

Nach der sog. „kleinen Novellierung" des BrDSG im Jahre 1982 trat am 1. Oktober 1987 eine umfangreiche Änderung des BrDSG in Kraft. Es gilt nunmehr das BrDSG

in der Fassung der Bekanntmachung vom 14. Oktober 1987 (BremGBl. S. 263). Mit dieser Novellierung wurde das BrDSG in wesentlichen Punkten geändert und um spezifische Regelungen ergänzt. Ziel dieser Novelle ist es, das verfassungsrechtlich geschützte Recht auf informationelle Selbstbestimmung einfachgesetzlich zu verwirklichen und die Anwendung der Informations- und Kommunikationstechnik datenschutzrechtlich mitzugestalten.

Dem neuen Bremischen Datenschutzgesetz kommt somit neben seiner Funktion als Auffanggesetz insbesondere Leitfunktion für die Fortentwicklung bereichsspezifischer Landesregelungen zu. Hervorzuheben sind vor allem die Einbeziehung der Akten, die Regelung der Zweckbindung, die Aufnahme der Erhebung und sonstigen Nutzung, die Regelungen zum automatisierten Abrufverfahren und das Geräteverzeichnis und schließlich die Wissenschaftsklausel sowie der Datenschutz bei Dienst- und Arbeitsverhältnissen.

Folgende wesentliche Änderungen des BrDSG sind in Kraft getreten:

Aufgabe des Datenschutzes

Aufgabe des Datenschutzes ist nicht mehr bloß die Verhinderung von mißbräuchlicher Datenverarbeitung, sondern Gegenstand des Datenschutzes ist nunmehr die Verarbeitung personenbezogener Daten in deren Verwendungs- und Verknüpfungszusammenhang. Damit wird der Rechtsprechung des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung Rechnung getragen. Nach diesem Recht wird die Befugnis des Einzelnen geschützt, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. In § 1 Abs. 1 BrDSG ist diese Aufgabe des Datenschutzes nunmehr bestimmt.

Anwendungsbereich

Der Anwendungsbereich des BrDSG erstreckt sich neben der Verarbeitung personenbezogener Daten in oder aus Dateien, jetzt auch auf die Verarbeitung personenbezogener Daten in oder aus Akten. Für den Bürger war es ohnehin nie verständlich, warum seine Daten, wenn sie in Akten gespeichert waren, nicht den Datenschutzbestimmungen unterliegen sollten. Gegenüber der Datenverarbeitung im automatisierten Verfahren oder in nicht-automatisierten Dateien sind für die manuelle Verarbeitung in und aus Akten abweichende Regelungen vorgesehen. So gilt nach § 6 Abs. 3 BrDSG, daß technische und organisatorische Maßnahmen sich insbesondere darauf zu richten haben, daß der Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung von Daten verhindert wird. Nach § 20 Abs. 2 Satz 2 BrDSG ist bei Akten anstelle eines Sperrvermerks zu vermerken, daß der Betroffene die Richtigkeit bestreitet. Besonderheiten für die Verarbeitung in Akten enthalten auch die Regelungen in §§ 13 Abs. 2, 19 Abs. 1, 20 Abs. 4 BrDSG. Ausdrücklich klargestellt wurde die Kontrollbefugnis des Datenschutzbeauftragten bzgl. der Datenverarbeitung in oder aus Akten.

Für das Verhältnis des BrDSG zum Bremischen Verwaltungsverfahrensgesetz gilt, daß auch bei Anwendung des Verwaltungsverfahrensgesetzes die Behörden die Bestimmungen des Datenschutzgesetzes zu beachten haben.

Für das Verhältnis zum Akteneinsichtsrecht in § 29 BremVwVfG bei laufenden Verwaltungsverfahren sei ausdrücklich auf § 19 Abs. 1 Satz 4 BrDSG hingewiesen.

Schutz für die Erhebung und Nutzung von Daten

Der Schutz des Rechts auf informationelle Selbstbestimmung wird auch dadurch verwirklicht, daß das bisherige 4-Phasen-Modell (Speichern, Übermitteln, Verändern und Löschen) erweitert wird um die Phase des Erhebens und jede sonstige Verwendung personenbezogener Daten als „Nutzen" (§ 2 Abs. 2 Nrn. 1 und 7 BrDSG). So ist die Phase der Erhebung personenbezogener Daten den gesetzlichen Zulässigkeitsvoraussetzungen unterworfen. Zum Schutz des Betroffenen dürfen diese Daten grundsätzlich nur bei ihm mit seiner Kenntnis erhoben werden (§ 10 Abs. 2 BrDSG). Damit soll gewährleistet werden, daß der Betroffene nachvollziehen kann, für welche Zwecke und Maßnahmen er seine Daten preisgeben soll, und er sich über die Konsequenz der Datenoffenbarung ein Urteil bilden und sich bewußt entscheiden kann. Werden gleichwohl Daten ohne seine Kenntnis erhoben, so ist er davon grundsätzlich zu benachrichtigen (§ 10 Abs. 5 BrDSG).

Zweckbindung

Eine wichtige Ergänzung zu dem Vorstehenden erfährt der Schutz des Betroffenen durch die Zweckbindung der Datenverarbeitung in § 12 Abs. 1 BrDSG. Danach dürfen Daten nur für einen bestimmten Zweck erhoben und für diesen Zweck übermittelt und auch nur für diesen Zweck verarbeitet werden. Der Bürger soll davor geschützt werden, daß ohne sein Wissen Zweckänderungen vorgenommen und so seine Daten losgelöst vom Erhebungszweck vielfältig genutzt werden.

Das Recht auf informationelle Selbstbestimmung gewährt dem Einzelnen einen Anspruch darauf zu erfahren, wer was wann bei welcher Gelegenheit über ihn weiß. Aufgrund dieses Rechtes und dem darauf beruhenden Zweckbindungsprinzip ist in § 13 Abs. 1 BrDSG vorgesehen, die Datenübermittlung dem Zweckbindungsprinzip zu unterwerfen. Hiervon darf nur abgewichen werden, wenn die in § 12 BrDSG vorgesehenen Ausnahmen es zulassen. Entsprechend darf der Empfänger nach § 13 Abs. 4 BrDSG die ihm übermittelten personenbezogenen Daten nur für die Zwecke verwenden, zu deren Erfüllung sie ihm übermittelt worden sind. Sind diese personenbezogenen Daten mit weiteren personenbezogenen Daten des Betroffenen oder eines Dritten in Akten so verbunden, daß sie nicht oder nur mit unvertretbarem Aufwand voneinander getrennt werden können, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder des Dritten an deren Geheimhaltung offensichtlich überwiegen. Allerdings ist eine weitere Verarbeitung dieser zusätzlichen Daten unzulässig.

Berichtigung, Sperrung und Löschung von Daten

Die Behörden sind nach § 20 Abs. 3 BrDSG nunmehr verpflichtet, personenbezogene Daten, deren Speicherung unzulässig oder deren Kenntnis zur rechtmäßigen Erfüllung der Aufgabe nicht mehr erforderlich ist, zu löschen. Im übrigen besteht nach § 20 Abs. 5 BrDSG die Verpflichtung, von der Berichtigung, Sperrung oder Löschung unzulässig gespeicherter Daten die Stellen zu unterrichten, an die Daten regelmäßig übermittelt worden sind.

Gestaltung der Informations- und Kommunikationstechnik durch Datenschutz

Das Datenschutzrecht gestaltet auch die Entwicklung und Anwendung der Informations- und Kommunikationstechnik unter dem Aspekt der Sozial- und insbesondere der Datenschutzverträglichkeit.

Erweiterung der Anwendung

Die moderne Text- und Datenverarbeitung war mit dem bisherigen Datei- und Verarbeitungsbegriff nicht vollständig abgedeckt, so daß dieser Begriff entsprechend der technischen Entwicklung zu erweitern war. Die Aktualisierung der technischen und organisatorischen Maßnahmen war ebenfalls notwendig geworden. Sie wurden überarbeitet und zum Bestandteil des Gesetzes (§ 6 Abs. 2 BrDSG) gemacht.

Dem zunehmenden Einsatz von Personal-Computern ist in der Weise Rechnung getragen worden, daß die speichernde Stelle nunmehr nach § 7 Abs. 3 BrDSG zusätzlich verpflichtet ist, ein Geräteverzeichnis zu erstellen, um eine Kontrolle der Anwendung überhaupt ermöglichen zu können. Darüber hinaus hat die speichernde Stelle für jede Datei eine Dateibeschreibung anzulegen (§ 7 Abs. 1 BrDSG).

Automatisierte Abrufverfahren

Eine besondere Gefährdung geht von Direktzugriffsverfahren (online-Verbindungen) aus, so daß es notwendig war, für den Bereich der öffentlichen Stellen des Landes solche online-Verbindungen nur aufgrund einer Rechtsvorschrift zuzulassen (§ 14 BrDSG). In Fällen, in denen bis zum Inkrafttreten des BrDSG ein solches Verfahren ohne entsprechende Rechtsgrundlage eingerichtet worden ist, wird durch eine Übergangsregelung sichergestellt, daß für höchstens zwei Jahre die bisherige Praxis weitergeführt werden darf.

Nach § 14 Abs. 2 BrDSG werden die Senatoren ermächtigt, für ihren Bereich automatisierte Abrufverfahren durch Rechtsverordnung einzuführen. Es wird ihnen aber auch vorgegeben, ein solches Verfahren nur nach Abwägung der Interessen der Betroffenen und der beteiligten Stellen einzurichten.

Nach § 14 Abs. 2 Satz 4 BrDSG bin ich vorher zu beteiligen.

Datenschutz bei Dienst- und Arbeitsverhältnissen

Die Verarbeitung von Daten durch öffentliche Stellen der bei ihnen Beschäftigten und von Bewerbern (Arbeitnehmerdatenschutz) ist in § 22 BrDSG geregelt. Die Notwendigkeit bereichsspezifischer Arbeitnehmerdatenschutzregelungen ergibt sich daraus, daß der Arbeitnehmer einem besonders starken Informationsdruck ausgesetzt ist, da der Arbeitgeber eine Vielzahl von Daten über ihn verarbeitet, beginnend mit der Datenerhebung bei der Einstellung, sich fortsetzend bei der Durchführung des Arbeits- und Dienstverhältnisses, der Personalplanung, der Speicherung von Überwachungs- und Protokollierungsdaten sowie der Datenverarbeitung aufgrund vielfältiger gesetzlicher Anforderungen. Mit Hilfe der automatisierten Personaldatenverarbeitung können die erhobenen Daten der Beschäftigten für die verschiedensten Zwecke genutzt werden, der Gefahr des Übergangs von der Personalverwaltung zur Personalüberwachung soll mit dem Arbeitnehmerdatenschutz begegnet werden.

Die Voraussetzungen und Zwecke, unter denen personenbezogene Daten verarbeitet werden dürfen, sind in § 22 Abs. 1 BrDSG abschließend aufgeführt. Die Verarbeitung in automatisierten Verfahren bedarf künftig der Zustimmung der obersten Dienstbehörde. Nach § 22 Abs. 6 BrDSG ist es jedoch verboten, daß dienst- und arbeitsrechtliche Beurteilungen sowie medizinische und psychologische Befunde des Beschäftigten automatisiert verarbeitet werden. Nach Abs. 2 dürfen personenbezogene Daten der Beschäftigten für Planungszwecke oder zur Durchführung dienstlicher, organisatorischer, sozialer oder personeller Maßnahmen verarbeitet werden, wenn dies hierfür erforderlich ist und schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden.

Bei Eignungsuntersuchungen zum Zwecke der Eingehung eines Dienst- oder Arbeitsverhältnisses darf nur das Ergebnis dieser Untersuchung mitgeteilt werden.

Wissenschaftsklausel

Als bereichsspezifische Norm des Datenschutzes regelt § 21 BrDSG die Verarbeitung personenbezogener Daten für wissenschaftliche Forschung. Mit dieser Norm soll die Konkordanz von grundgesetzlich garantierter Forschungsfreiheit einerseits und dem ebenfalls verfassungsrechtlich verankerten informationellen Selbstbestimmungsrecht des Bürgers andererseits hergestellt und bisherige Rechtsunsicherheiten beseitigt werden. Nach § 21 BrDSG ist die Datenverarbeitung zum Zwecke wissenschaftlicher Forschung grundsätzlich nur für bestimmte Forschungsvorhaben und nur mit Einwilligung des Betroffenen zulässig. Von dieser Einwilligung kann nur dann abgesehen werden, wenn die schutzwürdigen Belange der Betroffenen wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verarbeitung nicht beeinträchtigt werden. Auch haben Stellen mit der Aufgabe unabhängiger wissenschaftlicher Forschung dann Zugang zu den Daten ohne Einwilligung der Betroffenen, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, sind gesondert zu speichern, sobald der Forschungszweck dies erlaubt. Sie sind zu löschen, wenn dieser Zweck erreicht ist (§ 21 Abs. 3 BrDSG).

Nach § 21 Abs. 4 BrDSG ist es verboten, die Daten zu anderen als zu Forschungszwecken zu verarbeiten.

Findet das Bremische Datenschutzgesetz auf den Empfänger keine Anwendung, dürfen Daten an ihn nur dann übermittelt werden, wenn er sich verpflichtet, § 21 Abs. 3 und 4 BrDSG einzuhalten und sich der Kontrolle des Landesbeauftragten zu unterwerfen (§ 21 Abs. 5 BrDSG).

Auskunftsanspruch

Nach § 19 BrDSG hat der Bürger einen Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten, den Zweck und die Rechtsgrundlage der Speicherung und sonstigen Verarbeitung sowie über die Herkunft der Daten. Der Bürger kann anstelle der Auskunft auch Akteneinsicht verlangen. Leider besteht für die Sicherheitsorgane nach wie vor keine Verpflichtung, Auskunft zu erteilen. Wohl aber sind diese Behörden bei der Abwägung, ob Auskunft erteilt wird, gehalten, von ihrem pflichtgemäßen Ermessen Gebrauch zu machen. Es verbleibt deshalb bei der

bisherigen Rechtsauffassung, die in zwei Entscheidungen des OVG Bremen bestätigt wurde. Besser wäre allerdings eine eindeutige gesetzliche Regelung gewesen, die dieser Rechtsauffassung entspricht. Um die Prüfung der Ermessensentscheidung zu ermöglichen, ist in § 19 Abs. 4 BrDSG vorgeschrieben, daß die Verweigerung der Auskunft oder der Akteneinsicht zu begründen ist. Die Begründung ist nur dann nicht bekanntzugeben, wenn durch die Mitteilung der Gründe der mit der Verweigerung verfolgte Zweck gefährdet würde. Die wesentlichen Gründe für die Entscheidung sind aber aufzuzeichnen (§ 19 Abs. 4 BrDSG). Der Betroffene ist darauf hinzuweisen, daß er sich zur Überprüfung an mich wenden kann.

Anrufung des Landesbeauftragten

Jedermann kann sich an den Landesbeauftragten für den Datenschutz wenden, wenn er annimmt, daß er durch die Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt worden sei. Klargestellt wurde in § 30 BrDSG, daß niemand (auch nicht der öffentlich Bedienstete) dafür gemaßregelt oder benachteiligt werden darf, wenn er sich aufgrund tatsächlicher Anhaltspunkte, die für einen Verstoß gegen das Datenschutzgesetz sprechen, an mich wendet.

Stellung des Landesbeauftragten

Mit den neuen Vorschriften des 3. Abschnitts sollte insgesamt die Rechtsstellung des Landesbeauftragten für den Datenschutz gestärkt werden. Dies kann nicht allein dadurch erreicht werden, daß der Landesbeauftragte nunmehr der Dienstaufsicht des Senats unterstellt worden ist. Auch die Regelung in § 26 BrDSG, wonach die Entscheidung in den dort genannten Fällen der Aussagegenehmigung nach dem Beamtenrecht und nach § 96 StPO von der obersten Dienstbehörde lediglich im Benehmen mit dem Landesbeauftragten getroffen wird, die hinter den Regelungen in Hessen und in Nordrhein-Westfalen zurückbleibt, stärkt nicht die Unabhängigkeit des Landesbeauftragten, sondern beeinträchtigt diese in verfassungsrechtlich bedenklicher Weise.

Die rechtzeitige Beteiligung des Landesbeauftragten insbesondere an Planungen zur Einführung neuer Informationstechniken und -systeme, mit denen personenbezogene Daten verarbeitet werden sollen, sieht § 27 Abs. 4 BrDSG vor.

Die Kontrollbefugnis des Landesbeauftragten erstreckt sich nun auch auf Radio Bremen, soweit dort nicht ausschließlich zu eigenen publizistischen Zwecken personenbezogene Daten verarbeitet werden.

Straftaten und Ordnungswidrigkeiten

Wer Straftaten nach dem BrDSG begeht, wird nunmehr von Amts wegen gemäß § 37 BrDSG durch die Staatsanwaltschaft verfolgt. Es bedarf keines Strafantrages mehr.

Neu aufgenommen wurde in § 38 BrDSG eine Regelung über Ordnungswidrigkeiten. Danach kann derjenige, der personenbezogene Daten entgegen den Vorschriften des BrDSG erhebt, speichert, übermittelt, löscht, zum Abruf bereit hält, abruft oder nutzt, mit einer Geldbuße belegt werden.

2.1.2 Gesetz zum Datenschutz im Schulwesen

Die in den Vorjahren begonnenen Arbeiten zur Schaffung spezifischer Datenschutzregelungen im Schulbereich konnten im Berichtsjahr endlich mit einem Gesetzesbeschluß abgeschlossen werden. Anfang September, noch vor Ablauf der alten Legislaturperiode, verabschiedete die Bremische Bürgerschaft das Gesetz zum Datenschutz im Schulwesen. Es tritt am 1. Juni 1988 in Kraft.

Der abschließenden parlamentarischen Beratung vorausgegangen waren langwierige, verwaltungsinterne und parlamentarische Erörterungen sowie zum Teil sehr kontroverse öffentliche Diskussionen. Ich war an diesen Beratungen beteiligt und habe mich bemüht, zwischen dem Persönlichkeitsschutz der Betroffenen (Schüler, Eltern, Lehrer) und den Erfordernissen der Schulen und der Schulbehörden einen vernünftigen Ausgleich herzustellen. Nicht alle Wünsche der Beteiligten konnten berücksichtigt werden, doch insgesamt hat der Datenschutz im Schulbereich mit diesem Gesetz eine wesentlich verbesserte und präzisere Rechtsgrundlage erhalten. Das Land Bremen hat mit diesem speziellen Datenschutzgesetz gesetzgeberisches Neuland betreten. Es handelt sich bei diesem Gesetz um das erste eigenständige bereichsspezifische Datenschutzgesetz eines Landes. Ursprünglich

war geplant gewesen, das Schulverwaltungsgesetz um einige bereichsspezifische Datenschutzbestimmungen zu ergänzen und Details in einer Rechtsverordnung zu regeln. Im Verlauf des Gesetzgebungsverfahrens wurde dieser Gedanke jedoch fallengelassen. Statt dessen entschloß man sich zu einem eigenständigen Gesetz, das auch die notwendigen Details selbst regelt.

Die Zeit bis zum Inkrafttreten des neuen Gesetzes soll dazu genutzt werden, eine breite Schulöffentlichkeit und alle datenverarbeitenden Stellen und Personen im Schulbereich mit den Neuregelungen vertraut zu machen (vgl. zu diesem Gesetzgebungsvorhaben auch meine Ausführungen im 8. und 9. Jahresbericht unter Pkt. 5.4.1.1 und Pkt. 5.4.1).

2.1.3 Meldedatenübermittlungsverordnung

Im Berichtsjahr wurde die „Verordnung zur Durchführung des Meldegesetzes, insbesondere zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden (MeldDÜV)" von der Innendeputation beschlossen und am 12. Mai 1987 im Gesetzblatt der Freien Hansestadt Bremen verkündet. Damit fand eine lange und in vielen Punkten auch kontroverse Beratung dieser Rechtsmaterie ihren Abschluß. Ich hatte zum Entwurf dieser Rechtsverordnung ausführlich im 9. Jahresbericht unter Pkt. 5.2.2.1 Stellung genommen und konnte an den Beratungen der Innendeputation bzw. des entsprechenden Unterausschusses teilnehmen. Im Ergebnis habe ich mich nur mit einem Teil meiner Bedenken bzw. Anregungen durchsetzen können. Die Rechtsverordnung ist ohne Übergangsfrist am Tage nach ihrer Verkündung in Kraft getreten.

2.1.4 Richtlinien des Ausschusses für ADV (AADV)

Mit Wirkung vom 20. Mai 1987 wurden die AADV-Richtlinien, die das Antrags- und Genehmigungsverfahren von ADV-Systemen regeln, geändert. Im wesentlichen handelt es sich dabei um Änderungen, die die Wirtschaftlichkeit, Finanzierung und Organisation betreffen. Für den Datenschutz ist die Neuformulierung der Nr. 4 von Bedeutung:

„Sind Stellungnahmen ... und/oder des Landesbeauftragten für den Datenschutz erforderlich, sind diese den Anträgen hinzuzufügen." Damit wird die bisherige Praxis einiger Behörden, meine Stellungnahme — wenn überhaupt — unmittelbar vor AADV-Sitzungen oder vor Verfahrenseinführung einzuholen, hoffentlich zukünftig unterbunden.

Inzwischen wurde das BrDSG novelliert und unter § 27 Abs. 4 verpflichtend bestimmt, daß der Landesbeauftragte für den Datenschutz „über Planungen zum Aufbau automatisierter Informationssysteme rechtzeitig zu unterrichten ist, sofern in den Systemen personenbezogene Daten verarbeitet werden sollen".

2.1.5 Dienstvereinbarungen zum Einsatz von Informationstechnik

Im Rahmen des vom Senat beschlossenen Sparkonzeptes ist vorgesehen, in der bremischen Verwaltung schrittweise ein integriertes Bürokommunikationssystem einzuführen. Zunächst sollen Sachbearbeiter mit autonomen Rechnern und Rechnersystemen ausgestattet werden, um dann untereinander und/oder mit dem Rechenzentrum der bremischen Verwaltung verbunden zu werden. Wegen der behördenübergreifenden Bedeutung und der mit der Einführung dieses Systems verbundenen Gefahren für die Persönlichkeitsrechte und andere Rechte der Bediensteten sowie der personellen, sozialen und organisatorischen Veränderungen in den davon betroffenen Verwaltungen hat der Senat mit dem Gesamtpersonalrat Dienstvereinbarungen im Zusammenhang mit der Einführung neuer Technologien am 09. 09. 1986 abgeschlossen (Brem.ABl. 1986, S. 479), und zwar

— Dienstvereinbarung zur Sicherung der Arbeitsplätze und Arbeitsbedingungen der Mitarbeiter/innen bei einem Personalausgleich,

— Dienstvereinbarung über berufliche Weiterbildung der Mitarbeiter/innen,

— Dienstvereinbarung über den Einsatz automatischer Datenverarbeitungsanlagen.

Nach dem Bremischen Personalvertretungsgesetz gelten Dienstvereinbarungen unmittelbar und zwingend. Werden Bediensteten durch Dienstvereinbarungen Rechte eingeräumt, so ist ein Verzicht auf sie nur mit Zustimmung des Personalrats zulässig. Die Verwirkung dieser Rechte ist ausgeschlossen.

Weil gerade die Beachtung des Arbeitnehmerdatenschutzes bei der Einführung der neuen Informations- und Kommunikationstechnologien von entscheidender

Bedeutung ist, bin ich gebeten worden, zu den Dienstvereinbarungen aus datenschutzrechtlicher Sicht Stellung zu nehmen.

Die Dienstvereinbarungen regeln den Arbeitnehmerdatenschutz nicht umfassend, das ist die Aufgabe besonderer Rechtsvorschriften. Sie können nur ergänzend und ausgestaltend im Rahmen von Rechtsvorschriften (z. B. Bremisches Datenschutzgesetz) wirken.

Aus datenschutzrechtlicher Sicht sind folgende Bestimmungen hervorzuheben:

— Grundsatz der sozialverträglichen Technikgestaltung

Dieser Grundsatz beinhaltet, daß der Einsatz der automatisierten Datenverarbeitung menschengerecht zu gestalten ist. Dabei wird besonders die Wahrung des informationellen Selbstbestimmungsrechts der Beschäftigten hervorgehoben.

— Keine Datenverarbeitung in nichtdienstlichen Räumen

Diese Regelung verbietet nicht nur die Tele-Heimarbeit, sondern besagt generell, daß der Einsatz der automatisierten Datenverarbeitung zur Erledigung dienstlicher Aufgaben in privaten und nichtdienstlichen Räumen unzulässig ist. Damit wird der ADV-Einsatz überschaubarer. Die Festschreibung, nur in dienstlichen Räumen automatisierte Datenverarbeitung zu betreiben, gewährleistet im übrigen auch meine Kontrolltätigkeit.

— Verbot von Leistungs- und Verhaltenskontrollen

Danach werden automatische Datenverarbeitungsanlagen und Bildschirmgeräte nicht als Hilfsmittel zur individuellen Leistungs- und Verhaltenskontrolle eingesetzt. Ebenso ist eine Leistungs- und Verhaltenskontrolle durch technische Einrichtungen unzulässig. Auch die Programme und Daten dürfen nur für zugelassene Zwecke verwendet werden und nicht darauf ausgerichtet sein, individuelle und diesen vergleichbare Kontrollen von Gruppen durchzuführen.

Darüber hinaus dürfen die Ergebnisse maschineller Fehlerprüfungen nicht Gegenstand personalrechtlicher Vorgänge (z. B. Beurteilungen) werden.

— Einsichtsrecht des Personalrats in die Dokumentationsunterlagen

Die Dienststellen haben ein Verzeichnis der automatischen Datenverarbeitungsanlagen und Bildschirmgeräte und der daran beschäftigten Mitarbeiter/innen zu führen. Außerdem führt die Senatskommission für das Personalwesen ein derartiges Verzeichnis für den bremischen öffentlichen Dienst.

Die Führung derartiger Verzeichnisse kann neben der Erleichterung für den Personalrat bzw. Gesamtpersonalrat, ihre ihnen zugewiesenen Aufgaben zu erfüllen, auch meine Kontrolltätigkeit erleichtern.

— Zweckbindung der erhobenen Daten

Im Rahmen eines Personalausgleichs sind alle Umstände, die sich aus der Vor- und Ausbildung, der seitherigen Beschäftigung einschließlich zurückgelegter Bewährungszeiten und sonstige persönlichen und sozialen Verhältnisse der/des betroffenen Mitarbeiterin/Mitarbeiters angemessen zu berücksichtigen.

Die Regelung soll gewährleisten, daß die dazu erhobenen personenbezogenen Daten der Betroffenen nicht für andere Zwecke verwendet werden.

— Berufliche Weiterbildung

Soweit in einem neuen Aufgabengebiet neue Technologien eingesetzt werden, sind im Rahmen der dazu notwendigen Fortbildungsmaßnahmen auch Kenntnisse über die Wirkungsweise des Datenschutzes zu vermitteln.

Schließlich wird den einzelnen Dienststellen die Möglichkeit eingeräumt, ergänzende und konkretisierende Dienstvereinbarungen abzuschließen. In solchen Fällen bin ich gerne bereit, hinsichtlich der Formulierung von Datenschutzanforderungen beratend mitzuarbeiten.

Die Dienstvereinbarungen können eine gute Voraussetzung dafür bieten, daß das Recht auf informationelle Selbstbestimmung der Beschäftigten gewahrt bleibt.

— Bund —

2.1.6 Strafprozeßordnung

Die Datenschutzbeauftragten des Bundes und der Länder hatten die datenschutzrechtlichen Anforderungen an Informationsverarbeitungen im Strafverfahren for-

muliert. Ich habe die wesentlichen Punkte in meinem letzten Jahresbericht (vgl. Pkt. 5.3.1.6) hervorgehoben und den gesamten Beschluß im 9. Jahresbericht in Anlage 4 dokumentiert.

Der Bundesminister der Justiz hatte in seinem „Arbeitsentwurf eines Gesetzes zur Regelung der rechtlichen Grundlagen für Fahndungsmaßnahmen, Fahndungshilfsmittel und für die Akteneinsicht im Strafverfahren" (Stand: 31. 07. 1986) bereits einige dieser Anregungen aufgegriffen. Dieser Teilaspekt wurde vom Bundesminister der Justiz mittlerweile durch einen weiteren Entwurf für „Allgemeine Bestimmungen über die Speicherung, Verwendung und Übermittlung personenbezogener Daten durch die Strafverfolgungsbehörden" (Stand: 16. 07. 1987) ergänzt. Dieser Entwurf enthält Rechtsgrundlagen für die Speicherung und weitere Nutzung von Daten zu Zwecken der Strafverfolgung in verfahrensbezogenen und verfahrensübergreifenden Dateien. Weitere Bestimmungen betreffen die Errichtung von Dateien zu Zwecken der Vorgangsverwaltung und der Mitteilung über den Verfahrensausgang an die Polizei.

Der letztgenannte Entwurf, der mir vom Senator für Rechtspflege und Strafvollzug zugeleitet wurde, war auch Gegenstand von Erörterungen unter den zuständigen Referenten der Datenschutzbeauftragten. Auf dieser Grundlage habe ich gegenüber dem Senator für Justiz und Verfassung meine Stellungnahme abgegeben.

Der Gesetzentwurf trägt den Überlegungen der Datenschutzbeauftragten, die Informationsverarbeitung im Strafverfahren gesetzlich zu regeln, insoweit Rechnung, als er im einzelnen viele Vorschläge der Datenschutzbeauftragten zur Regelung der Informationsverarbeitung im Strafverfahren aufgreift. Der Entwurf enthält aber in seiner derzeitig vorliegenden Fassung nur erste Formulierungsvorschläge. Im Hinblick auf die vom Bundesminister der Justiz selbst geäußerte Vorläufigkeit der Formulierung habe ich die Vorschriften aus datenschutzrechtlicher Sicht nicht in aller Tiefe geprüft und bewertet. In meiner Stellungnahme gegenüber dem Senator für Justiz und Verfassung habe ich u. a. auf folgendes hingewiesen:

— Der Entwurf regelt die zulässige Nutzung von in Strafverfahren gewonnenen Daten durch Dritte (Nutzungsänderung). So beschreibt der Entwurf die Nutzung von Strafverfolgungsdaten durch die Polizei zum Zwecke der Gefahrenabwehr und der Verhütung von Straftaten. Der Regelung ist zuzustimmen, soweit damit anerkannt wird, daß eine zweckändernde Nutzung von Daten, die zu Strafverfolgungszwecken erhoben wurden, auch dann einer Ermächtigungsgrundlage bedarf, wenn der Nutzer mit einer Strafverfolgungsbehörde (hier: Polizei) organisatorisch identisch ist. Die Voraussetzungen für eine Nutzung der Daten durch die Polizei im präventiven Bereich müssen aber ausschließlich im Polizeirecht geregelt werden. Dem trägt der Entwurf nicht hinreichend Rechnung.

— Der Entwurf macht deutlich, daß eine Nutzung von Daten durch die Polizei nur möglich ist, wenn die in Polizeigesetzen bestimmten besonderen Voraussetzungen für die Erhebung der Informationen durch eine solche Maßnahme (z. B. polizeiliche Beobachtung, Durchsuchung) zur vorgesehenen Nutzung erfüllt sind. Dementsprechend habe ich angeregt zu verdeutlichen, daß ein Zugriff der Polizei auch dann ausgeschlossen bleibt, wenn die fraglichen Informationen durch Maßnahmen gewonnen werden, für die das Polizeirecht besondere Kompetenzen nicht enthält und die aufgrund der Generalklausel des Polizeirechts nicht zulässig wären. Eine entsprechende Regelung könnte etwaige Zweckbindungsvorschriften der Befugnisnormen für die Datenerhebung durch die Strafverfolgungsbehörden ergänzen.

— Der Entwurf regelt weiter die Speicherung von Strafverfahrensdaten in Dateien durch Behörden der Strafverfolgung und -vollstreckung sowie der Gerichte. Voraussetzung hierfür ist, daß die Datensammlungen den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit entsprechen. Dies kommt im Entwurf nur unzureichend zum Ausdruck. Insbesondere für die Errichtung von SPUDOK-Dateien sind im Hinblick auf die damit verbundenen erheblichen Eingriffe in das informationelle Selbstbestimmungsrecht von Beschuldigten und Dritten weitere einschränkende Anforderungen erforderlich (Im einzelnen hatten die Datenschutzbeauftragten hierauf schon im Beschluß vom 24./25. 11. 1986, den ich in meinem 9. Jahresbericht in Anlage 4 veröffentlicht habe, hingewiesen). Die Errichtung einer SPUDOK-Datei sollte im übrigen unter den Vorbehalt einer Errichtungsanordnung gestellt werden.

— Der Entwurf bringt nicht genügend zum Ausdruck, daß die Speicherung und Weitergabe personenbezogener Informationen in Strafverfahrensdateien grundsätzlich auf rechtmäßig erhobene Daten zu begrenzen ist. Einer ergänzenden Regelung bedarf daher die Speicherung und weitere Nutzung von Daten, die unter Verstoß gegen ein Datenerhebungsverbot gewonnen wurden; die Weiterverarbeitung in Strafverfahrensdateien kann nur zugelassen werden, sofern die Verwertung der Daten nicht im Hinblick auf die Rechtswidrigkeiten der Datenerhebung nach den dafür maßgebenden Bestimmungen unzulässig ist.

— Soweit dem Verteidiger das Recht eingeräumt wird, in Dateien gespeicherte Verfahrensdaten abzufragen, erhält er insbesondere bei SPUDOK-Dateien Zugriffsmöglichkeiten auf personenbezogene Daten von Verfahrensbeteiligten und Dritten, die weit über die Möglichkeiten der Akteneinsicht hinausgehen. Soweit der Verteidiger von seinen Rechten Gebrauch macht, ist er ebenso wie Strafverfolgungsbehörden für die Wahrung der Persönlichkeitsrechte Dritter verantwortlich; er hat die Zweckbindung der Daten auch im Verhältnis zu seinen Mandanten sicherzustellen. Um dies zu gewährleisten, ist zu prüfen, ob mit der Erweiterung des Datenzugriffs von Anwälten nicht sinnvollerweise auch eine effizientere Datenschutzkontrolle im Anwaltsbereich erforderlich sein wird, die über eine bloße Anlaßaufsicht (§ 30 BDSG) hinausgeht. Im übrigen verweise ich auch hier auf den im 9. Jahresbericht als Anlage 4 veröffentlichten Beschluß der Datenschutzbeauftragten unter Ziffer 1 Pkt. 2e bb.

— Im Entwurf fehlt eine Regelung für den Einsatz von sogenannten Falldateien, die für eine Vielzahl von Strafverfahren einer bestimmten Deliktsgruppe — zum Teil in Form von SPUDOK-Dateien — geführt werden (z. B. Rauschgift, Falschgeld, Wirtschaftskriminalität). Deren Einsatz bedingt strengere Forderungen und konkretere Voraussetzungen als die zu SPUDOK-Dateien im Entwurf getroffenen Regelungen. Insbesondere auf die Speicherung sogenannter „anderer Personen" und die Löschungsfristen ist besonderes Augenmerk zu richten. Die Einrichtung einer solchen Datei setzt in jedem Falle eine Rechtsverordnung voraus.

— Der Entwurf enthält auch Regelungen zur Errichtung verfahrensübergreifender Dateien mit Zugriffsmöglichkeiten anderer Strafverfolgungsbehörden. Meine Bedenken hierzu hatte ich bereits im letzten Jahresbericht unter Pkt. 5.3.1.7 (SISY) geäußert.

— Der Entwurf sieht den Erlaß von Errichtungsanordnungen für verfahrensübergreifende Dateien vor. Damit trägt er einer wesentlichen Forderung der Datenschutzbeauftragten weitgehend Rechnung. Es fehlt allerdings eine Anordnung über die Feststellung

  - vor allem der Suchmerkmale (Informationen, die der Erschließung der Datei dienen können),
  - der für die Anlage und Führung der Sammlung zuständigen Stelle,
  - der Zugriffsberechtigten,
  - im Falle eines automatisierten Verfahrens der Betriebsart des Verfahrens,
  - der Art der Geräte
  - sowie des Verfahrens zur Sperrung und Löschung.

— Die Übermittlungsregelung für verfahrensübergreifende Dateien muß den Grundsatz der Erforderlichkeit zum Ausdruck bringen. Ferner sind besondere Vorschriften für den Datenabruf im automatisierten Verfahren vorzusehen, ein Direktabruf durch andere Stellen als Strafverfolgungsbehörden ist auszuschließen.

— Soweit der Entwurf die Schaffung einer gesetzlichen Grundlage für Mitteilungen an die Polizei über den Verfahrensausgang enthält, verweise ich auf den in Anlage zu diesem Jahresbericht veröffentlichten Beschluß der Konferenz der Datenschutzbeauftragten (vgl. Anlage 1).

2.1.7 Entwurf eines Steuerreformgesetzes 1990

Durch einen anderen Datenschutzbeauftragten bin ich in den Besitz des Referentenentwurfs zum Steuerreformgesetz 1990 gekommen. Da sich auch im vorliegenden Falle der Senator für Finanzen nicht entschließen konnte, mich frühzeitig zu

beteiligen, obwohl schon beim ersten Hinsehen festzustellen ist, daß der Entwurf Vorschriften enthält, die einen tiefen Eingriff in das informationelle Selbstbestimmungsrecht von Empfängern von Sozialleistungen bedeuten, verblieben mir nur wenige Tage für die Erarbeitung einer Stellungnahme. Ich habe wie folgt vorläufig Stellung genommen:

Art. 15 des Entwurfes sieht eine Änderung der Abgabenordnung (AO) vor. Es soll ein neuer § 93 b eingeführt werden.

Nach dieser neuen Vorschrift wird den Trägern der Sozialleistungen eine Mitteilungspflicht auferlegt, wonach sie den Finanzbehörden zum Schluß eines Kalenderjahres den Empfänger, den Rechtsgrund und die Höhe der in diesem Kalenderjahr geleisteten Zahlungen (z. B. Krankengeld, Arbeitslosengeld, Kurzarbeitergeld, Schlechtwettergeld und Arbeitslosenhilfe etc.) schriftlich mitzuteilen haben, wenn diese DM 800— im Kalenderjahr übersteigen und soweit diese nicht vom Arbeitgeber im Rahmen seiner Aufzeichnungspflichten beim Lohnsteuerabzug zu bescheinigen sind.

Vorgesehen ist, daß der mitteilungspflichtige Träger der Sozialleistung den Betroffenen von dieser Verpflichtung, Mitteilungen zu erstellen, spätestens bei der Übersendung der ersten Mitteilung an die Finanzbehörde zu unterrichten hat. Der Betroffene ist hierbei in allgemeiner Form auf seine steuerlichen Erklärungspflichten hinzuweisen.

Aus datenschutzrechtlicher Sicht ist für das Recht des Sozialdatenschutzes von der Leitlinie auszugehen, daß niemand dadurch, daß er der Sozialversicherung angehört oder Ansprüche auf Sozialleistungen hat, mehr als andere Bürger der Preisgabe seiner personenbezogenen Daten ausgesetzt werden darf (vgl. Protokoll der 35. Sitzung des Arbeits- und Sozialausschusses des Deutschen Bundestages vom 15. 03. 1978). Vor diesem Hintergrund habe ich gegen die vorgesehene Einführung eines § 93 b AO erhebliche Bedenken:

Die darin enthaltenen Mitteilungspflichten über Lohnersatzleistungen entsprechen nicht dem Grundsatz der Verhältnismäßigkeit. Ein überwiegendes Allgemeininteresse, das die damit bewirkte Beschränkung des Rechts auf informationelle Selbstbestimmung der Betroffenen rechtfertigen könnte, läßt sich nicht feststellen. Die gesetzliche Verpflichtung aller Steuerpflichtigen, den Finanzbehörden die für die Besteuerung erheblichen Umstände vollständig und wahrheitsgemäß anzugeben, gilt auch für die Empfänger von Lohnersatzleistungen im Sinne des vorgesehenen § 93 b AO. Soweit die Betroffenen dabei der Unterrichtung bedürfen, welche Umstände den Finanzbehörden anzugeben sind, genügen entsprechende Hinweise der Leistungsträger in jedem Bewilligungsbescheid über Lohnersatzleistungen, wie dies in § 93 b Abs. 4 des Entwurfs — dort als zusätzliche Hilfe — bestimmt werden soll.

Ein Grund, die Empfänger von Lohnersatzleistungen über die allgemein geltende steuerliche Erklärungspflicht hinaus einer Kontrolle der Finanzbehörden zu unterwerfen, ist nicht ersichtlich. Die Begründung zu dieser Gesetzesänderung, wonach von der Einbeziehung der Lohnersatzleistungen in den Progressionsvorbehalt nach § 32 Einkommensteuergesetz (EStG) in erheblichem Umfang steuerlich unerfahrene Bürger betroffen sind und bei diesem Personenkreis nicht ohne weiteres vorausgesetzt werden kann, daß er seine steuerliche Erklärungspflicht erkennen und damit erfüllen kann, bedeutet durchaus eine Diskriminierung dieser Bürger.
Darüber hinaus wäre die Mitteilung nach § 93 b AO vielfach mangels steuerpflichtigen Einkommens der Betroffenen überhaupt nicht erforderlich. Vielmehr würde damit lediglich weitergehend ein unnützer und damit ungerechtfertigter Datenvorrat bei den Finanzbehörden geschaffen.

Ich habe daher den Senator für Finanzen gebeten, sich gegen eine Einfügung des § 93 b AO einzusetzen.

Außerdem widerspricht eine Vorschrift zur Durchbrechung des Sozialgeheimnisses nach § 35 Abs. 1 Sozialgesetzbuch I (SGB I) außerhalb des Sozialgesetzbuches dem Volkszählungsurteil des Bundesverfassungsgerichts, wonach eine Einschränkung des informationellen Selbstbestimmungsrechts bereichsspezifisch zu regeln ist, so daß Offenbarungsbefugnisse nur in den §§ 67—77 SGB X zugelassen sind. Dieses Prinzip, das im Sozialgesetzbuch durchgängig beachtet worden ist, dient der praktischen Handhabung und Transparenz dieses Gesetzes und darüber hinaus dem Schutz des Sozialgeheimnisses.

Unter Beachtung dieses Prinzips habe ich keine Bedenken, wenn die Träger der Sozialleistungen verpflichtet werden, die Betroffenen auf ihre steuerliche Auskunftspflicht nach § 93 Abs. 1 AO hinzuweisen.

2.1.8 Gesundheits-Reformgesetz und Sozialversicherungsausweisgesetz

Der Senator für Arbeit hat mir den Referenten-Entwurf eines Gesundheits-Reformgesetzes des Bundesministers für Arbeit und Sozialordnung zur datenschutzrechtlichen Bewertung vorgelegt. Wegen der Kürze der Zeit konnte ich zu diesem umfangreichen Gesetzesvorhaben zunächst nur vorläufig Stellung nehmen.

Der Entwurf soll das System der gesetzlichen Krankenkasse in einem neuen Sozialgesetzbuch V regeln und damit die entsprechenden Vorschriften der Reichsversicherungsordnung ablösen. Darüber hinaus sollen die in diesem neuen SGB V vorgesehenen Regelungen zu einer erheblichen Kostendämpfung im Gesundheitswesen führen.

Die im Rahmen dieses Gesetzentwurfes vorgesehene automatisierte Speicherung und Verarbeitung medizinischer Daten führt in erster Linie zum „gläsernen Patienten". Erheblich stärker als im bisherigen Verfahren wird in das informationelle Selbstbestimmungsrecht des versicherten Patienten eingegriffen und die Herstellung von Gesundheitsprofilen ermöglicht. Ein solcher Eingriff darf nur zugelassen werden, wenn er im überwiegenden Allgemeininteresse unabweisbar notwendig ist. Diese Voraussetzung ist bisher nicht ausreichend dargetan.

Der Referentenentwurf sieht die umfangreiche Verarbeitung von sehr sensiblen personenbezogenen Daten der Versicherten vor und eröffnet eine umfassende Verknüpfung von Versichertendaten zwischen den unterschiedlichsten Einrichtungen der gesetzlichen Krankenversicherung. Die Vereinheitlichung des Abrechnungsverfahrens, die die vollständige Automatisierung des Informationsflusses zwischen den beteiligten Einrichtungen bedeutet, erstreckt sich z. B. mit der Verwendung der Rentenversicherungsnummer und der beabsichtigten Einrichtung eines Medizinischen Dienstes der Krankenkassen auf andere Sozialleistungsträger.

Die Schaffung und Legitimierung dieser Vernetzungsstrukturen greift tief in das Recht auf informationelle Selbstbestimmung der Versicherten ein. Eine Vielzahl von Einzelregelungen entspricht nicht den Anforderungen, die das Bundesverfassungsgericht für die Zulässigkeit zur Einschränkung des informationellen Selbstbestimmungsrechts aufgestellt hat. Im Kontext betrachtet läßt der Referentenentwurf deutlich erkennen, daß mit der Erreichung des gesellschaftspolitisch unbestreitbar bedeutsamen Zieles der Kostendämpfung im Gesundheitswesen eine umfassende Überwachung und Kontrolle der Arbeitnehmer bzw. Versicherten einhergeht.

Unter Berücksichtigung des Volkszählungsurteils habe ich erhebliche verfassungsrechtliche Bedenken. Nach diesem Urteil ist eine Einschränkung des mit Grundrechtscharakter ausgestatteten Rechts auf informationelle Selbstbestimmung nur zulässig, wenn sie auf einer verfassungsgemäßen und bereichsspezifischen Rechtsgrundlage beruht, die den Prinzipien der Normenklarheit, Zweckbindung und Verhältnismäßigkeit entspricht.

Meine datenschutzrechtlichen Bedenken ergeben sich unter Beachtung dieser Anforderungen im einzelnen wie folgt:

Einschaltung des Betriebsarztes bei Teilarbeitsfähigkeit

Der Arzt soll verpflichtet werden, in Fällen, in denen er eine Teilarbeitsfähigkeit für möglich hält, in nicht näher bestimmten Fällen eine Stellungnahme des Betriebsarztes und des Medizinischen Dienstes einzuholen. Das beinhaltet Datenübermittlungen zwischen den genannten Institutionen.

Die Vorschrift sagt jedoch nichts darüber aus, welche Daten in diesem Zusammenhang von wem an wen übermittelt werden dürfen und wer welche Daten in welchem Umfange verarbeiten darf.

Den Institutionen ist insoweit ein weitgehendes Ermessen eingeräumt. Der Umfang einer Einschränkung des informationellen Selbstbestimmungsrechts kann aber nach dem Volkszählungsurteil im wesentlichen nur vom Gesetzgeber bestimmt werden. Der Betroffene hingegen kann den Umfang der damit verbundenen Datenverarbeitung aus der Vorschrift nicht erkennen. Es muß im übrigen bezweifelt werden, ob die damit verbundene Datenübermittlung überhaupt erforderlich ist und damit dem Prinzip der Verhältnismäßigkeit gerecht wird.

Nach der Begründung zu dem Gesetzentwurf soll die Norm vornehmlich dem Ziel dienen, den behandelnden Arzt anzuhalten, mehr und stärker als bisher bei der Bescheinigung der Arbeitsunfähigkeit die Möglichkeit der Teilarbeitsfähigkeit zu prüfen. Dazu bedarf es jedoch nicht des tiefen Eingriffs in das informationelle Selbstbestimmungsrecht des Versicherten. Dieses Ziel kann auch mit anderen Mitteln, die den Arzt verpflichten, erreicht werden.

Soweit der Arzt Informationen über die betrieblichen Gegebenheiten für die Prüfung benötigt, kann er diese beim Betroffenen selbst mit Sicherheit besser erfragen. Insbesondere bei größeren Betrieben wird der Betriebsarzt über die Gegebenheiten eines einzelnen Arbeitsplatzes ohnehin keine vollständigen Kenntnisse haben. Er wird diese in aller Regel selbst erst erfragen müssen. Das aber würde die Bekanntgabe von mit der Krankheit des Versicherten verbundenen Angaben an weitere Stellen im Beschäftigungsbetrieb voraussetzen. Ich vermag keinen Grund dafür zu erkennen, den Medizinischen Dienst für das gesetzte Ziel einzuschalten. Soweit der Arzt zu Problemen der Teilarbeitsfähigkeit der Beratung bedarf, mag ihm ein Anspruch oder gar eine Verpflichtung dazu dergestalt gegeben werden, daß er sich generell beim Medizinischen Dienst informiert. Über den Einzelfall könnte der Medizinische Dienst mangels Kenntnis der Umstände ohnehin nur nach Erheben von auf den Versicherten bezogenen Daten Auskunft geben.

Allgemeine Wirtschaftlichkeitsprüfungen

Diese Regelung stellt keine dem Prinzip der Normenklarheit entsprechende Rechtsgrundlage dar, soweit im Rahmen des Verfahrens zur Überwachung und Prüfung der Wirtschaftlichkeit personenbezogene Daten sowohl der Ärzte als auch der Versicherten den Prüfungsinstanzen zugänglich gemacht werden sollen. Im Zusammenhang mit anderen Regelungen dieses Gesetzentwurfes ergibt sich die Verarbeitung solcher Daten von hoher Sensibilität in erheblichem Umfange, deren Festlegung den am Gesamtvertrag beteiligten Institutionen überlassen bleiben soll. Die damit verbundene Regelungsbefugnis zur Einschränkung des informationellen Selbstbestimmungsrechts kann der Gesetzgeber nicht an die Verbände delegieren.

Der Gesetzgeber muß selbst regeln, in welchem Umfange welche personenbezogenen Daten der Versicherten und Ärzte offenbart werden sollen. Inwieweit die zu schaffende Rechtsgrundlage dann als verhältnismäßig angesehen werden kann, vermag ich erst bei Vorliegen einer normenklaren Rechtsgrundlage zu beurteilen.

Prüfung der Geschäfts-, Rechnungs- und Betriebsführung der Krankenkassen

Die vorgesehene Ermächtigungsnorm, wonach der Bundesminister für Arbeit und Sozialordnung allgemeine Verwaltungsvorschriften für die Durchführung von Prüfungen erlassen kann, kann das informationelle Selbstbestimmungsrecht der Versicherten bzw. Ärzte nicht einschränken, soweit im Rahmen dieser Prüfungen personenbezogene Daten eingesehen werden sollen. Hierzu bedürfte es ggf. einer Rechtsnorm.

Medizinischer Dienst der Krankenkassen

Die Neuschaffung eines Medizinischen Dienstes der Krankenkassen als Ersatz für den mit erheblich weniger Aufgaben und Befugnissen versehenen bisherigen vertrauensärztlichen Dienst als rechtsfähige Körperschaft des öffentlichen Rechts mit Selbstverwaltung stellt eine besondere Qualität der Kontrolle und Überwachung von Versicherten und Leistungserbringern dar.

Bei der Aufgabenstellung des Medizinischen Dienstes entstehen dort umfangreiche neue Datensammlungen, insbesondere über Versicherte. Der Gesetzentwurf enthält dazu einige Datenschutzregelungen. So werden z. B. die Krankenkassen und die Leistungserbringer verpflichtet, dem Medizinischen Dienst die für die Erfüllung seiner Aufgaben erforderlichen Unterlagen vorzulegen und Auskünfte zu erteilen. Der Medizinische Dienst ist befugt, selbst Daten in Kliniken, Krankenhäusern und Beschäftigungsbetrieben zu erheben.

Art und Umfang der Datenerhebung müssen jedoch so geregelt werden, daß für die Betroffenen das Ausmaß der Datenverarbeitung klar erkennbar wird (Grundsatz der Normenklarheit). Die Regelung muß auch erkennen lassen, welche Daten für welchen Zweck erhoben und verarbeitet werden dürfen (Grundsatz der Zweckbindung).

Erst wenn Regelungen vorgelegt werden, die diesen Grundsätzen genügen, kann ich beurteilen, ob der Grundsatz der Verhältnismäßigkeit gewahrt bleibt.

Soweit der Gesetzentwurf eine enge Zusammenarbeit des Medizinischen Dienstes mit anderen Institutionen vorschreibt, muß befürchtet werden, daß dadurch weitere personenbezogene Daten aus anderen Bereichen beim Medizinischen Dienst bekannt und gespeichert werden. Dies kann zu einer unverhältnismäßigen Verflechtung der einzelnen Leistungsbereiche führen, deren Notwendigkeit nicht ersichtlich ist. Soweit das Gebot der Zusammenarbeit die Verarbeitung personenbezogener Daten der Betroffenen beinhalten soll, bedarf es gerade hier einer datenschutzrechtlichen Regelung durch den Gesetzgeber.

In Verbindung mit der Vergabe einer Krankenversicherungsnummer, die mit der Rentenversicherungsnummer identisch sein soll, ergeben sich weitere Verknüpfungsmöglichkeiten, die zur Schaffung von Gesundheitsprofilen der Versicherten führen können.

Versichertennummer, Krankenversichertenkarte und Sozialversicherungsausweis

Inzwischen liegt neben dem Entwurf eines Gesundheitsreformgesetzes ein Referentenentwurf zu einem „Gesetz zur Einführung eines Sozialversicherungsausweises und zur Änderung anderer Sozialgesetze" vor. Danach ist u. a. vorgesehen, auch für den Bereich der gesetzlichen Krankenversicherung die Rentenversicherungsnummer zu verwenden. Diese „Gesamtversicherungsnummer" eröffnet unter Berücksichtigung der nicht zuletzt durch diesen Referentenentwurf zunehmenden Vernetzungsstrukturen so erhebliche Gefährdungspotentiale für die Versicherungspflichtigen, daß die insoweit vorgesehene Vergabe einer Versicherungsnummer nicht mit dem Verfassungsgrundsatz der Verhältnismäßigkeit zu vereinbaren ist.

Die Datenschutzbeauftragten des Bundes und der Länder haben wiederholt auf die Gefahren hingewiesen, die von der Einführung einer allgemeinen Personenkennziffer ausgehen.

Diese Bedenken werden durch den neuerdings vorgelegten Entwurf eines Gesetzes zur Einführung eines Sozialversicherungsausweises nicht ausgeräumt, sondern im Gegenteil verstärkt.

Durch die Einführung eines Sozialversicherungsausweises wird die Entwicklung, durch die die Rentenversicherungsnummer zu einem allgemeinen Personenkennzeichen wird, begünstigt und beschleunigt. Der Gesetzentwurf läuft somit allen bisher geäußerten Bedenken kraß zuwider. Die vorgesehene Mitführungspflicht nicht nur gegenüber „den zuständigen Behörden", sondern auch gegenüber „sonstigen Behörden nach anderen Vorschriften" kennzeichnet diese Entwicklung unmißverständlich.

Durch die allgemeine Verwendung der Rentenversicherungsnummer und die dadurch erleichterte Vernetzbarkeit mit Daten aus dem gesamten Bereich der Sozialverwaltung und der Gesundheitsverwaltung werden zusätzliche Mißbrauchsmöglichkeiten und Risiken für jene personenbezogenen Daten geschaffen, die sowohl nach höchstrichterlicher Rechtsprechung als auch nach einer Vielzahl gesetzlicher Regelungen als besonders schutzwürdig anzusehen sind, weil sie sowohl die intimsten Verhältnisse als auch das soziale Beziehungsgefüge und die persönliche Gesundheit eines Menschen betreffen.

Die Verpflichtung jedes Arbeitnehmers zur Mitführung eines Sozialversicherungsausweises stellt einen Grundrechtseingriff dar, der unter den im Gesetzentwurf vorgesehenen Regelungen nicht zulässig ist. Insbesondere bestehen Bedenken, ob die Grundsätze der Verhältnismäßigkeit und Geeignetheit gewahrt sind. Im übrigen ist es zweifelhaft, ob ein solcher Ausweis — nach der vorgesehenen und zu erwartenden Verwendungsvielfalt — überhaupt Mißbrauch ausschließen kann.

Es bestehen Bedenken, ob die im Entwurf vorgesehene Verordnungsermächtigung einer verfassungsrechtlichen Prüfung standhalten kann, weil dort die Verwaltung bei der Gestaltung des Ausweises zu Maßnahmen ermächtigt wird, die nach dem Volkszählungsurteil nur durch den Gesetzgeber angeordnet werden können. Dies betrifft insbesondere die Ermächtigung zur Regelung des Inhalts des Sozialversicherungsausweises.

Da der Ausweis nach der derzeitigen Fassung des Referentenentwurfs kein Lichtbild enthalten soll, ist er als Instrument der Kontrolle nur geeignet, wenn zusätz-

lich der Personalausweis mit kontrolliert wird. Dies begünstigt zumindest eine mißbräuchliche Verknüpfung mit Daten aus anderen Quellen, die das informationelle Selbstbestimmungsrecht weiter beeinträchtigen können, ohne daß der Betroffene dies beeinflussen kann.

Eine weitere Gefahr bei der Einführung eines Sozialversicherungsausweises besteht darin, daß er weit über den öffentlichen Bereich hinaus im Privatrechtsverkehr (z. B. beim Kreditgewerbe, beim Versandhandel, bei der Wohnraumvermietung, bis hin zur Einlaßkontrolle auf das Gelände von Privatfirmen) verwendbar ist.

Es ist davon auszugehen, daß der nach dem Entwurf eines Sozialversicherungsausweisgesetzes vorgesehene Sozialversicherungsausweis wegen der Nummernidentität gleichzeitig als Krankenversicherungskarte im Sinne des Referentenentwurfes eines Gesundheits-Reformgesetzes angesehen werden kann, zumal die Karte maschinell verwendbar ausgestaltet werden kann. Daß die bundeseinheitliche Gestaltung der Karte (bzw. des Sozialversicherungsausweises) unter Berücksichtigung der Anforderungen des Volkszählungsurteils nicht per Vertrag vorgenommen werden kann, sei hier immerhin noch erwähnt.

Weitergabe von Leistungsdaten

Es ist vorgesehen, daß die Spitzenverbände der Krankenkassen, der Kassenärztlichen Vereinigungen und Apotheken in noch abzuschließenden Verträgen bzw. Vereinbarungen das Nähere über die Art und Weise, Inhalt, Form und den Umfang der Übermittlungen von Leistungsdaten bestimmen sollen. Solche Vereinbarungen stellen keine den Anforderungen des Volkszählungsurteils entsprechende Rechtsgrundlage zur Übermittlung von personenbezogenen Daten Versicherungspflichtiger dar. Eine so geartete gesetzliche Regelung würde einer verfassungsrechtlichen Prüfung (überwiegendes Allgemeininteresse, Verhältnismäßigkeit und Übermaßverbot, Normenklarheit und Zweckbindung) nicht standhalten. Die Bestimmungen dieses Abschnittes bedürfen einer grundlegenden Überarbeitung.

Im Entwurf vorgesehene Datenschutzregelungen

Der hier vorgesehene Verweis auf die Vorschriften des SGB I und SGB X reicht unter Berücksichtigung der durch die Automatisierung zunehmenden Gefährdungspotentiale hinsichtlich der Persönlichkeitsrechte der Versicherten und den Anforderungen des Volkszählungsurteils, wie sich aus meinen vorstehenden Ausführungen ergibt, nicht aus.

Insbesondere die Vorschrift des § 79 SGB X mit Verweis auf Regelungen des Bundesdatenschutzgesetzes, soweit Sozialdaten in Dateien verarbeitet werden, bedarf einer die höchstrichterliche Rechtsprechung beachtenden Überarbeitung.

Der Entwurf zum Gesundheitsreformgesetz greift wegen der vorgesehenen vielfältigen Verknüpfungen von Daten und der verschiedenen automatisierten Auswertungen und Abgleiche einschneidend in das Recht auf informationelle Selbstbestimmung der Betroffenen ein.

Die bisherigen Regelungen hinsichtlich der Bestellung von betrieblichen Datenschutzbeauftragten sind überarbeitungsbedürftig. Die Stellung, die Unabhängigkeit und die besonderen Fachkenntnisse sollten für diese internen Datenschutzbeauftragten bereichsspezifisch geregelt werden.

Auswertung personenbezogener Daten

Der Entwurf sieht eine versichertenbezogene bzw. leistungserbringerbezogene Auswertung vor, ohne daß klargestellt wurde, wer in welchem Umfang welche Auswertungen personenbezogener Daten vornehmen darf. Diese Regelungen stellen einen gravierenden Eingriff in das informationelle Selbstbestimmungsrecht verschiedender Betroffenengruppen (z. B. Versicherte, Familienangehörige, Ärzte, Zahnärzte, Hebammen, Masseure etc.) dar. Die hier ermöglichte Erstellung von Persönlichkeitsprofilen der verschiedenen Betroffenen stellt einen so weitgehenden Eingriff in deren Persönlichkeitsrecht dar, so daß hier nicht nur verfassungsrechtliche Bedenken hinsichtlich des Regelungsinhaltes, sondern auch wegen des Fehlens jeglicher Verfahrens- und organisatorischer Vorkehrungen zur Datensicherung, bestehen.

Beratung der Versicherten

Erst aus der Begründung ergibt sich, daß diese Vorschrift offensichtlich insbesondere dazu dienen soll, vermutete mißbräuchliche Inanspruchnahmen von Versicherungsleistungen durch den Versicherten aufzudecken.

Diese Vorschrift unterstellt, daß eine Vielzahl von Versicherten Versicherungsleistungen mißbräuchlich in Anspruch nimmt. Da eine Überprüfung der Leistungsdaten durch den Medizinischen Dienst vorgesehen ist, kann die Einschränkung des informationellen Selbstbestimmungsrechts nur dann verhältnismäßig sein, wenn eine relevante Zahl von Mißbrauchsfällen besteht. Die Vermutung allein reicht nicht aus, eine solche Überwachung und Kontrolle als verhältnismäßig anzusehen. Soweit hier auch die Daten von Leistungserbringern ausgewertet werden sollen, bedarf es hierzu einer verfassungskonformen Regelung.

Auskunftspflicht der Krankenkasse

Der hier vorgesehene Umfang des Auskunftsanspruchs entspricht nicht dem Prinzip der Transparenz. Da es sich um eine bereichsspezifische Regelung handelt und in der Begründung zu dieser Vorschrift darauf hingewiesen wird, daß die bisherigen Regelungen im Sozialgesetzbuch X und im Bundesdatenschutzgesetz unberührt bleiben, sollte diese Absicht in diesem Entwurf eingesetzt werden. Darüber hinaus halte ich es bei der Vielzahl der hier zu verarbeitenden intimsten Daten für unabdingbar, den Auskunftsanspruch des Versicherten erheblich auszuweiten.

Der Auskunftsanspruch muß sich auf jeden Verarbeitungsvorgang der personenbezogenen Daten des Betroffenen erstrecken. Eine Einschränkung des Auskunftsrechts durch Satzung ist nicht vorzusehen. Außerdem ist der Auskunftsanspruch gegenüber dem Medizinischen Dienst und den Kassenärztlichen Vereinigungen festzulegen.

Verwendung zu Forschungszwecken

Die unter der Überschrift „Besonderer Verwendungszweck" vorgesehene Forschungsklausel stellt keine den Prinzipien der Normenklarheit, Zweckbindung und Verhältnismäßigkeit entsprechende Rechtsgrundlage dar. Soweit personenbezogene Daten der Versicherten für Forschungsvorhaben verarbeitet werden sollen, liegt eine Zweckänderung vor. Es ist zwar zu begrüßen, daß nach der vorgelegten Begründung durch diese Regelung die Erstellung von Leistungs- und Gesundheitsprofilen auf Umwegen verhindert werden soll, doch läßt die Vorschrift dies erstaunlicherweise wohl auf direktem Wege zu. Die Vorschrift bedarf bezüglich ihrer Zweck- und Zielrichtung und hinsichtlich des Verhältnisses zu § 75 SGB X einer Überarbeitung. Außerdem ist es nicht erforderlich, personenbezogene Daten über die im Entwurf genannten Fristen hinaus aufzubewahren.

Ich habe den Senator für Arbeit gebeten, meine verfassungsrechtlichen Bedenken bei den weiteren Erörterungen dieser Gesetzentwürfe einzubringen und mich über das Ergebnis seiner Bemühungen zu unterrichten.

2.2 Informationstechnik-Entwicklung

2.2.1 TELEBOX-Dienst der Deutschen Bundespost

In meinen vergangenen Jahresberichten habe ich wiederholt über die computergesteuerten Dienstleistungen der Deutschen Bundespost berichtet und auf Gefahren und Risiken hingewiesen. Eine weitere Dienstleistung stellt sich mit dem Mailbox-System TELEBOX dar. Dieser Dienst ist eine „Postkasten"-Datei, in die man Nachrichten für bestimmte oder unbestimmte Empfänger hinterlegen kann. Diese Datei ist in einem Zentralrechner der Deutschen Bundespost gespeichert, der auch die Zugriffsberechtigung überprüft. TELEBOX-Nachrichten können entweder asynchron über das Fernmeldenetz, mit Hilfe eines Akustikkopplers über einen beliebigen Telefonanschluß oder über die DATEX-Netze der Deutschen Bundespost übertragen werden, wenn entsprechend genormte Übertragungsprotokolle vorhanden sind. TELEBOX ist auch mit dem Btx-Mitteilungsdienst verbindbar, so daß die Nutzer beider Systeme untereinander Nachrichten austauschen können. TELEBOX kann auch grenzüberschreitend verwendet werden, wenn im Ausland entsprechende gleichartige Systeme verwendet werden. Die Datenendeinrichtung PAD (Paketierer-Depaketierer) sorgt für die Zeichenumsetzung. Eingabe und Ausgabe können von beiden Endbenutzern über computergesteuerte Terminals (PC, Drucker usw.) vorgenommen werden.

Gesichert ist das TELEBOX-System mit einem Zugriffsschutz. Eine offene Identifikationsnummer erlaubt dem bekannten Benutzer den Einstieg in das System selbst, während ein verdecktes Paßwort, das vom Benutzer selbständig änderbar ist, den Zugriff auf Teilbereiche der Bundespost-Datei erlaubt. Die Bundespost empfiehlt, die Box nur von einer Person benutzen zu lassen, damit Mißbrauch ver-

hindert werden kann. Sie bietet aber auch gleichzeitig eine Zugriffsprotokollierung an, die dem Benutzer zur Verfügung gestellt wird. Dieser hat damit die Möglichkeit zu kontrollieren, ob ein unbefugter Zugriff (und damit Erkenntnis seines persönlichen Paßwortes) erfolgt ist.

Den weiteren unbefugten Zugriff mit Hilfe des ausspionierten Paßwortes kann er verhindern, indem er das Paßwort verändert.

Zusätzliche Sicherheit soll ein mitteilungsbezogenes Paßwort bieten, das zwischen Sender und Empfänger einer Mitteilung vereinbart werden muß.

Die hier skizzierten Sicherungsmaßnahmen dürfen jedoch nicht darüber hinwegtäuschen, daß es sich um ein prinzipiell offenes System handelt, das durch Paßwortschutz nur eingeschränkt gegen unberechtigten Zugriff zu sichern ist. Im übrigen bestehen die gleichen Sicherungsrisiken, die auch bei Btx oder anderen Postdiensten vorhanden sind.

Die TELEBOX-Datei der Deutschen Bundespost oder einer Gruppe von Anwendern bietet dem nicht-berechtigten „Einsteiger" ein unter Umständen sehr deutliches Kommunikationsprofil des TELEBOX-Nutzers. Die Deutsche Bundespost hat durch geeignete automatisierte und organisatorische Kontrollverfahren zu gewährleisten, daß weder von innen noch von außen der Nachrichtentransfer oder die -speicherung unbefugt verfolgt werden kann. Es ist zwar teilweise in der Telekommunikationsordnung geregelt, jedoch scheint hier eine ständige Verbesserung des Sicherheitssystems notwendig zu sein. Ich denke dabei insbesondere an die Meldungen aus der jüngsten Vergangenheit, daß „Hacker" in der Lage waren, sich unberechtigt Zugang zu Systemen zu verschaffen und dort abgelegte Informationen unberechtigt lesen, verändern und neue Mitteilungen hinterlegen bzw. in Umlauf bringen konnten.

2.2.2 Dienstleistungen im Zahlungsverkehr

Die Kreditinstitute gehören zu den Institutionen der Wirtschaft, die intensiv automatisierte Datenverarbeitung betreiben. Die rationelle Verarbeitung des umfangreichen Datenanfalls beim Zahlungsverkehr führt fast zwangsweise zur Standartisierung und Automatisierung von Dienstleistungen im Zahlungsverkehr. Im „besonderen" Angebot der Banken und Sparkassen sind neben dem originären Kundendienst zwischenzeitlich DV-gestützte Systeme, die dem Kunden umfassende Informationen, schnellere Bedienung, risikogeminderte Geschäftsverbindungen, einfachere Kontenführung und bessere Liquidität bieten können. Dazu gehören Geldausgabe- und Annahmeautomaten, Selbstbedienung bei der Kontenführung, Expertensysteme für Beratung und Vermittlung, interne und externe Informationssysteme sowie Cash-Management-Systeme für die Optimierung der Zahlungsströme bei Unternehmen (auch im internationalen Zahlungsverkehr). Zu nennen sind hier auch das Btx-Homebanking, Kreditkarten und die POS (Point-of-sale)-Zahlungsverfahren im Einzelhandel.

Die durch die Automatisierung hervorgerufenen Veränderungen im Zahlungssystem führen dazu, daß die personenbezogene Informationsverarbeitung insgesamt erheblich zunimmt. Deshalb gewinnen Fragen des Datenschutzes (z. B. Zulässigkeit und Transparenz der Verarbeitung, Betroffenenrechte und Datensicherheit) zunehmend an Bedeutung.

Datenschutzrechtlich stellen sich vor allem die Probleme der Differenzierung, wer speichernde Stelle oder Auftragnehmer insbesondere bei ausländischen Kreditinstituten ist, wie die Datensicherheit bei Zahlungsverkehrssystemen gewährleistet wird, wie der Bürger seine Datenschutzrechte verwirklichen kann und wie die Datenschutzkontrolle im internationalen Zahlungsverkehr erfolgen soll.

Ein zentrales Problem bei den automatisierten Dienstleistungen im Zahlungsverkehr ist darin zu sehen, daß immer stärker die Verantwortlichkeit für den sicheren Zahlungsverkehr dem Kunden aufgebürdet wird. Obwohl der Kunde die Datenströme kaum verfolgen kann, trägt er den größten Teil des Verarbeitungs- bzw. Handhabungsrisikos. Wenngleich die Banken einer Haftungspflicht unterliegen, so steht doch der Kunde bei Mißbrauch von z. B. Scheckkarte und Persönliche Identifikationsnummer (PIN) stets in der Beweispflicht, die bis zum Beweis des unsicheren Systems und der Sicherheitslücken geht. Dabei ist ein besonderer Schwachpunkt die PIN, die oftmals an offenen von mehreren Seiten einsehbaren Eingabestationen benutzt werden muß. Da die Änderung dieser PIN vom Kunden selbst nicht durchgeführt werden kann, die „Stillegung" und „Neuvergabe" einer

PIN mit großen Umständen verbunden ist, ist die Gefahr der Benutzung einer ausgespähten PIN groß.

Insgesamt sollte die Kreditwirtschaft ihre Anstrengungen zur Sicherheit des Scheckkartensystems erhöhen.

Die Scheckkarte selbst ist zwischenzeitlich zu einem Sicherheitsinstrument durch Einsatz der sog. MM-Box im automatisierten Zahlungsverkehr geworden. Die MM-Box prüft den Kartenkorpus als Unikat. Somit ist nahezu gewährleistet, daß Kopien nicht verwendet werden können. Dennoch muß zur Erhöhung der Sicherheit des Systems gefordert werden, daß die persönliche Identifikationsnummer auch tatsächlich persönlich wird und einer flexiblen Änderung unterliegt.

Die Datenströme in vernetzten Zahlungsverkehrs-Systemen unterliegen besonderen Sicherheitsrisiken. Wie unter Pkt. 2.2.3 erläutert wird, ist das Eindringen in Netze und Netzrechner infolge nicht ausreichender Sicherheitsvorkehrungen möglich. Inwieweit hier eine Datenverschlüsselung für zusätzliche Sicherheit sorgen kann, hängt von dem installierten System ab. Neben den „Netzrisiken" sind weitere datenschutzrechtliche Belange bei Verfahren zu beachten, die

— grenzüberschreitend Zahlungsverkehrsdaten untereinander austauschen. Das trifft nicht nur für den Datenaustausch zwischen den Banken untereinander zu, sondern auch für den Datentransfer über zwischengeschaltete internationale Clearing-Zentralen, die dem Kunden nicht bekannt sind;

— die Benutzung von POS-Kassen ermöglichen. Je nach Ausgestaltung des Systems kann dies zur Identifizierung und zur Abbildung seines Verhaltens führen. So können dort z. B. sowohl Bankverbindung und Name als auch „Liquiditätsengpässe" bekannt werden.

  Der Kunde begibt sich durch die Verwendung besonderer Kreditkarten an POS-Kassen in ein System der „Liquiditätsüberwachung" außerhalb der Kreditinstitute, vor dem er sich nicht schützen kann.

Die Entwicklung im internationalen Zahlungsverkehr und die Überlegungen zur Einführung neuer Kreditkartensysteme erfordern auch, daß die Verantwortlichen dieser Systeme Datenschutzkonzepte vorlegen. Beobachtet man die Diskussion auf Fachtagungen und Kongressen zu dieser Thematik, so ist sie überwiegend dadurch gekennzeichnet, daß Datenschutzprobleme so gut wie keine Rolle spielen.

Da sich hier aber Datenschutzprobleme stellen, hat die Konferenz einen eigenen Arbeitskreis eingesetzt, der sich diesen Fragen zuwendet. An diesem Arbeitskreis nehme ich teil.

2.2.3 Netzsicherheit

Im Rahmen der Beschreibung der integrierten Bürokommunikation und arbeitsplatzorientierten Datenverarbeitung habe ich in den vergangenen Jahresberichten wiederholt Teilprobleme der Vernetzung angesprochen. In diesem Jahresbericht will ich mich mit der Netzproblematik allgemein auseinandersetzen, ohne den Anspruch auf Vollständigkeit zu erheben.

Die steigende Leistungsfähigkeit von Rechnern und Übertragungsmedien bietet privaten Unternehmen und öffentlicher Verwaltung zunehmende Möglichkeiten, die dezentralen Rechnersysteme untereinander und/oder mit zentralen Rechnersystemen zu verbinden, um hierdurch Informationsverarbeitungsprozesse rationeller zu gestalten. Gemeinsame und individuelle Datenbestände können leichter genutzt werden; der Nachrichten- und Informationsaustausch kann erheblich beschleunigt werden. Dieses kann innerhalb privater Netze, aber auch über Verbindungen zu öffentlichen Netzen geschehen.

Der Trend zu vernetzten ADV-Systemen zeichnet eine neue Generation von Informationssystemen vor und führt zu der Frage, ob wir uns schon in der „vernetzten Informationsgesellschaft" befinden. Eine derartige Gesllschaftsform ist leichter verwundbar, als das bisherige System mit autonomer, voneinander unabhängiger Informationsverarbeitung. Die Mißachtung von Übertragungs- und Verarbeitungsregeln birgt die Gefahr unbefugter Eingriffe in geschützte Rechtspositionen des Individuums in sich und führt damit zur Verletzlichkeit der Gesellschaft und zum Überwachungsstaat.

In diesem Zusammenhang weise ich beispielhaft auf die anstehende Gesundheitsstruktur-Reform (siehe Pkt. 2.1.8) hin. Der Plan, die Sozialversicherungsnummer

für alle Sozialleistungsträger als Klientennummer einzusetzen, birgt die Gefahr in sich, daß die Sozialleistungssysteme miteinander verzahnt werden und die Daten jedes einzelnen miteinander so verknüpft werden können, daß ein individuelles „Sozialleistungsbild" entsteht. Das kann weder im Interesse des einzelnen noch der Gesellschaft sein. Dies ist ein elementares Datenschutzproblem.

Ein Netz im Sinne der automatisierten Datenverarbeitung (ADV) ist die Verbindung von Dateien bzw. Datenbanken über rechnergestützte Datenstationen. Die Übertragung der Daten erfolgt über posteigene oder betriebsinterne Leitungen. Es wird zwischen öffentlichen und privaten Netzen unterschieden, die sowohl, jedes für sich, geschlossene Bereiche umfassen als auch untereinander verknüpft sein können.

Über öffentliche Netze wie DATEX-L, DATEX-P, Direktrufnetz und Telefonnetz bietet die Deutsche Bundespost ihre Dienste, z. B. Fernsprechen, Telex, Telefax, Teletex, Telebox ,an, die für alle Anschlußinhaber offen zugänglich sind. Der Postdienst „Bildschirmtext" (Btx) kann auch in einem geschlossenen Benutzergruppensystem verwendet werden. Dieses geschlossene System soll verhindern, daß der Benutzergruppe nicht angehörende Personen, Institutionen oder Firmen Zugang zum System erhalten.

Private Netze können vom Grundsatz her als geschlossene wie auch als offene Netzwerke betrieben werden. Übergänge von einem Privat-Netz zum anderen und zum öffentlichen Netz sind möglich.

Netzübergreifende Nachrichten- und Datenkommunikation führt dazu, daß technische und organisatorische Standards notwendig sind. Es haben sich verschiedene Organisationen und Institutionen auf nationaler und internationaler Ebene gebildet, die hinsichtlich der Standardisierung Grundlagen und Normen geschaffen haben. Über diese Bemühungen zur einheitlichen internationalen Normung soll an dieser Stelle nicht weiter berichtet werden.

Wenn über die Architektur eines Netzes (Kommunikationssystem) geschrieben wird, dann muß auch über Übertragungsprotokolle und deren Normung gesprochen werden. Die Schnittstellen-Normierung ist insbesondere durch die ISO (International Standardization Organisation) vorangetrieben worden. Grundlage für die Verbindung von Datensystemen ist dabei das Referenzmodell OSI (Open Systems Interconnect). In diesem Modell ist die Durchführung der Übertragung in Schichten aufgeteilt, deren Beziehungen untereinander in einem hierarchischen System festgelegt sind. Die Einteilung erfolgt in sieben Schichten, wobei die unterste Schicht die physikalische Datenübertragung abdeckt, während die höchste Schicht das vereinbarte Protokoll der Ebene Anwendung beinhaltet.

Für den Entwurf von Software und für eine übersichtliche Beschreibung der Funktionen ist das Referenz-Modell nützlich. Obwohl es einerseits zeigt, daß der Benutzer eines Netzes keine Vorstellung zu haben braucht, wie im speziellen Benutzungsfalle der Transport seiner Daten und die Kontrolle darüber vonstatten geht, ist hier dennoch ein Ordnungsprinzip gegeben, das über den organisierten logischen Weg der Informationen zwischen zwei Kommunikationspartnern jederzeit Aufschluß gibt. Schichten-Protokolle (Schnittstellenprogramme zwischen den einzelnen Ebenen einer Übertragung, wie sie ISO festgelegt hat) können einige Sicherheit bieten.

Das Schichten-Modell der ISO ist zwischenzeitlich bei der Kommunikationsüberwachung und -steuerung allgemein anerkannt. Nicht alle Netzwerke sind jedoch nach diesem System aufgebaut. Es ist in jedem Fall Sache des Anwenders, für die Sicherheit des Übertragungsprozesses zu sorgen und bei der Auswahl der Netzsoftware auf die Realisierung der genormten Schnittstellen zu achten.

Mit dieser Normung sind jedoch nicht alle Risiken ausgeschaltet, die bei der Vernetzung entstehen. Ich will in diesem Zusammenhang nur die „Hacker"-Aktivitäten in internationalen Netzen nennen, die über Pressemeldungen bekannt wurden. Sicherlich kann man derartig spektakuläre unbefugte Zugriffe, z. B. auf Rechner eines internationalen Forschungsnetzes, durch intensivierten Zugriffsschutz vermeiden. Angriffe auf das Transportmedium (Leitung) lassen sich jedoch kaum verhindern. So ist die Übertragung über Lichtwellenleiter sicherlich weniger anfällig als die Übertragung über Kupfer- (z. B. Koaxial-)Kabel. Dennoch müssen hier zusätzlich organisatorische und technische Maßnahmen ergriffen werden, um das „Anzapfen" zu verhindern, zumindest jedoch zu erschweren. Die Verwendung von entsprechenden Übertragungsstrukturen, die die Kontrolle der abgehenden und

ankommenden Informationen durch Abgleich übernehmen, wie z. B. die Token-ring-Kommunikation, können das Risiko der Informationsmanipulation weiter mindern. Das Abhören von Übertragungen, z. B. durch Aufnahme von Induktiv-Strömen, läßt sich ebenfalls nicht immer vermeiden. Diese Art von „Hacking" ist relativ einfach. Hier hilft letztlich nur eine Verschlüsselung der Daten bzw. Informationen.

Da offene Netze, insbesondere die öffentlichen, für Angriffe besonders anfällig sind, weil die Leitungen und Leitungsanschlüsse relativ ungeschützt zugänglich sind, besteht die Forderung gegenüber der Deutschen Bundespost, im Rahmen der Digitalisierung der Postdienst-Übertragungen (ISDN = Integrated services digital network) u. a. einen Verschlüsselungsdienst als Sicherheitsdienstleistung mit anzubieten. Das wäre sicherlich ein Service, der, mit der Möglichkeit der flexiblen Handhabung durch die Kommunikationsteilnehmer, zusätzliche Sicherheit schaffen könnte.

Der Schutz eines Informationssystemes ist nur bis zu einer gewissen Grenze möglich. Eigentliche Schwachstelle ist der Mensch. Kaum ein technisches Sicherheitssystem wird in der Lage sein, alle Risiken voll abzudecken. Insoweit ist neben dem Einsatz sicherer Leiter (z. B. Glasfaser) die automatische Authentifizierung und eine lückenlose Organisationskontrolle von besonderer Bedeutung. Sie verhindern dennoch nicht gänzlich unbefugte Eingriffe.

Nicht nur technische und Normungsaspekte werfen fundamentale Datenschutzfragen auf. Ich sehe insbesondere, daß das Individuum zum technischen Bestandteil — seine Daten zur abstrakten Bit-Kombination — von vernetzten Informationssystemen wird. Die Kontrolle und sein Einfluß werden immer mehr erschwert, wenn nicht sogar unmöglich gemacht. Sein Recht auf informationelle Selbstbestimmung wird dadurch beeinträchtigt. Es wird innerhalb der an und für sich schützenden — jedoch durch „vernetzte" Kontrolle verwundbar gemachten — Gesellschaft zu Verhaltensänderungen gezwungen, gegen die der einzelne sich nicht zu wehren vermag. Das zu verdeutlichen und letztlich zu verhindern, stellt sich mir in Zukunft als besondere Aufgabe.

2.3 Gentechnologie

In meinem 8. Jahresbericht habe ich mich unter Pkt. 2.4 bereits mit dem Thema Gentechnik, Reproduktionstechnik und informationelle Selbstbestimmung befaßt. Zwischenzeitlich liegt der Bericht der Enquete-Kommission „Chancen und Risiken der Gentechnologie" (BT-Drucksache 10/6775 vom 6. Januar 1987) vor. In diesem Bericht ist an mehreren Stellen auch das Recht auf informationelle Selbstbestimmung und deren datenschutzrechtliche Berücksichtigung bei der Humangenetik aufgegriffen worden. So stellt sich das Datenschutzproblem bei der pränatalen Diagnostik, dem Neugeborenenscreening, im Bereich der Pharmako- und Ökogenetik, der Genomanalyse bei Arbeitnehmern, bei Versicherungsnehmern und schließlich im Straf- und Zivilverfahren.

Genetische Beratung und pränatale Diagnostik

Datenschutzrechtlich geht es um die Wahrung des Rechts auf informationelle Selbstbestimmung des Kindes bei pränataler Datenerhebung. An wen dürfen diese Daten weitergegeben werden und können solche genetischen Daten für beliebige, auch verdeckte Motivationen verwendet werden?

Neugeborenen-Screening

Die beim Neugeborenen-Screening bekanntwerdenden genetischen Daten sind vor Mißbrauch zu schützen. In Frage kommen z. B. Erbkrankheiten, unbehandelbare Krankheiten etc. Informationen über solche genetischen Daten beeinflussen auch die Entscheidung von Eltern, so daß es also auch hier um ethische verantwortliche Verwendung der hierbei entstehenden Daten geht.

Pharmako- und Ökogenetik

In der Genomanalyse im Rahmen der Pharmakogenetik geht es z. B. darum, für den einzelnen Patienten ein geeignetes Medikament festzustellen. Die Ökogenetik könnte Chancen bei der Prävention von genetisch bedingten Unzuträglichkeitsreaktionen auf Umweltfaktoren bieten. Derartige Untersuchungen fördern Daten zu Tage, die durchaus Stigmatisierungswirkung von Trägern bestimmter genetischer Merkmale haben können.

Genomanalyse von Arbeitnehmern

Diese Möglichkeit wird gelegentlich in der Presse unter dem Aspekt der Zusammenstellung sogenannter olympiareifer Belegschaften erörtert. Die datenschutzrechtliche Problematik liegt darin, daß z. B. medizinische und genetische Daten von Arbeitnehmern bei Einstellungen, bei ärztlichen Untersuchungen etc. erhoben werden und dadurch Beschäftigungsbeschränkungen entstehen können, eine bestimmte präventivmedizinische Vorauswahl auftreten kann und schließlich keinerlei Beschränkungen des Fragerechts des Arbeitgebers bezüglich bestimmter Testverfahren vorhanden sind. Schließlich muß die Problematik gesehen werden, die entsteht, wenn genetische Daten und medizinische Daten z. B. in Personal-Informationssystemen oder in anderen Dateien des Arbeitgebers elektronisch gespeichert und verarbeitet werden dürften. Ob durch geeignete Maßnahmen sichergestellt werden kann, daß — wenn eine solche Genomanalyse an Arbeitnehmern in eng begrenzten und definierten Ausnahmesituationen überhaupt zugelassen werden soll — dies durch ein förmliches Zulassungsverfahren mit strenger Überprüfung und Transparenz geschehen kann, ist zu bezweifeln. Auf jeden Fall muß gesetzlich verboten werden, daß Arbeitgeber Atteste über bestehende oder nicht-bestehende genetische Dispositionen fordern.

Genomanalyse für Versicherungen

Auch hier stellt sich das Problem, inwieweit Versicherungsnehmer genetische Dispositionen für die fernere Zukunft der Versicherungsgesellschaft mitzuteilen haben, um so Risikodifferenzierungen durch die Versicherung zu ermöglichen.

Genomanalyse im Strafverfahren

Gerade im Strafverfahren zeigt sich die Schwierigkeit der Genomanalyse besonders deutlich, bei der es um die Feststellung genetisch bedingter Eigenschaften des Menschen und die Verwendung von Erkenntnissen hierüber geht. Unter dem Aspekt, ob es Schuld oder biologische Anlage eines Täters ist, entsteht die Frage, inwieweit z. B. im Rahmen einer Gentherapie Straftäter resozialisiert werden können, um so genetisch bedingte Persönlichkeitsmerkmale als verborgene Krankheit zu heilen. Bei solchen Untersuchungen und Entscheidungen fallen genetische Daten an. Darüber hinaus werden Einzeldaten und biologische Einmaligkeiten mit der Erstellung des „genetischen Fingerabdrucks" erhoben. Die Enquete-Kommission hat die Frage aufgeworfen, inwieweit bei der anstehenden Novellierung des Strafverfahrensrechtes und bei der Diskussion um das Polizeirecht des Bundes und der Länder diese besondere Problematik der Erhebung, Verwertung und Speicherung genetischer Analysen bei der Strafverfolgung und bei der polizeilichen Prävention gesetzlich geregelt werden müssen.

Gentechnische Eingriffe in das Erbgut menschlicher Zellen

Während der gentechnische Eingriff in die Keimbahn des Menschen strafrechtlich verboten werden soll, ist bei der somatischen Gentherapie unter datenschutzrechtlichem Aspekt insbesondere der Schutz der Vertraulichkeit bei der Durchführung des Therapieversuches zu garantieren.

Die Enquete-Kommission hat in ihrem Bericht an mehreren Stellen die Konferenz der Datenschutzbeauftragten des Bundes und der Länder gebeten, sich diesen oben skizzierten Fragestellungen zuzuwenden.

Die Konferenz hat auf meine Anregung hin eine Arbeitsgruppe eingesetzt, die sich diesen Fragen widmet. Bei der Erörterung dieser Fragestellungen handelt es sich um neuartige und schwierige Themen, die grundlegender Diskussion und wissenschaftlicher Durchdringung bedürfen, so daß die Arbeit an diesem Arbeitskreis eine gewisse Dauer in Anspruch nehmen wird. Ich werde in Abständen hierüber berichten.

2.4 AIDS

2.4.1 Grundsätzliche Betrachtung

Die Immunschwächekrankheit AIDS ist gegenwärtig eines der Hauptthemen in der öffentlichen Diskussion. Die Krankheit breitet sich inzwischen auch außerhalb sogenannter Risikogruppen aus. Durch die unterschiedlichen Berichte in den Medien besteht in der Bevölkerung Unsicherheit und wegen der nicht zu beschönigenden Gefährlichkeit auch Angst gegenüber dieser Krankheit. So wurde zuletzt in den Medien über die Ergebnisse zweier amerikanischer Wissenschaftler berichtet, die

in ihrer Studie zu dem Ergebnis kamen, daß inzwischen über 3 Millionen Amerikaner infiziert seien. Sie haben auch diverse Lösungen für die Bewältigung des Problems parat, wie großflächige Zwangstests z. B. für Schwangere, Heiratswillige und alle Krankenhauspatienten im Alter zwischen 15 und 60 Jahren. Künftige Sexualpartner sollten sich zunächst testen lassen und dann dem getesteten Partner treu bleiben. Dies schürt Ängste und Mißtrauen im privaten Bereich, was sich darin zeigt, daß sich Intimpartner gegenseitig mißtrauen und jeweils den anderen verdächtigen, mit dem AIDS-Virus infiziert zu sein. Diese Ängste auf individueller Ebene schaffen gesamtgesellschaftlich ein Mißtrauen gegen Angehörige bestimmter Gruppen und mündet schließlich in politische Forderungen, die nur eine gesellschaftliche Ausgrenzung und Abschottung dieser Gruppen von der übrigen Gesellschaft zur Folge haben können. Bezeichnenderweise geben die beiden amerikanischen Forscher auch keine Hinweise darauf, was mit den Infizierten geschehen soll. Ich sehe daher meinen Bericht über AIDS auch als einen Beitrag zur Versachlichung der Diskussion und als Anregung zur kritischen Reflexion über bestimmte, noch in der Planung befindliche Maßnahmen, wie etwa der personenbezogenen Meldepflicht und von Reihenuntersuchungen.

Datenschutzrechtlicher Anknüpfungspunkt bei der Beurteilung von staatlichen Maßnahmen zur Bekämpfung von AIDS ist, ob die jeweilige Maßnahme geeignet ist zur Bekämpfung der Krankheit und ob sie außer Verhältnis zu dem angestrebten Erfolg steht. Diese Abwägung, die dem in der Verfassung verankerten Verhältnismäßigkeitsgrundsatz entspricht, hat einmal das Grundrecht der Nicht-Infizierten auf Leben und Gesundheit und auf der anderen Seite die Grundrechtsposition des Infizierten zu berücksichtigen. Für die Beurteilung sind Kenntnisse über das Krankheitsbild und die Erkennbarkeit der Krankheit sowie die Übertragungsmöglichkeiten erforderlich.

Antikörpertest und Krankheitsbild

AIDS steht als Abkürzung für „**A**cquired **I**mmune **D**eficiency **S**yndrome" und bedeutet erworbene Immun-Abwehrschwäche. Das AIDS verursachende HIV-Virus wird übertragen, wenn es aus dem Blut oder einer anderen Körperflüssigkeit eines Menschen über Verletzungen oder direkt in die Blutbahn eines anderen Menschen gelangt. Aus den bisher vorliegenden Untersuchungen wird geschlossen, daß das AIDS-Virus durch die verschiedenen Formen des ungeschützten Geschlechtsverkehrs, gemeinsame Benutzung von blutverunreinigten Injektionskanülen, HIV-positive Mütter auf ihre Kinder, vor, bei oder kurz nach der Geburt übertragen wird. Eine Infektion ist ferner möglich durch Bluttransfusionen, sofern nicht durch geeignete und vorgeschriebene Untersuchungen infizierte Spender ausgeschlossen werden. Bisher wurden als Risikogruppen angenommen:

Homo- und bisexuelle Männer mit (häufig) wechselnden Intimpartnern,

Drogenabhängige, die benutzte Spritzen untereinander weitergeben,

Sexualpartner dieser Gruppen,

Heterosexuelle mit häufig wechselnden Partnern beim Geschlechtsverkehr.

Ob eine Person mit dem AIDS-Virus infiziert ist, wird durch einen sogenannten Antikörper-Test festgestellt. AIDS wird durch ein Virus verursacht, das seit 1986 international HIV (Human Immunodeficiency Virus) genannt wird. Es gibt bislang kein Verfahren, das dies Virus unmittelbar nachweisen kann. Jedoch bildet das menschliche Immunsystem als Reaktion auf eine Infektion sogenannte Antikörper, die den Erreger identifizieren. Wenn im folgenden von AIDS-Tests die Rede sein wird, so handelt es sich um die HIV-Antikörper-Tests, die bei positiven Ergebnis insoweit aussagefähig sind, daß die getestete Person AIDS-Virusträger ist. Der Nachweis HIV-spezifischer Antikörper ist der einzige Hinweis auf einen Virusbefall. Diese Tests werden in der Praxis hauptsächlich mit Hilfe des ELISA- und des Western-blot-Verfahrens durchgeführt.

Die Infektion führt mit einer gewissen Latenzzeit von bis über 10 Jahre zur Erkrankung (Vollbild von AIDS). AIDS unterscheidet sich von anderen Krankheiten dadurch, daß sie mit Sicherheit einen tödlichen Ausgang hat. Die Dauer von der Infektion über den Ausbruch bis hin zum Tod ist nicht bekannt. Es existiert bislang kein Heilmittel, das die AIDS-Viren aus dem Organismus des Infizierten wieder vertreibt. Daher können staatliche Maßnahmen nur darauf gerichtet sein, eine weitere Verbreitung der Infektion und Krankheit zu verhindern bzw. einzudämmen.

Im übrigen bestehen in der Wissenschaft noch erhebliche Unsicherheiten über die tatsächliche Ausbreitung des AIDS-Virus in der Bevölkerung, was darin begründet

ist, daß die Krankheit meist erst Jahre nach der Infektion ausbricht. Z. B. liegen in der Bundesrepublik noch keine epidemiologischen Daten vor. Die Erkrankung befindet sich vermutlich z. Z., wie oben schon angesprochen, in dem Prozeß des Übergreifens von den primären Gruppen (Risikogruppen) auf andere Bevölkerungsgruppen. Auch hier liegen keine Daten zur quantitativen Schätzung dieses Prozesses vor. Es wird die Mutationsfähigkeit des AIDS-Virus angenommen. Über die Häufigkeit der Mutation bestehen keine exakten Erkenntnisse.

Datenverarbeitung und AIDS

Die bisher umfangreich geführte Diskussion zu den mit AIDS verbundenen Fragestellungen hat gezeigt, daß damit auch Datenverarbeitungsvorgänge verbunden sind. Das Recht auf informationelle Selbstbestimmung schützt den Einzelnen auch vor einer unzulässigen Erhebung von Informationen. Daher ist der AIDS-Test für den Datenschutz der erste Anknüpfungspunkt und setzt bei der Frage an, wer überhaupt getestet werden soll. Dazu zähle ich auch diejenigen AIDS-Tests, von deren Durchführung eine staatliche Leistung oder die Einnahme einer Rechtsposition (AIDS-Tests bei Beamtenanwärtern) abhängig gemacht wird. Daran schließt sich an die Frage, ob der Arzt Angehörige und Sexualpartner des Getesteten informieren darf, unter Umständen auch gegen den Willen des Patienten. Sollen über diesen Personenkreis hinaus auch Behörden, Versicherungen etc. informiert werden von einem positiven Testergebnis? Wann darf das positive Testergebnis auf einem Datenträger festgehalten werden? Sollen Zwangstests, Reihenuntersuchungen durchgeführt oder eine Meldepflicht eingeführt werden? Es reicht nicht aus, daß nur aufgrund von Vermutungen oder Hörensagen der Betroffene als AIDS-Infizierter in einer Datei gespeichert wird, sondern es ist allgemein erforderlich, soweit daneben die anderen Voraussetzungen für eine Speicherung erfüllt sind, daß das positive Ergebnis aufgrund eines ärztlichen Befundes feststeht.

Datenschutzrechtlich sind mit AIDS daher die Erhebung, Speicherung und Übermittlung von Informationen angesprochen. Darüber hinaus ist für die Frage der Übermittlung die Einhaltung der ärztlichen Schweigepflicht nach § 203 StGB bedeutsam.

Meldepflicht, Zwangstest und Reihenuntersuchungen

Es stellt sich die Frage, ob Zwangstests für ganze Bevölkerungsgruppen oder Reihenuntersuchungen eingeführt werden dürfen. Hierbei ist zu prüfen, ob die beabsichtigte Maßnahme geeignet ist, Übertragungswege zu unterbinden. Erhebung und Speicherung von positiven Testergebnissen vermag dieses Ziel nicht zu erreichen. Abzuklären ist, bevor über solche Maßnahmen entschieden werden soll, welche Folgemaßnahmen möglicherweise getroffen werden sollen. Hierzu gibt es aber bislang keine eindeutigen Aussagen. Ich gebe dabei zu bedenken, daß sich die Verbreitung von AIDS hauptsächlich durch den Intimverkehr vollzieht und die Folgemaßnahmen, wenn sie wirksam sein sollen, einen tiefen Eingriff in die Intimsphäre der Betroffenen und damit auch in die Persönlichkeitsrechte der Infizierten darstellen würden.

Abgesehen davon, ob solche Maßnahmen überhaupt politisch durchsetzbar wären, wird mit einer Meldepflicht und Einführung von Reihenuntersuchungen die Grundlage für eine umfassende Überwachung der Betroffenen geschaffen. An dieser Stelle ist gerade der Datenschutz gefordert. Hier geht es auch nicht mehr nur um die Wahrung der einzelnen Rechte der Betroffenen, sondern man muß sich an dieser Stelle auch überlegen, daß ein großer Teil der verfassungsrechtlichen Werte von Freiheit und Demokratie aufgegeben würde, wenn der Weg mit Einführung einer Meldepflicht oder Reihenuntersuchungen beschritten werden sollte.

Es besteht kein gesetzlicher Handlungsbedarf. Ich teile die Auffassung des Bundesverfassungsgerichts, welches im Beschluß vom 28. 07. 1987 (Az.: 1 BvR 842/87) ausgeführt hat, daß es keine wirklich überzeugenden und zwingenden Gründe gibt, die schon jetzt für die Einführung einer allgemeinen Meldepflicht der Krankheit oder von Reihenuntersuchungen der Gesamtbevölkerung sprechen. Hier wird vielmehr das Trugbild einer Patentlösung vermittelt, wodurch eine falsche Beruhigung erzeugt und letztlich die gesamte Aufklärung und der notwendige Selbstschutz der Bürger unterlaufen würde. Denn dann würde das Vertrauensverhältnis zwischen Arzt und Patient enorm leiden, und AIDS-Verdächtige würden sich keinem Test unterziehen aus Angst vor weiteren Maßnahmen. Sie würden wahrscheinlich dann lieber mit der Ungewißheit leben wollen, was aber als die größte epidemiologische Bedrohung anzusehen ist. Darum vertreten auch nahezu alle AIDS-Exper-

ten die Auffassung, daß eine strenge Anonymisierung im Umgang mit AIDS-Kranken oder HIV-Infizierten eine unabdingbare Voraussetzung für eine erfolgreiche präventive Arbeit ist.

Auch Reihenuntersuchungen bilden nicht die Lösung des Problems. Wem heute bescheinigt wird, daß er keine Antikörper in sich trage, kann morgen schon infiziert sein. Insofern wird hier für den einzelnen aber auch für die Gesellschaft eine Scheinsicherheit erzeugt. Reihenuntersuchungen sind nur dann praktikabel, wenn sich daran Impfungen oder dergleichen anschließen könnten. Ein Serum gegen AIDS konnte aber noch nicht entwickelt werden.

Was jetzt gefordert ist, ist der rationale Umgang mit dieser nicht zu verharmlosenden Gefahr durch AIDS und ein Maß an Vertrauen in die Selbstverantwortung des Einzelnen. Ich bin auch der Meinung, daß Infizierte und Kranke, die unverantwortlich handeln, mit staatlichen Maßnahmen rechnen müssen, die heute schon möglich sind. Ich warne aber davor, Wege zu beschreiten, die irreparable Schäden sowohl für den Einzelnen als auch für die Gesellschaft nach sich ziehen.

2.4.2 AIDS-Test bei Beschäftigten des öffentlichen Dienstes

Die Senatskommission für das Personalwesen hat mich gebeten, zu einem vom Bundesminster des Inneren zugesandten Fragenkatalog Stellung zu nehmen. Der Fragenkatalog läßt erkennen, daß der Bundesminister des Innern sich ernsthaft und eingehend mit der Frage befaßt, ob und in welchem Umfang bei Bewerbern und Beschäftigten des öffentlichen Dienstes künftig AIDS-Tests durchgeführt werden sollen. Inhalt und Umfang dieses Fragenkataloges lassen vermuten, daß beim Bundesminister des Innern eine Tendenz für eine umfangreiche Überwachung der im öffentlichen Dienst Beschäftigten auf AIDS-Erkrankungen gegeben ist.

In meiner Stellungnahme bin ich zu dem Ergebnis gekommen, daß nach meinem bisherigen Erkenntnisstand erheblich bezweifelt werden muß, ob die Durchführung von AIDS-Tests sowohl für in den öffentlichen Dienst Einzustellende als auch im Laufe der weiteren Beschäftigung öffentlich Bediensteter datenschutzrechtlich zulässig und opportun ist. Es bleibt zu bemerken, daß es sich hier nur um eine erste globale Stellungnahme handeln kann, da für die Lösung der sich aus der Materie ergebenden spezifischen Schwierigkeiten weder der vorhandene Zeitrahmen noch der Umfang der bisher vorliegenden Materialien ausreichen. Ich bin dabei von den bisher als gesichert anzusehenden Erkenntnissen hinsichtlich der Übertragungswege und des Krankheitsverlaufes ausgegangen.

Bei der datenschutzrechtlichen Beurteilung der möglichen Absicht, Beschäftigte des öffentlichen Dienstes im vorher dargelegten Umfange auf AIDS-Erkrankungen zu überwachen, geht es vornehmlich um die Erhebung und Speicherung der Daten beim Arzt, deren Übermittlung an die Personalstellen und deren weitere Nutzung. Nachfolgend beschränke ich mich im wesentlichen auf die Zulässigkeit der Erhebung der Daten.

Zulässigkeit ärztlicher Untersuchungen von Beschäftigten im öffentlichen Dienst

Im Recht des öffentlichen Dienstes gilt es bisher als unumstritten, daß der Arbeitgeber vor einer Einstellung verlangen kann, daß der Bewerber seine körperliche Eignung durch das Zeugnis eines vom Arbeitgeber bestimmten Arztes (Amtsarzt) nachweist. Eine ärztliche Untersuchung kann während der weiteren Dienstzeit wiederholt werden, so oft ein ausreichender Grund dafür gegeben ist. Sie muß sogar in regelmäßigen Abständen wiederholt werden, wenn es sich um Arbeitnehmer handelt, die besonderer Ansteckungsgefahr ausgesetzt oder in gesundheitsgefährdenden Betrieben beschäftigt sind. Diesem liegt zugrunde, daß der Arbeitgeber zum einen verpflichtet ist, im jeweiligen Amt nur Personen zu beschäftigen, die dafür körperlich geeignet sind. Zum anderen soll der Arbeitgeber durch laufende Kontrolle des Gesundheitszustandes der Beschäftigten in die Lage versetzt werden, seiner Fürsorgepflicht gegenüber den Beschäftigten oder gegenüber Bürgern, die mit Beschäftigten des öffentlichen Dienstes in Berührung kommen, gerecht zu werden. Rechtsgrundlagen für diese Auffassung sind für die Beamten das Beamtenrecht, für Angestellte und Arbeiter das allgemeine Arbeitsrecht und die für diesen Personenkreis abgeschlossenen Tarifverträge. Soweit der Schutz der Bürger angesprochen ist, ergibt sich ein solcher Anspruch aus der Verfassung.

Nachweis der körperlichen Eignung für die Einstellung von Beamten

Das Berufbeamtentum hat seine Grundlage in Art. 33 des Grundgesetzes. Nach Abs. 2 dieses Artikels hat jeder Deutsche nach seiner Eignung, Befähigung und

fachlichen Leistung gleichen Zugang zu jedem öffentlichen Amt. Dieser Grundsatz findet sich wieder in den entsprechenden Beamtengesetzen. Nach bisher einmütiger Rechtsauffassung umfaßt der Begriff „Eignung" auch die gesundheitliche Konstitution des Bewerbers für ein öffentliches Amt. Unter diesem Begriff werden nicht nur anlage- und entwicklungsbedingte Persönlichkeitsmerkmale (z. B. Begabung) sowie emotionale und intellektuelle Vorausetzungen der Persönlichkeit im allgemeinen, sondern auch physische und psychische Kräfte des Bewerbers verstanden. Das Kriterium körperliche Eignung soll dabei nicht abstrakt verstanden werden, sondern konkret auf das jeweilige Amt bezogen werden. Im Verlauf der Ausgestaltung des Beamtenrechts hat sich jedoch bei der Zielsetzung der Verwendung des Begriffs „Eignung" eine weitergehende Funktion herausgebildet. Die öffentlichen Arbeitgeber sollen danach nämlich davor geschützt werden, Personen in das Beamtenverhältnis, insbesondere auch in das Beamtenverhältnis auf Lebenszeit zu berufen, die aufgrund ihrer körperlichen Konstitution nicht die Gewähr dafür bieten, daß sie während der üblichen Dauer der Dienstzeit so gesund bleiben, daß sie das ihnen übertragene Amt ausfüllen können. Als für ein Beamtenverhältnis geeignet gelten deshalb nur Personen, die aufgrund der medizinischen Erkenntnisse am Tage der Untersuchung mit hinreichender Wahrscheinlichkeit Gewähr dafür bieten, daß sie das Pensionsalter erreichen.

Vereinfacht dargestellt wird der Begriff „Eignung" hier mit der Zielsetzung verwendet, daß der öffentliche Arbeitgeber davor geschützt werden soll, daß er Personen in das Beamtenverhältnis beruft, bei denen das amtsärztliche Gutachten vermuten läßt, daß sie ihren Dienst nicht lange ausüben können und somit dem öffentlichen Arbeitgeber durch langjährige Pensionszahlungen finanziell erheblich belasten.

Zulässigkeit des AIDS-Tests für die Feststellung der körperlichen Eignung für die Berufung in das Beamtenverhältnis

Folgt man der Auslegung des Begriffes „Eignung" im Sinne der letztgenannten Zielsetzung, nämlich den öffentlichen Arbeitgeber vor möglicher übermäßiger finanzieller Belastung bei der Berufung von Personen in das Beamtenverhältnis zu schützen, liegt es nahe, daraus den Schluß zu ziehen, daß ein AIDS-Test zulässig ist. Bei Beachtung der Beobachtungen des Krankheitsverlaufes bei AIDS-Infizierten, muß nämlich damit gerechnet werden, daß zumindest Laufbahnbeamte in aller Regel die übliche Dienstzeit nicht erreichen. Daraus folgt, daß bei der Berufung von AIDS-infizierten Personen in das Beamtenverhältnis durchaus für eine verhältnismäßig kurze Dienstzeit der Betroffenen erhebliche Folgeleistungen auf den öffentlichen Arbeitgeber in Form von Zahlungen an Unterhalt und Beihilfen zukommen können.

Eine solche Betrachtungsweise würde jedoch weder der verfassungskonformen Verwendung des Begriffs „Eignung" noch den rechtspolitischen Erwägungen im Zusammenhang mit der Notwendigkeit der Bewältigung des Phänomens AIDS als gesellschaftspolitisches Problem gerecht. Es mag späteren gründlichen Analysen vorbehalten bleiben, ob der vom Verfassungsgeber im Zusammenhang mit der Konstituierung des Bürgerrechts auf gleichen Zugang zu öffentlichen Ämtern geschaffene unbestimmte Rechtsbegriff „Eignung" überhaupt unter dem Gesichtspunkt der Abwehr möglicher finanzieller Leistungen des öffentlichen Arbeitgebers verwendet werden kann oder ob der den Einstellungsbehörden mit diesem Begriff eingeräumte Beurteilungsspielraum sich nicht vielmehr darauf beschränkt, für die Besetzung eines öffentlichen Amtes nur Personen auszuwählen, welche die für die Ausübung des jeweiligen Amtes erforderliche körperliche Konstitution besitzen.

Bei der Ausfüllung des Beurteilungsspielraumes ist nicht außer Acht zu lassen, daß die Bestimmungen des Art. 33 GG grundrechtsähnlichen Charakter haben und der Begriff „Eignung" nicht dem Gesetzesvorbehalt unterworfen ist. Es handelt sich um einen Positivbegriff, der unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes von anderen Verfassungsprinzipien durchbrochen werden kann. Als solche Prinzipien kommen für den vorliegenden Fall die Sozialstaatlichkeit und das Recht auf freie Entfaltung der Persönlichkeit infrage. Bei der Frage der Zulässigkeit von AIDS-Tests bei Bewerbern für den öffentlichen Dienst ist in diesem Zusammenhang zu prüfen, ob eine mögliche Zurückweisung von AIDS-Infizierten vor dem Hintergrund möglicher finanzieller Belastungen des öffentlichen Arbeitgebers, gemessen an den Folgen, die ein solches Handeln für die Betroffenen und die Gesellschaft hat, dem Grundsatz der Verhältnismäßigkeit gerecht würde.

Bei der Prüfung der Frage der Auswirkungen muß einbezogen werden, daß ein

AIDS-Test nicht mit letzter Sicherheit Auskunft darüber geben kann, ob der Betroffene sich im Untersuchungszeitpunkt bereits infiziert hat oder nicht. Bedeutsam ist dabei, daß es nach dem augenblicklichen Stand der Medizin keine Therapie zur Heilung der AIDS-Erkrankung gibt. Es muß nicht bewiesen werden, daß in den Fällen, in denen sich durch die Durchführung eines solchen Tests eine Infektion des Betroffenen ergibt, diese Tatsache der Umwelt nicht verborgen bleiben wird. Das bedeutet aber für den Betroffenen, daß ihm auch keine andere Beschäftigungsmöglichkeit für die Zeit, in der er noch nicht an AIDS erkrankt ist, verbleibt. Wegen der Art und Weise, wie heute über AIDS öffentlich diskutiert wird, muß davon ausgegangen werden, daß der Betroffene nicht nur im beruflichen Bereich, sondern im gesamten gesellschaftlichen Bereich isoliert wird und ihm somit jede Möglichkeit genommen wird, mit den schwierigen Problemen der AIDS-Infizierung fertig zu werden. Dem Betroffenen bliebe somit in dem genannten Zeitraum keinerlei Möglichkeit mehr, sich als Persönlichkeit in der Gesellschaft zu behaupten. Die aus einer solchen Situation der öffentlichen Hand letztendlich entstehenden Aufwendungen für den weiteren Lebenslauf der Betroffenen dürften um ein Erhebliches höher zu veranschlagen sein, als vorher genannte Aufwendungen, die sich aus einer kürzeren Dienstzeit eines Beamten ergeben würden.

Schon hieraus ergibt sich, daß bei einer Abwägung zwischen den Gütern des Betroffenen und der Absicht, der öffentlichen Hand als Arbeitgeber Kosten zu ersparen, eine Entscheidung zu Gunsten des AIDS-Tests das Gebot der Verhältnismäßigkeit bei der Ausfüllung des Beurteilungsspielraumes im Begriff „Eignung" überschreiten würde.

Wollte man den öffentlichen Arbeitgebern das Recht auf Durchführung von AIDS-Tests für eine Einstellung zugestehen, gibt es keine Begründung dafür, einen solchen Test auch Arbeitgebern im nicht-öffentlichen Bereich zu erlauben. Das aber würde bedeuten, daß die Gesellschaft eine Teilung in Infizierte und Nichtinfizierte hinnehmen müßte. Solche Verhältnisse wären gesellschaftlich nicht mehr zu beherrschen. Nur beispielhaft mag eine Folge solcher Verhältnisse genannt werden: Die Bekämpfung der Ausbreitung der Krankheit, die insbesondere bei Risikogruppen ansetzen muß, würde dadurch fast unmöglich gemacht, weil betroffene Menschen sich anstatt im Rahmen eines Klimas des Vertrauens den Beratungsstellen anzuvertrauen, in die Anonymität untertauchen und damit für die gesamte Gesellschaft ein weitaus größeres Risiko darstellen würden.

Letztlich mag ein Vergleich der Forderung nach AIDS-Tests für die Feststellung der Eignung für den öffentlichen Dienst mit der bisherigen Praxis ergeben, daß diese Forderung wohl mehr unkontrollierter Ratlosigkeit als tatsächlicher Notwendigkeit entspringt.

Bei den bis jetzt durchgeführten amtsärztlichen Untersuchungen zum Zweck der Feststellung der Eignung für den öffentlichen Dienst werden im wesentlichen die nachfolgenden Daten erhoben:

— chronischer Status

— neurologischer Status

— psychischer Status

— Urinstatus auf Feststellung von Eiweißgehalt

— bei bestimmten Berufsgruppen Polizei, Feuerwehr usw. auf den ergometrischen Status und den röntgenologischen Thoraxzustand

— Gleichzeitig erfogt eine ausschließlich visuelle Feststellung, ob ansteckende Krankheiten vorliegen.

Nicht untersucht werden dagegen Bewerber auf weitere ansteckende Erkrankungen, z. B. die Hepatitis, obwohl es sich bei ihr um eine weit mehr verbreitete Erkrankung handelt als bei AIDS. Es soll allerdings nicht verkannt werden, daß bei Hepatitis A und Hepatitis B die Folgen der Erkrankung andere sein mögen, weil sie weniger Tendenz zur Chronisierung aufzeigen und von daher als heilbar angesehen werden müssen; anders jedoch bei der Hepatitis Non A und Non B. Hier liegt die Kontaminationsmöglichkeit ähnlich wie bei der AIDS-Erkrankung. Sie hat überwiegend die Tendenz zur Chronisierung und damit ähnliche Folgen wie die AIDS-Erkrankung. Auch ist das Vorkommen dieser Erkrankung durchaus nicht als geringer zu bezeichnen als das bisherige AIDS-Vorkommen. Trotz allem ist bisher

keine Stimme laut geworden, wonach bei der Einstellung von Bewerbern für den öffentlichen Dienst eine entsprechende Untersuchung Voraussetzung sein sollte.

Zulässigkeit von AIDS-Tests zur Wahrung der Fürsorgepflicht durch den Dienstherrn

Im Hinblick auf die Möglichkeiten der Übertragung des AIDS-Virus gibt es keinen Grund, in den öffentlichen Dienst Einzustellende einem AIDS-Test zu unterziehen mit der Begründung, die bereits im öffentlichen Dienst Befindlichen vor Ansteckungsgefahren zu schützen, weil sich eine Infektionsgefahr eben nicht aus der gemeinsamen Tätigkeit in einer Dienststelle ergibt. Soweit sich für bestimmte Gruppen des öffentlichen Dienstes überhaupt eine besondere Infektionsgefahr ersehen läßt, geht diese im wesentlichen nicht von Beschäftigten aus, sondern von Gruppen, mit denen die Beschäftigten des öffentlichen Dienstes in Ausübung ihres Amtes in Kontakt kommen. Soweit es dem Dienstherrn im Rahmen seiner Fürsorgepflicht obliegt, die Beschäftigten vor Infektionen zu schützen, ist eine laufende Überwachung durch Vornahme eines AIDS-Tests dazu völlig ungeeignet. Das ergibt sich schon allein daraus, daß im Falle der Feststellung einer AIDS-Infektion keine Therapiemöglichkeiten zur Verfügung stehen.

Soweit gelegentlich die Meinung geäußert wird, daß die Fürsorgepflicht des Dienstherrn laufende AIDS-Tests gebietet, um dem betroffenen infizierten Beamten eine Möglichkeit zu geben zu beweisen, daß er sich die Erkrankung im Dienst zugezogen hat, bedarf es keiner näheren Erläuterung, daß damit ein Beweis, ob die Infektion während des Dienstes oder im privaten Lebensbereich erfolgt ist, nicht geführt werden kann, denn bei der Möglichkeit der Übertragung des AIDS-Virus wird in solchen Fällen zunächst davon ausgegangen werden müssen, daß die Infektion nicht während des Dienstes erfolgt ist. Bei den fehlenden Therapiemöglichkeiten und den Folgen für die Betroffenen (Ausgrenzung) würde die Fürsorgepflicht eher ins Gegenteil verkehrt. Die Fürsorgepflicht kann vom Dienstherrn für den vorliegenden Fall nur durch präventive Maßnahmen wie Aufklärung und Schaffung von Schutzvorkehrungen erfüllt werden.

Zulässigkeit von AIDS-Tests bei Angestellten und Arbeitern

Das für die Zulässigkeit von AIDS-Tests für Beamte Gesagte kann ohne weiteres auch auf die Zulässigkeit von Tests für Arbeiter und Angestellte angeführt werden. Das ergibt sich allein daraus, daß nach überwiegender Rechtsmeinung das in Art. 33 GG normierte Recht auf Zugang zu einem öffentlichen Amt ohne Rücksicht darauf gilt, ob dieses Amt im Beamtenverhältnis oder aufgrund eines Privatvertrages wahrgenommen werden soll. Dieser Grundsatz hat auch dazu geführt, daß das Tarifrecht für die im öffentlichen Dienst Beschäftigten weitgehend den beamtenrechtlichen Gegebenheiten angepaßt ist.

Zulässigkeit von AIDS-Tests für Bewerber des öffentlichen Dienstes zum Schutz der Bürger

Der dem Bürger zustehende Anspruch, im Kontakt mit Behörden oder seinen Bediensteten vor Infektionen geschützt zu werden, vermag im Hinblick auf die Möglichkeiten der Übertragung des AIDS-Virus eine laufende Überwachung der Beschäftigten des öffentlichen Dienstes auf AIDS-Infektion nicht zu begründen. Das gilt auch für bestimmte Gruppen wie z. B. Krankenhauspersonal. Die Durchführung laufender AIDS-Tests könnte einen solchen Schutz allein schon deshalb nicht gewährleisten, weil die Infektion eines Betroffenen erst nach Ablauf eines längeren Zeitraums, nämlich bis zur Bildung von Antikörpern festgestellt werden könnte. Der dem Bürger durchaus zuzuerkennende Schutz kann wirkungsvoll ausschließlich durch die Schaffung geeigneter Präventivmaßnahmen wirkungsvoll gestaltet werden.

Hier bleibt im übrigen darauf hinzuweisen, daß der Schutz des Bürgers gegen Infektionen durch staatliche Maßnahmen auch gegenüber nicht-öffentlichen Stellen gegeben ist. Gerade an dem Beispiel von Krankenhauspersonal mag verdeutlicht werden, welche Auswirkungen die Einführung von AIDS-Tests für öffentlich Beschäftigte auf unsere Gesellschaft haben muß. Wollte man z. B. die laufende Überwachung von Ärzten auf AIDS-Infektion durch AIDS-Tests zum Schutz des Bürgers durchführen, wäre es ohne Belang, ob er von einem beamteten Arzt in einem öffentlich-rechtlich organisierten Krankenhaus oder von einem Arzt in einem privatrechtlich organisierten Krankenhaus oder von einem niedergelassenen Arzt behandelt wird. Das Schutzbedürfnis bliebe gleich. Würde man aber nur die Ärzte öffentlich-rechtlich organisierter Krankenhäuser einer solchen Überwachung durch

AIDS-Tests unterziehen, wäre damit gleichzeitig eine Ungleichbehandlung innerhalb einer Berufsgruppe mit dem gleichen Gefahrenrisiko verbunden.

Ich habe die Senatskommission für das Personalwesen gebeten, sich entsprechend zu verwenden.

2.4.3 AIDS im Strafvollzug

Auch im Strafvollzug mit den besonderen Gegebenheiten einer Justizvollzugsanstalt und dem Umstand, daß die Inhaftierten zum Teil Angehörige sogenannter Risikogruppen sind, steht die Immunschwächekrankheit AIDS im Mittelpunkt der Diskussion.

Seit Mitte Januar 1986 ist in Bremen eine Dienstanweisung betreffend Maßnahmen zur Verhütung und Behandlung von AIDS im Justizvollzug in Kraft. Gemäß dieser Anweisung soll eine geeignete Aufklärung durchgeführt und auf die Möglichkeit einer individuellen Beratung hingewiesen werden.

Dem Gefangenen soll erklärt werden, daß sie sich auf Wunsch einem AIDS-Test unterziehen können; soweit bekannt, wird den Angehörigen von Risikogruppen die Teilnahme an einer solchen Blutuntersuchung empfohlen.

Die Durchführung des AIDS-Test bedarf — wie andere ärztliche Maßnahmen — der Zustimmung des betroffenen Gefangenen. Der Gefangene muß intensiv darüber informiert werden, d. h. er muß in die Lage versetzt werden, beurteilen zu können, welche Konsequenzen seine Einwilligung in einen Test haben könnte. Man muß ihn darüber unterrichten, wer im Falle einer Infektion mit dem AIDS-Virus oder dessen AIDS-Erkrankung üblicherweise innerhalb der Vollzugsanstalt davon erfährt. Der Anstaltsarzt hat die Entscheidung zu treffen, ob er seine Kenntnis anderen offenbaren darf. Dabei muß er immer prüfen, ob nicht auch ein anderer Weg zum gewünschten Ergebnis führen kann.

Grundsätzlich sind daher die Berufsordnung des Arztes und die Schweigepflicht gem. § 203 StGB zu beachten. Bei beamteten und angestellten Ärzten kommt zu der allgemeinen ärztlichen Schweigepflicht noch die sogenannte Amtsverschwiegenheit. Diese berührt andere Dimensionen als die ärztliche Schweigepflicht. Während Letztere vor allem die Funktion der Behörde und deren ungestörte Entscheidungsfindung schützen will, ist das von § 203 StGB zu schützende Rechtsgut der von Geheimhaltungswillen des Betroffenen getragene persönliche Lebens- und Geheimbereich, der gerade von Trägern solcher sozial bedeutsamen Berufe nicht verletzt werden soll, denen die Allgemeinheit besonderes Vertrauen entgegen bringt. Dieses Vertrauen bringt in der Regel ein Gefangener einem Anstaltsarzt entgegen.

Demnach ist ein Arzt ausdrücklich auch dann zur Verschwiegenheit verpflichtet, wenn er im amtlichen Auftrag, also als Amtsarzt im Auftrag der Vollzugsanstalt tätig wird.

Nach der Bremer Dienstanweisung hat der Anstaltsarzt den Anstaltsleiter oder seinen Vertreter in anonymisierter Form darüber zu unterrichten, wenn bei Gefangenen ein HIV-positiver Befund festgestellt wird. Der Anstaltsleiter hat die senatorische Behörde in anonymisierter Form zu unterrichten. Befundträger sind zur Nachtzeit grundsätzlich einzeln unterzubringen. Die gemeinschaftliche Unterbringung ist möglich, wenn die Mitgefangenen mit ausdrücklicher Einwilligung des Befundträgers informiert werden und damit einverstanden sind. Dieses Verfahren kann zur Folge haben, daß die geforderte anonymisierte Form durchbrochen wird.

Es besteht keine Rechtspflicht für den Anstaltsarzt, seine Kenntnisse über die HIV-infizierten oder AIDS-erkrankten Gefangenen personenbezogen gegenüber Dritten zu offenbaren.

Ob und inwieweit der Arzt seine Schweigepflicht durchbrechen kann, hat er eigenverantwortlich zu prüfen und zu entscheiden. Denn der Arzt allein macht sich auch persönlich strafbar, wenn seine Handlung nicht gerechtfertigt ist. Die Güterabwägung ist allein Sache des Arztes. Er könnte sich in einem Strafverfahren nicht darauf berufen, daß man von ihm die Offenbarung verlangt hat. Auch seine Dienstpflichten können ihn nicht entlasten, da er sowohl als Beamter als auch als Angestellter die volle persönliche Verantwortung für die Richtigkeit seiner dienstlichen Handlungen trägt.

Es stellt sich daher die Frage, ob der Arzt nach den Grundsätzen des rechtfertigenden Notstandes gem. § 34 StGB eine Infektion oder Erkrankung eines Gefangenen

Dritten, insbesondere den dort Bediensteten offenbaren kann oder muß. § 34 StGB ist nicht geeignet, als Rechtsgrundlage für regelmäßiges Handeln öffentlicher Stellen oder als Instrumentarium für Eingriffe in das informationelle Selbstbestimmungsrecht zu dienen, sondern ist individueller Rechtfertigungsgrund für das Handeln einzelner Personen.

Den betroffenen Gefangenen muß unbedingt vor der Untersuchung eröffnet werden, inwieweit der Arzt seine hierbei gemachten Feststellungen anderen mitzuteilen hat und mit wem er zusammenarbeitet.

Diese erforderliche umfassende Information der Gefangenen sollte möglichst schriftlich erfolgen, damit bei keinem Gefangenen Unklarheiten über die Bedeutung seiner Einwilligung entstehen können. Darüber hinaus sollte die Einwilligung schriftlich geschehen.

Die Bedenken hinsichtlich der schriftlichen Offenbarung sollten auch Eingang in die Dienstanweisung betreffend Maßnahmen zur Verhütung und Behandlung von AIDS im Justizvollzug finden.

Ich habe meinen Standpunkt dem Senator für Justiz mitgeteilt und ihn gebeten, die Dienstanweisung entsprechend zu ergänzen.

2.4.4 Speicherung von AIDS-Infizierten in polizeilichen Informationssystemen

Die Innenministerkonferenz (IMK) hatte sich auf ihrer Sitzung am 3. Oktober 1986 mit dem Problem befaßt, daß Polizeibeamte in Ausübung ihres Dienstes sich dem Risiko einer AIDS-Infizierung aussetzen könnten. Als eine Abwehrmaßnahme war beabsichtigt, Personen, die HIV-infiziert sind, in das polizeiliche Informationssystem INPOL einzuspeisen. Der Arbeitskreis II „Öffentliche Sicherheit und Ordnung" (AK II) wurde beauftragt, entsprechende Kriterien für eine Speicherung zu erarbeiten und der IMK zur Beschlußfassung vorzulegen. Der AK II hat sich auf Veranlassung der IMK mit Vertretern der Datenschutzbeauftragten des Bundes und der Länder in zwei Sitzungen über die Zulässigkeit und den Umfang von AIDS-Speicherungen aus datenschutzrechtlicher Sicht auseinandergesetzt.

Der AK II ging dabei davon aus, daß die Tatsache der AIDS-Infektion zentral in dem bundesweit verfügbaren Informationssystem INPOL gespeichert werden sollte. Dies hätte bedeutet, daß eine Vielzahl von Polizeibeamten in der ganzen Bundesrepublik zu jeder Zeit auf diese Daten hätten zugreifen können. Es bestand die Vorstellung, daß die irgendwann einmal der Polizei bekanntgewordene AIDS-Infektion eines Betroffenen unabhängig davon, ob er Straftäter oder einer Straftat verdächtig war, gespeichert werden sollte, damit z. B. auch der Verkehrspolizist sich bei Unfallopfern — nach Abfrage des Informationssystems — entsprechend verhalten könne. Dabei wollte man sich nicht nur auf amtsärztlich festgestellte Tatsachen verlassen, sondern neben Angaben des Betroffenen selbst auch Angaben Dritter, z. B. Angehörige, ausreichen lassen, um eine AIDS-Speicherung vorzunehmen.

Ich habe gegenüber den Vertretern des AK II die Auffassung vertreten, daß für eine derart weitgehende Speicherungspraxis eine Rechtsgrundlage fehlt. Bei einer solchen Speicherung handelt es sich um einen Eingriff in das informationelle Selbstbestimmungsrecht, das einer expliziten Rechtsgrundlage bedürfte. Die Überlegung eines Übergangsbonus greift nicht, weil es sich hier um das Auftreten eines neuen Virus und damit um einen neuen Sachverhalt handelt.

Ich halte die Speicherung von AIDS-Infizierten in polizeilichen Computern für nicht erforderlich. Zwar ist das Schutzbedürfnis der Polizei nicht zu bestreiten, wenn man bedenkt, daß Teile der Polizei eher mit entsprechenden Risikogruppen zu tun haben, doch muß man erkennen, daß die Polizei bei vielen Einsätzen gar nicht erst auf ihr Informationssystem zurückgreifen kann, sondern sofort handeln muß.

Angesichts der tatsächlichen Ausbreitung und der möglichen weiteren Übertragung in der Bevölkerung wäre die Polizei in der Lage, maximal ca. 5 % der AIDS-Infizierten zu erfassen. Dies bedeutet aber, daß der überwiegende Teil Infizierter nicht in polizeilichen Informationssystemen gespeichert wäre. Die Speicherung würde dem Polizisten eine trügerische Sicherheit geben, die ihn evtl. sogar dazu veranlassen würde, gesonderte Sicherheitsmaßnahmen nicht zu ergreifen. Der Polizist muß aber angehalten sein, in jeder Risiko-Situation entsprechende Sicherheitsmaßnahmen zu ergreifen, um eine AIDS-Infizierung auszuschließen. Es ist darauf zu drängen, daß diese Sicherungsmaßnahmen eingehalten werden, da die Speicherung im polizeilichen Informationssystem ohnehin keinen Schutz bieten würde.

FFD 12/163

Schließlich sind auch die für die Betroffenen mit der Speicherung verbundenen Probleme zu berücksichtigen. Dies gilt insbesondere, weil nicht nur Straftäter gespeichert werden sollen. Das Risiko eines Bekanntwerdens ist nicht auszuschließen. Auch Dritten könnten entsprechende Kenntnisse nicht vorenthalten bleiben etwa bei Grenz- und Kfz-Kontrollen, wenn weitere Insassen im Fahrzeug sind.

Bei der Abwägung ist auch die Stigmatisierung der Betroffenen mit Folgen wie Berufs- und Arbeitsplatzverlust, Wohnungsverlust und dem Verlust sozialer Kontakte zu berücksichtigen.

Ich habe deshalb die Auffassung vertreten, daß eine Speicherung von AIDS in polizeilichen Informationssystemen weder erforderlich noch geeignet ist, den Schutz der Polizeibeamten zu gewährleisten und erwarte, daß dieses Merkmal nicht gespeichert wird.

Die Datenschutzbeauftragten der Länder und des Bundes haben sich ausführlich mit diesem Thema beschäftigt und den in der Anlage 4 abgedruckten Beschluß gefaßt.

Auch der Innenausschuß des Deutschen Bundestages hat sich in seiner 10. Sitzung im September 1987 unter Tagesordnungspunkt 1 mit diesem Problem beschäftigt. Der Innensenator des Landes Bremen hat in diesem Zusammenhang zu Protokoll gegeben, daß es in Bremen eine Speicherung entsprechender Hinweise in landesinternen Datensystemen nicht geben wird. Bezüglich des bundeseinheitlichen INPOL-Systems will er sich im Rahmen der IMK mit dieser Frage abschließend befassen. Bis zu einer abschließenden Erörterung in der IMK werde er im Land Bremen keine Speicherungen veranlassen.

2.4.5 AIDS-Tests beim Bluttransfusionsdienst

Ich habe mich anläßlich eines Besuchs beim Bluttransfusionsdienst über die datenschutzgerechte Verfahrensweise des Blutspendeverfahrens insbesondere im Hinblick auf AIDS-Tests überzeugt.

Dazu erklärte der Leiter, daß AIDS-Tests seit dem 8. März 1985 durchgeführt werden und bei ca. 20 000 Spenden im Jahr bis zu diesem Zeitpunkt lediglich bei vier Spendern ein positives Testergebnis festgestellt werden konnte. In drei von diesen vier Fällen wurde das Ergebnis schon in den ersten beiden Monaten festgestellt. Ein weiterer Fall ereignete sich im Jahre 1986. In den ersten drei Fällen wurde mit den Betroffenen ein ärztliches Gespräch geführt.

Der Test wird nach dem ELISA-Verfahren durchgeführt. Bei positivem Ergebnis wird der Test wiederholt. Sollte sich auch hier ein positives Ergebnis einstellen, wird die Blutprobe nach München geschickt, um das Western-blot-Verfahren durchzuführen. Dieses Verfahren nimmt mehrere Wochen in Anspruch. Auf der Blutkonserve ist lediglich die Konservennummer angegeben. Eine Identifizierung ist nur im Zusammenhang mit der Spendernummer möglich. Diese Identifizierung kann nur vom Arzt beim Blutspendedienst in Bremen vorgenommen werden. Die Korrespondenz mit München wird nur von Ärzten geführt. Ist auch das Ergebnis nach dem Western-blot-Verfahren positiv, wird die Blutkonserve nicht zur Bluttransfusion freigegeben und vernichtet. In der Spenderkartei wird die Sperrung des Spenders für die Bluttransfusion vermerkt ohne Angabe des Grundes.

Das Verfahren ist so ausgestaltet, daß jeder Blutspender einen Informationsbogen über AIDS lesen muß. Auf einem Anamnesebogen, auf dessen Rückseite später die Laborbefunde eingetragen werden, hat der Spender diverse Angaben, z. B. zu vorherigen Krankheiten zu machen. Mit der Unterschrift auf diesem Bogen (Blutspendeschein) bestätigt der Spender, daß er den AIDS-Informationsbogen gelesen hat, und willigt darin ein, daß sein Blut auf HIV-Antikörper untersucht wird. Ich habe an der Erstellung des Informationsbogens und der Formulierung der Einwilligungsklausel mitgewirkt (vgl. hierzu den 8. Jahresbericht unter Pkt. 5.8.1.8.).

Der Blutspendeschein (BTD-1-3 2/87) ist bei jeder Spende auszufüllen. Zusammen mit der Blutkonserve gelangt der Blutspendeschein in das Labor. Dort wird die Transfusionseignung des Blutes festgestellt und neben anderen Untersuchungen auch der AIDS-Test durchgeführt. Auf dem Blutspendeschein wird die Konservennummer aufgeklebt, die einer fortlaufenden Nummerierung entspricht. Auch die Spendernummer wird auf diesem Schein vermerkt.

Nach dem Labortest wird der Blutspendeschein in der Blutspenderkartei abgelegt, die nach Spendernummern sortiert ist. Daneben gibt es noch eine Suchkartei, in der nur Name, Spendernummer und Adresse aufgeführt sind.

FFD 12/163

Nach der Ablage des Blutspendescheines in der Blutspenderkartei befindet sich am Blutbeutel nur noch die Konservennummer. Die Zuordnung der Konserve zum Spender ist dann nur noch mit Hilfe des Konservennachweisbuches, das nach Konservennummern geführt wird, in Verbindung mit der Blutspenderkartei möglich.

Aufgeführt in diesem Buch sind nur die Konservennummer, die Spendernummer, gewisse Labordaten und der endgültige Verbleib der Konserve. Welchem Patienten letztendlich das Blut übertragen wurde, ist aus den Eintragungen nicht ersichtlich, da nur die Stationen des Krankenhauses dort aufgeführt sind. Nur Neuspender, die noch keine Spendernummer haben, werden mit Namen dort aufgeführt.

Welcher Patient welche Blutkonserve erhalten hat, ist auch nur über dieses Konservennachweisbuch möglich in Verbindung mit den Konservenbegleitschein/ Transfusionsbericht zurückzuverfolgen. Diese Bogen werden monatlich sortiert nach der Auftragsnummer der einzelnen Stationen. Bei Rückfragen, in denen die Auftragsnummer bekanntgegeben wird, kann dann Konserve, Patient und Spender zusammengeführt werden, wenn man das Konservennachweisbuch und die Blutspenderkartei hinzuzieht. Dies ist aber nur in Einzelfällen möglich.

Ich habe gegen dieses Verfahren keine datenschutzrechtlichen Bedenken.

2.4.6 Meldung an zentrale Register

Im Berichtszeitraum hatte ich zwei Erhebungsbogen unter datenschutzrechtlichen Gesichtspunkten zu prüfen. Es handelt sich dabei um den freiwilligen „vertraulichen AIDS-Fallberichtsbogen" für die AIDS-Arbeitsgruppe des BGA und den „Erhebungsbogen für Viruserkrankungen" über HIV-Testuntersuchungen.

Die in den Erhebungsbogen aufgeführten Daten sollen in zentralen Registern erfaßt werden. Nach Aussage des BGA soll eine Verknüpfung der Register nicht stattfinden. Bislang ist die Meldung in anonymisierter Form vorgesehen. Meine Bedenken gegen eine namentliche Meldepflicht habe ich bereits unter Pkt. 2.4.1 dargelegt.

2.4.6.1 Vertraulicher AIDS-Fallbericht

Es handelt sich bei diesem Fallberichtsbogen um ein mehrfach überarbeitetes Formblatt für freiwillige Meldungen von AIDS-Erkrankungen durch behandelnde Ärzte an die AIDS-Arbeitsgruppe des BGA.

Da eine Einwilligung des Patienten nicht vorliegt und auch eine gesetzliche Grundlage nicht vorhanden ist, kommt nur eine Meldung in anonymisierter Form in Betracht.

Neben Geschlecht, Geburtsjahr, Staatsangehörigkeit enthält der Bogen den jeweils dritten Buchstaben des Vor- und Familiennamens und die Anzahl der Buchstaben sowie das Bundesland und die beiden ersten Ziffern der Postleitzahl als personenbezogene Daten.

Da nach Mitteilung der Bundespost der räumliche Bereich, der von den ersten beiden Ziffern der Postleitzahl abgedeckt wird, eine Bevölkerungszahl von 500 000 bis 1 000 000 Menschen abdeckt und ich davon ausgehe, daß eine Deanonymisierung ansonsten nur mit einem unverhältnismäßigen Aufwand erfolgen kann, habe ich dem Hauptgesundheitsamt mitgeteilt, daß dieser Bogen die datenschutzrechtlichen Anforderungen hinsichtlich der Anonymisierung erfüllt.

Ich stimme mit den übrigen Datenschutzkontrollbehörden darin überein, daß die aufgrund der Laborberichtsverordnung gespeicherten Datenbestände nicht mit den durch die AIDS-Fallberichtsbogen gewonnenen Datenbestände zusammengeführt bzw. abgeglichen werden dürfen.

2.4.6.2 Erhebungsbogen für Viruserkrankungen

Zu Beginn des Berichtszeitraumes wurde mir ein Erhebungsbogen über HIV-Testuntersuchungen vorgelegt. Bei dem Erhebungsbogen handelt es sich um ein Formular, welches die Deutsche Vereinigung zur Bekämpfung der Viruskrankheiten e.V. (DVV) als Grundlage für ein neues epidemiologisches Programm entworfen hat. Er wird an die Stellen, die AIDS-Tests durchführen (Labors, Hygiene-Institute etc.) versandt. Mitglieder der DVV sind sowohl die Bundesländer und der Bund, als auch zahlreiche Institutionen, die sich mit dem Gesundheitswesen beschäftigen. Die Auswertungen sollen vom BGA vorgenommen werden. Der Erhebungsbogen ist mehrfach überarbeitet worden, seine endgültige Fassung liegt mir nicht vor.

FFD 12/1 KB

Die Erhebung der Daten und Übermittlung an das zentrale Register, die zunächst auf freiwilliger Basis erfolgen sollte, ist nunmehr durch Rechtsverordnung (Laborberichtverordnung) vorgeschrieben. Die „Verordnung über die Berichtspflicht für positive HIV-Bestätigungstests" ist inzwischen unbefristet in Kraft getreten.
Zu dieser Verordnung wurde mir keine Gelegenheit zur Stellungnahme gegeben.

2.4.7 AIDS-Forschung

Die AIDS-Erkrankung hat bei Forschern verschiedener wissenschaftlicher Disziplinen das Interesse an Daten über Entstehungszusammenhänge, Art und Verlauf der Erkrankung, Übertragungswege bis in den sozialen und intimen Bereich geweckt. Insbesondere mit der Argumentation einer möglichen Kostenexplosion für die gesetzliche Krankenversicherung wird dargelegt, daß es auch hierfür sehr wichtig sei, das Dunkelfeld AIDS-Infizierter und -Erkrankter zu erforschen. Aus diesem Grunde wird seit einiger Zeit verstärkt an Forschungsvorhaben gearbeitet, um die fehlenden Grunddaten zu ermitteln. Diese Forschungsvorhaben nehmen für sich in Anspruch, nur in anonymisierter Form Daten zu verarbeiten.

Die Prüfung, ob die Daten anonym oder personenbeziehbar verarbeitet werden, setzt die Kenntnis der Verfahrensweise bei der Meldung sowie der weiteren Verwendung der Daten voraus. Daher reicht es nicht aus, wenn Forschungsträger lediglich die Erhebungsbögen mir zur Prüfung vorlegen, sondern es sind präzise Informationen darüber erforderlich, wie die weitere Datenverarbeitung erfolgen soll und wie die Dateien gegen den Zugriff Unbefugter gesichert werden. Insbesondere ist auch eine Verknüpfung bzw. Verknüpfbarkeit mit anderen Dateien auszuschließen, da hierbei das Risiko der Deanonymisierung eintritt.

Von aktuellem Interesse ist eine bundesweite multizentrische Studie zur Langzeitbetreuung HIV-infizierter und HIV-exponierter Kinder. Bestandteil der Studie sollen mütterliche Daten vor der Entbindung und bei der Geburt, neonatale und vierteljährliche Untersuchungs- und Labordaten des Kindes sein, die in überregionalen Studienzentren gesammelt werden sollen. Zwar ist in Bremen kein Studienzentrum vorgesehen, doch ist diese Studie auch für Bremen insoweit relevant, als diese Daten nur mit Einverständniserklärung der Mutter von den verschiedenen Gynäkologen oder Krankenhäusern an die Studienzentren übermittelt werden sollen und es sich um eine bundesweite Studie handelt. Daher ist davon auszugehen, daß auch die Daten von in Bremen lebenden Müttern und Kindern weitergegeben werden sollen.

In Übereinstimmung mit dem Bundesbeauftragten und den Landesbeauftragten anderer Länder kann ich den Anamnesebogen in der bisher vorliegenden Form nicht als anonym ansehen. Insbesondere ist entsprechend der oben dargelegten Grundsätze noch klärungsbedürftig, wer speichernde Stelle für welche Daten ist und wie der genaue Verfahrensablauf einschließlich aller Datenflüsse zwischen allen Beteiligten ausgestaltet werden soll. Auch fehlt noch ein konkretes Konzept zur Datensicherung bei allen beteiligten Stellen.

Bislang liegt auch keine den Anforderungen des Datenschutzes entsprechende Einwilligungserklärung vor.

3. Kooperationen

3.1 Koperation mit dem Datenschutzausschuß der Bremischen Bürgerschaft (Landtag)

Die Zusammenarbeit mit dem Datenschutzausschuß der Bremischen Bürgerschaft (Landtag) wurde über den Legislaturperiodenwechsel hinaus kontinuierlich fortgeführt.

Folgende Themen waren u. a. Beratungsgegenstand:

— Novelle des Bremischen Datenschutzgesetzes

— Datenschutz im Bildungsbereich

— Meldedatenübermittlungsverordnung

— 9. Jahresbericht des Landesbeauftragten

— Personalkonzept und Haushalt des Landesbeauftragten

— Sachstandsberichte zur Volkszählung

FFD 12/163

— Datenschutzprobleme bei AIDS

— Datenschutzkontrollen beim Verfassungsschutz

— Datenschutz im Krankenhausbereich

— Novellierung des Bundesdatenschutzgesetzes

— Sicherheitsgesetze des Bundes

— Novellierung der Strafprozeßordnung.

In der Bremischen Bürgerschaft (Landtag) waren im letzten Jahr u. a. folgende datenschutzrechtliche Fragen Gegenstand von Anfragen, Mitteilungen und Plenardiskussionen:

Gegenstand	Antrag- und Fragesteller, Mitteiler	Plenarsitzung	Fundstellen
Stellungnahme des Senats zum 8. Jahresbericht des LfD	Senat	28. 01. 1987	PlPr 11/69
Bericht/Antrag des DS-Ausschusses zum 8. Jahresbericht des LfD	DS-Ausschuß	28. 01. 1987	PlPr 11/69
Ausreichender Schutz der Volkszählungsdaten	CDU	25. 02. 1987	PlPr 11/71
Schulung der ADV-Mitarbeiter in Datensicherheit und Datenschutz	CDU	25. 02. 1987	PlPr 11/69
9. Jahresbericht des LfD	LfD	11. 05. 1987	PlPr 11/76 Drs. 11/915
Datenschutz in den Krankenhäusern	CDU	12. 05. 1987	Drs. 11/861 PlPr 11/77
Datenschutz in der Schule	CDU	12. 05. 1987	Drs. 11/861 PlPr 11/77
	Senat	24. 06. 1987	Drs. 11/976 PlPr 11/80
Gesetz zum Datenschutz im Schulwesen	Senat	24. 06. 1987	Dr. 11/976 PlPr 11/80
	Senat SPD GRUNE	02. 09. 1987	PlPr 11/82 Drs. 11/989 Drs. 11/992
Gesetz zur Änderung des Bremischen Datenschutzgesetzes	Senat	24. 06. 1987	PlPr 11/80
	Senat CDU GRUNE CDU SPD CDU	02. 09. 1987	PlPr 11/82 Drs. 11/972 Drs. 11/990 Drs. 11/994 Drs. 11/1012 Drs. 11/1020
Stellungnahme des Senats zum 9. Jahresbericht des LfD	Senat	02. 09. 1987	PlPr 11/76 Drs. 11/915
Kfz.-Steuerdaten / Aktenaufbewahrung	CDU SPD	11. 11. 1987	PlPr 12/3
Regierungserklärung / Datenschutz	Senat	12. 11. 1987	PlPr 12/4

3.2 Mitarbeit im ADV-Ausschuß (AADV) Bremen

Die Mitarbeit im ADV-Ausschuß war gekennzeichnet durch die datenschutzrechtliche Prüfung einer Vielzahl von Anträgen auf Verfahrenserweiterungen, Ergänzungsbeschaffungen und Geräteaustausch im Rahmen der Einführung automatisierter Texbe- und -verarbeitung und der damit verbundenen Hardware-Beschaffung, die fast ausschließlich auf PC-Basis erfolgte. Die Problematik des PC-Ein-

satzes, bedingt durch seine über genehmigte Verfahren hinausgehenden universellen Einsatzmöglichkeiten, ist von mir schon wiederholt in früheren Berichten vorgetragen worden (siehe auch Pkt. 5.1.2 dieses Berichtes).

Darüber hinaus waren datenschutzrechtliche Stellungnahmen u. a. zu folgenden Verfahren zu erstellen:

— Kfz-Steuer-Festsetzungsverfahren

— Moderne Informationstechnologien in kaufmännisichen und bautechnischen Ausbildungsgängen

— DV-Verfahren Lagern, Abfüllen und Umschlagen wassergefährdender Stoffe (Anlagenverordnung)

— Technikunterstützte Informationsverarbeitung in der bremischen Verwaltung

— ADV-Verfahren AUTISTA im Standesamtsbereich

— Automatisierte Ferngesprächsaufzeichnung

— ADV-Anwendungen im Bereich Feuerschutz, Rettungsdienst, Zivil- und Katastrophenschutz

— Automatisierung der Wahlhelferwerbung und des Wahlhelfereinsatzes

— Überführung der Schülerindividualdatei in ein Schülerverzeichnis

— Datenabfragen der Vollzugspolizei im Rahmen der Verfahren EDAS, ISA, INPOL, FAZID und ZEVIS.

Eine vorherige Beteiligung meiner Behörde, wie sie in den Richtlinien des Ausschusses für ADV (siehe Pkt. 2.1.4 dieses Berichtes) gefordert wird, erfolgte nicht in allen Fällen. Verbunden damit war oftmals ein zeitlicher Arbeitsdruck.

3.3 Kooperation mit den Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz

Folgende wesentliche Themen wurden von der Konferenz der Datenschutzbeauftragten behandelt:

— Bewertung der Datenschutzvorkehrungen bei Auswertung der Volkszählung

— Landesstatistikgesetze

— Änderung des Personenstandsgesetzes

— Justizmitteilungsgesetz

— Rückmeldung von der Justiz an die Polizei

— Neukonzeption des Ausländerzentralregisters

— Fahrzeugregisterverordnung

— Prüfungen im Bereich Staatsschutz

— Telekommunikationsordnung

— Automatisierung bei Dienstleistungen

— Gentechnologie

— Datenschutzrechtliche Probleme bei AIDS

Beschlußfassungen wurden teilweise in Presseerklärungen veröffentlicht. Zu Einzelpunkten verweise ich auf Abschnitt 5 dieses Berichtes.

3.4 Kooperation mit den Obersten Aufsichtsbehörden für den Datenschutz

Seit Inkrafttreten des Bundesdatenschutzgesetzes werden datenschutzrechtliche Probleme im Bereich der privaten Wirtschaft von den Obersten Aufsichtsbehörden der Länder im „Düsseldorfer Kreis" und in von ihm eingerichteten Arbeitsgruppen erörtert mit dem Ziel, eine möglichst einheitliche rechtliche Bewertung gleicher oder ähnlicher Sachverhalte sicherzustellen.

Beratungspunkte in 1987 waren u. a.:

— Einzelprobleme aus der Kreditwirtschaft

— Verhandlungen mit dem Zentralen Kreditausschuß, der Bundes-Schufa und dem Bundeskartellamt

— SCHABS-DATA, Datenkommunikation mit dem SCHUFA-Auskunfts- und Beobachtungssystem

— Identitätsprüfungen im Rahmen von SCHUFA-Nachmeldungen, Gefahr von Personenverwechslungen

— Anforderungen zur Identitätsfeststellung bei SCHUFA-Selbstauskünften

— Anschluß von Möbelspeditionen an das SCHUFA-Kreditinformationssystem

— Anschluß von Inkassobüros an das SCHUFA-Kreditinformationssystem

— Meldepflichten nach § 39 Abs. 1 BDSG (Zweigniederlassung/unselbständige Zweigstellen) und Prüfungskompetenz der Aufsichtsbehörden

— Versandhandel, z. B. Verzeichnis von Notunterkünften

— Arbeitnehmerdatenschutz

— Versicherungswirtschaft, z. B. Einwilligungsklauseln, Übermittlung von Versicherungsdaten an Dritte

— Btx-Staatsvertrag, geschlossene Teilnehmergruppen

— Wohnungswirtschaft, Speicherung von Mieterdaten durch eine Vermieterauskunftei, Datenerhebung bei Mietgesuchen

— Gesundheitswesen, Weitergabe von Patientendaten an privatärztliche Verrechnungsstellen und an freie Rechenzentren

— Werbewirtschaft, Nutzung des Schuldnerverzeichnisses zu Werbezwecken.

Nähere Ausführungen zu einzelnen Beratungen siehe unter Pkt. 6 dieses Berichtes.

3.5 Kooperation mit Kammern, regionalen und überregionalen Verbänden und Institutionen

Bereits bestehende Kontakte zu Vertretern aus Wissenchaft und Forschung, Gesetzgebung und datenverarbeitender Wirtschaft und Verwaltung wurden im Berichtszeitraum fortgesetzt und vertieft.

Im Berichstzeitraum war eine umfangreiche Ausweitung der Informations- und Vortragstätigkeit festzustellen. Den vielfältigen Anforderungen an Beratungs-, Vortrags- und Bildungstätigkeiten konnte ich leider nicht immer entsprechen. Ich halte gerade diese Art der Tätigkeit insbesondere unter dem Gesichtspunkt des gegenseitigen Erfahrungsaustausches für auf Dauer unverzichtbar.

Die hieraus resultierende hohe Arbeitsbelastung für meine Dienststelle konnte teilweise nur durch den Einsatz von ABM-Kräften aufgefangen werden.

4. Beschwerden, Registerführung, Geräteverzeichnis

4.1 Beschwerden

Die Anzahl der Eingaben und Beschwerden hat sich 1987 erheblich erhöht. Allein die Zahl der ausführlich schriftlich beantworteten Vorgänge hat sich von 1986 = 125 auf 1987 = 175 gesteigert. Davon betrafen 72 den nicht-öffentlichen Bereich und 103 den öffentlichen Bereich. Insgesamt wandten sich rund 350 Bürgerinnen und Bürger schriftlich an mich. Wie auch in den vorherigen Jahresberichten dargestellt, sind Fälle, die den gleichen Beschwerdegrund (z. B. Volkszählung, Verfassungsschutz, Kammerwahlen, Telefon- und Mitgliederverzeichnisse) beinhalten, nur einfach gezählt, wobei bei einzelnen Sachverhalten bis zu über 40 Beschwerden eingegangen sind.

Darüber hinaus erreichten mich eine Vielzahl mündlicher und telefonischer Anfragen, Hinweise oder Beratungsersuchen mit unterschiedlichem Bearbeitungsaufwand.

Die häufigsten Anfragen und Beschwerden im nicht-öffentlichen Bereich betrafen wie in den Vorjahren Auskunfteien, Adreßhandel, Banken, Versicherungen, Inkassodienste und zunehmend Fragen des Arbeitnehmerdatenschutzes.

4.2 Register der meldepflichtigen Stellen nach dem BDSG

Die Anzahl der Eintragungen zum Register gemäß § 39 BDSG hat sich 1987 gegenüber dem Vorjahr leicht erhöht. Nach regionalen und sachlichen Gesichtspunkten ergibt sich folgende Übersicht:

Art der Tätigkeit	insgesamt	Bremen	Bremerhaven
1. Kredit- und Handelsauskunfteien	7	4	3
2. Markt- und Meinungsforschungsinstitute	2	2	—
3. Adreßhandel	3	2	1
4. Datenverarbeitung im Auftrag davon:	101	90	11
— Datenerfassung	16	16	—
— Service-Rechenzentrum	39	36	3
— DV für verbundene Betriebe	25	22	3
— DV für sonstige Dritte	19	14	5
— Datenlöschung und -vernichtung	2	2	—
	113	98	15

Neben den statistisch nicht ausgewerteten Änderungen einzelner Eintragungen (z. B. Geschäftsführerwechsel, Standortwechsel, Wechsel des EDV-Leiters, Wechsel des betrieblichen Datenschutzbeauftragten usw.) gab es allein gegenüber dem letzten Berichtszeitraum 25 Löschungen und 29 Neueintragungen.

Alle diese Eintragungsvorgänge sind mit detaillierten Prüfungen der Meldepflicht verbunden, die sich erst nach Bewertung der gesellschaftsrechtlichen- und technischen Organisationsform ergibt.

Leider wendet sich in den wenigsten Fällen die meldepflichtige Stelle an meine Dienststelle; vielmehr muß ich nach Auswertung von Handelsregistereintragungen, Werbeanzeigen, Pressemitteilungen und dgl. die einzelnen Firmen zur Überprüfung ihrer Meldepflicht auffordern.

4.3 Dateienregister nach dem BrDSG

Die Anzahl der zum Dateienregister gemeldeten Dateien hat sich im Berichtszeitraum von 1496 auf 1512 logische Dateien erhöht.

Das Register ist von einzelnen Betroffenen nur in sehr wenigen Fällen eingesehen worden. Seine eigentliche Bedeutung hat es jedoch als Arbeitsgrundlage zur Überwachung des Datenschutzes im öffentlichen Bereich, da es die einzige Zusammenstellung sämtlicher im öffentlichen Bereich verarbeiteten personenbezogenen Daten unter Hinweis auf betroffenen Personenkreis, Art der Daten, verarbeitende Behörden, Rechtsgrundlage für die Verarbeitung und Übermittlung an andere Stellen darstellt.

Mit der Novellierung des BrDSG wurde die Veröffentlichungspflicht der speichernden Stellen im Amtsblatt abgeschafft. Dafür wurde mir die Aufgabe übertragen, eine geeignete Übersicht über den Inhalt des Registers zu veröffentlichen (§ 28 BrDSG). Hierfür ist es erforderlich, das bisherige Verfahren grundlegend zu ändern. Zur Zeit erarbeite ich ein Konzept für die notwendige Umstellung.

4.4 Dateibeschreibung und Geräteverzeichnis (öffentlicher Bereich)

Um die automatisierte Datenverarbeitung transparenter zu gestalten, sieht die Neufassung des Bremischen Datenschutzgesetzes neben dem von mir zu führenden Dateienregister das Erstellen und die laufende Fortschreibung von Dateibeschreibungen und Geräteverzeichnissen durch die speichernden Stellen vor (§ 7 BrDSG). Die Dateibeschreibung entspricht im wesentlichen dem Dateienregister, ergänzt um Angaben von Fristen für Sperren und Löschen der Daten, getroffene organisatorische Maßnahmen nach § 6 BrDSG sowie Angaben über Betriebsart des Verfahrens, eingesetzte Geräte und Verfahrensvorschriften bei Übermittlung, Sperrung, Löschung und Auskunftserteilung.

Für manuell geführte Dateien, deren Daten nicht zur Übermittlung bestimmt sind, entfällt die Dateibeschreibung.

Dateiunabhängig ist für alle Geräte einer datenverarbeitenden Stelle, mit denen personenbezogene Daten verarbeitet werden, ein Geräteverzeichnis anzulegen (§ 7 Abs. 2 BrDSG). Dieses Verzeichnis umfaßt die Angaben

— Typ und Art der Geräte

— Hersteller

— Anzahl und Standort der Geräte

— verwendetes Betriebssystem

— Möglichkeiten zur Datenfernverarbeitung und Datenübertragung

— verwendete Standard- und Anwenderprogramme.

Die Aufnahme weiterer Angaben über die Ausstattung der Geräte ist noch in einer Rechtsverordnung festzulegen. Die Verordnung ist unter meiner Beteiligung zu erarbeiten.

Ich rege an, das Geräteverzeichnis in einem automatisierten Verfahren so zu führen, daß es zu datenschutzrechtlichen Kontrollzwecken von mir ebenfalls genutzt werden kann.

5. Öffentlicher Bereich

5.1 Senat

5.1.1 Integrierte Bürokommunikation

Wie mir inzwischen bekannt wurde, hat der Senat im April und Dezember 1986 die Einführung technik-unterstützter Informationsverarbeitung für die bremische Verwaltung beschlossen. In diesen Beschlüssen geht der Senat von einer schrittweisen dezentral bestimmten Einführung der Bürotechnik aus. Außerdem sollte ein Erfahrungsbericht von Pilotanwendern bis zum 31. September 1987 vorgelegt werden.

Die Senatskommission für das Personalwesen wurde damit beauftragt, über das Rechenzentrum der bremischen Verwaltung (RbV) eine Ausschreibung für einzusetzende PC zu veranlassen. Diese Ausschreibung sollte nach Test-Installationen eine Systemauswahl nach sich ziehen und letztlich eine Systementscheidung für ein bestimmtes PC-System bringen.

Des weiteren sollten die Ressorts zu Fragen der Rationalisierung bei Einsatz arbeitsplatzbezogener Automatisierung Stellung nehmen.

Ich wurde weder an der Systemauswahl beteiligt noch hatte ich Gelegenheit, meinerseits Stellung zu nehmen. Datenschutzaspekte bei der Einführung neuer Technologien haben in den Vorüberlegungen wohl offensichtlich keine Rolle gespielt. Ich weise dazu darauf hin, daß gemäß § 27 Abs. 4 BrDSG

> „der Landesbeauftragte für den Datenschutz zu den Auswirkungen des Einsatzes neuer Informationstechniken auf den Datenschutz Stellung nehmen soll. Er ist über Planungen zum Aufbau automatisierter Informationssysteme rechtzeitig zu unterrichten, sofern in den Systemen personenbezogene Daten bearbeitet werden sollen."

Diese vom Gesetzgeber vorgeschriebene frühzeitige Beteiligung ist bisher unterblieben (vgl. bereits meine Vorbemerkungen im 9. Jahresbericht unter Pkt. 1.1). Ich verweise in diesem Zusammenhang auch auf meinen 9. Jahresbericht unter Pkt. 2.2.1, in dem die Risiken beim Einsatz von PC als Datenstationen bzw. des willkürlichen und unkontrollierten Datenaustausches bei der Vernetzung unterschiedlicher Verwaltungsaufgaben aufgezeigt werden. Es reicht nicht aus, das Bremische Datenschutzgesetz erst dann anzuwenden, wenn konkrete Maßnahmen in einzelnen Ressorts geplant und eingeführt werden. Die vorgesehene umfangreiche Verwaltungsautomation wirft derartig grundsätzliche Datenschutzfragen auf, daß meine Beteiligung vor der Entscheidungsfindung durch den Senat unverzichtbar ist; dies insbesondere auch deshalb, weil inzwischen eine umfangreiche selbständige Systemversorgung der Ressorts erfolgt, ohne den Systementscheid und ein mögliches Einführungskonzept abzuwarten.

Bei diesen Anwendungen handelt es sich in den meisten Fällen um „Insellösungen", an deren Entwicklung ich teilweise frühzeitig vor den ADV-Anträgen beteiligt

bzw. zu deren Konzeption ich um Stellungnahme gebeten wurde. Ressortinterne Verbindungen oder sogar ressortübergreifende Schnittstellen waren jeweils bei der Ersteinführung oder beim Systemaustausch nicht erkennbar. Inwieweit zum späteren Zeitpunkt solche Verbindungen geschaffen werden, läßt sich kaum überwachen und kontrollieren, solange nicht ein Gesamtkonzept vorliegt. Ich verweise hierzu beispielhaft auf Pkt. 5.4.1.1.

Um ungewollte Vernetzung und die Aufweichung des zunächst strengen Zugriffsschutzes zu vermeiden, unterstreiche ich nochmals meine Forderung, dem Datenschutz und Sicherheitsaspekten schon vor der Rahmenkonzeptionierung von Hardware und Software Rechung zu tragen. Damit können letztlich nach der Hardware-Entscheidung und nach Einzeleinführungen unliebsame Überraschungen und aufwendige Korrekturen verhindert werden.

5.1.2 Datenschutzkonzept für den Einsatz von Arbeitsplatzrechnern

In meinem letzten Jahresbericht habe ich unter Pkt. 2.2.1 die Besonderheiten der Datenverarbeitung mit Personal-Computern (PC) und ihren Einsatz in der öffentlichen Verwaltung angesprochen. Die gestiegene Leistungsfähigkeit der Datenverarbeitungsanlagen und das verbesserte Preis-/Leistungsverhältnis ermöglichen zunehmend, komplexere Aufgabenstellungen automatisiert zu bearbeiten und immer mehr Arbeitsplätze mit solchen auszustatten.

Der Trend zur Datenverarbeitung auf dezentralen Arbeitsplatzrechnern fordert zunehmend den Datenschutz heraus. Die für zentrale Großrechnersysteme entwickelten Schutzkonzepte können nicht ohne weiteres auf die Benutzung der dezentralen Arbeitsplatzrechner übertragen werden. So ist z. B. die Trennung der Datenverarbeitungsfunktionen untereinander und von der Sachbearbeitung beim Einsatz verteilter Datenverarbeitung nicht durchführbar. Der Sachbearbeiter kann hier alle Funktionen selbst durchführen.

Immer mehr Sachbearbeiter werden zukünftig in der Lage sein, diese Rechner nicht nur zu bedienen, sondern auch zu programmieren und u. U. unberechtigt zuzugreifen oder Dateien anzulegen. Besonders dann, wenn mehrere Aufgabengebiete über einen oder auf einem Arbeitsplatzrechner bearbeitet werden, treten in erhöhtem Maße Datenschutzprobleme auf. Wegen der fehlenden Funktionstrennung ist der Benutzer eines solchen Rechners

— gleichzeitig Auftraggeber und Auftragnehmer,

— allein verantwortlich für die Datensicherung, da er über die Anlage und Datenträger (z. B. Disketten) selbst verfügt,

— in der Lage, das Betriebssystem selbst zu modifizieren,

— in der Lage, Programme zu entwickeln und Standard-Software selbst auszuwählen

— und in der Lage, letztlich über die Auswertungen aus der Datenverarbeitung zu verfügen.

Ein Teil der für Großrechner entwickelten Grundsätze der ordnungsgemäßen Datenverarbeitung ist auf den PC-Einsatz nicht übertragbar. Hieraus resultieren neue Gefährdungen für die Persönlichkeitsrechte der Betroffenen.

Software- und Hardware-Hersteller bemühen sich seit einiger Zeit, die besonderen Herausforderungen, die mit dem Einsatz von PC für den Datenschutz verbunden sind, zu berücksichtigen. So wird z. B. Datenschutz-Software entwickelt, die gleichsam als Schale über das Betriebssystem gestülpt werden kann, damit die Benutzung des PC streng menue-gesteuert erfolgen kann (der Zugriff auf das Betriebssystem und damit auf die Steuerung wird verhindert). Tests haben gezeigt, daß der Schutz insbesondere bei Individual-Software möglich ist, bei einigen Standardsoftware-Produkten läßt sich jedoch das Betriebssystem umgehen und ermöglicht dadurch den unbefugten Zugriff auf personenbezogene Dateien. Außerdem läßt die Zugriffsprotokollierung insoweit zu wünschen übrig, als der Nachweis des Dateien- und Felder-Zugriffs nicht möglich ist.

Somit bleibt vorerst nur die Möglichkeit, organisatorische Vorkehrungen zu treffen, die in einem Datenschutzkonzept für PC festzulegen sind.

Ich fordere nunmehr seit ca. drei Jahren die Vorlage eines ausreichenden Datenschutzkonzeptes für den PC-Einsatz in der gesamten bremischen Verwaltung.

Während dieser Zeit sind laufend weitere PC eingesetzt worden. Der Datenschutzausschuß hat sich aufgrund meiner Kritik im 9. Jahresbericht mit dieser Frage beschäftigt und Vertreter der Senatskommission für das Personalwesen hierzu gehört. Bisher sind als Konzept der Entwurf einer Systemakte und sehr vorläufige Überlegungen für das dringende PC-Konzept vorgelegt worden. Ich weise nachdrücklich darauf hin, daß es nicht mehr länger vertretbar ist, weitere PC-Einsätze zu beschließen, ohne daß ein Datenschutzkonzept vorgelegt wird.

5.1.3 Auftragsdatenverarbeitung durch das Rechenzentrum der bremischen Verwaltung (RbV)

Ein wesentliches Prinzip zur Gewährleistung der Datensicherung im Rechenzentrum ist die Trennung zwischen Entwicklung und Anwendung der Programme.

Diese Trennung ist im RbV wohl formal vollzogen, doch hat eine Prüfung gezeigt, daß sie praktisch nicht durchgehalten wurde. Dieses Fehlverhalten läßt die Vermutung zu, daß es sich bei dem Verstoß nicht um einen Einzelfall handelt. Dieser Sachverhalt veranlaßt mich, dazu einige grundsätzliche Bemerkungen zu machen:

Es wurden Programmänderungen durchgeführt, für die keine schriftlichen Aufträge vorlagen. Für alle Programmänderungen haben jedoch schriftliche Anweisungen des Auftraggebers vorzuliegen. Es ist ein Gebot der ordnungsgemäßen Datenverarbeitung, daß eine vollständige Dokumentation erfolgt. Ich verweise dazu auf die ADV-Anweisung vom 21. September 1981, die bezüglich der Dokumentation Mindestunterlagen fordert. Dazu gehören u. a. der Auftrag mit der Aufgabenstellung und der Nachweis der Änderung der Programme. Ich verweise in diesem Zusammenhang auch auf § 6 Abs. 2 Nr. 8 BrDSG, der die Kontrolle des Auftraggebers vorschreibt, ob weisungsgerecht verarbeitet worden ist. Diese Kontrolle kann im geschilderten Fall nicht durchgeführt werden. Der Auftragnehmer kann sich nicht darauf zurückziehen, daß der Auftraggeber nicht korrekt gearbeitet hat. Er steht ebenso in der Verantwortung, wenn weisungsgerechte Auftragsdatenverarbeitung nicht nachweisbar ist.

Es sind Originaldaten zu Testzwecken verwendet worden; dies widerpricht ebenfalls der o. g. ADV-Anweisung. Danach ist Testmaterial, das charakteristische Beispiele des Sachproblems enthält, von der auftraggebenden Stelle zu benennen und anonymisiert zu verarbeiten. Im nachhinein konnte nicht festgestellt werden, ob hierfür eine Weisung des Auftraggebers vorlag. Unter Umgehung der im RbV vorgesehenen organisatorischen Funktionstrennung hat sich die „Anwendungsentwicklung" selbständig Extrakte aus Original-Dateien gezogen. Damit wurde gegen das nach § 6 Abs. 2 Nr. 10 BrDSG vorgesehene Prinzip der Organisationskontrolle verstoßen.

Diese Mängel habe ich förmlich beanstandet und verlangt, daß das RbV zukünftig die ADV-Anweisung und die RbV-Anweisung strikt beachtet.

5.2 Personalwesen

Datenübermittlung an Dienstvorgesetzte bei Verstößen gegen Strafgesetze in der Freizeit durch Beschäftigte des Stadt- und Polizeiamtes.

Der Personalrat der Verwaltungspolizei hat mir mitgeteilt, daß es im Stadt- und Polizeiamt üblich ist, daß dem jeweiligen Dienstvorgesetzten oder Leiter der Beschäftigungsbehörde grundsätzlich eine Kopie der Strafanzeige übersandt wird. Dies geschieht durch das zuständige Kommissariat der Kriminalpolizei, wenn bei Bediensteten des Stadt- und Polizeiamtes der Verdacht besteht, daß sie in ihrer Freizeit gegen Strafgesetze verstoßen haben und es deshalb zu einer Strafanzeige kommt. Der Personalrat hält dies für unzulässig und hat mich um datenschutzrechtliche Beurteilung gebeten.

Ich habe dem Stadt- und Polizeiamt mitgeteilt, daß ich die dargestellte Praxis für unzulässig halte, da eine vom Bremischen Datenschutzgesetz geforderte Rechtsvorschrift für die Zulässigkeit des damit verbundenen Eingriffs in das Recht auf informationelle Selbstbestimmung der Betroffenen nicht in Sicht ist. Der vom Stadt- und Polizeiamt geäußerten Ansicht, daß die Datenübermittlung aus Gründen der Staatsräson gerechtfertigt sei, vermochte ich mich nicht anzuschließen, da das Bundesverfassungsgericht in ständiger Rechtsprechung insbesondere in seinem Urteil zum Volkszählungsgesetz 1983 entschieden hat, daß Eingriffe in Grundrechte nur aufgrund einer verfassungsmäßig zustande gekommenen Rechtsvorschrift zulässig sind. Bei Beamten können solche Eingriffe übergangsweise nur im Rahmen der Anordnung über Mitteilung in Strafsachen vom 15. März 1985 (MiStra) hingenommen werden.

Ich habe das Stadt- und Polizeiamt aufgefordert, die bisherige Übermittlungspraxis einzustellen und sich auf die nach der MiStra vorgesehenen Übermittlungen zu beschränken.

Das Stadt- und Polizeiamt konnte sich nicht entschließen, dem zu folgen. Es hat angeführt, daß der Leiter des Amtes seine Aufgaben als Dienstvorgesetzter nur erfüllen könne, wenn die Bediensteten der Behörde den Leumund hätten, den sie nach Ansprüchen der Öffentlichkeit benötigen, um die ihnen übertragenen Aufgaben sowohl in der Außenwirkung als auch im Innenverhältnis überzeugend erfüllen zu können. Ein Bediensteter, der einen Aufgabenbereich bearbeitete und darin hoheitlich tätig werde, in dem er selber gefehlt habe, werde vom Bürger nicht ernst genommen. Daran werde letztendlich die rechtmäßige Aufgabenerfüllung scheitern und den Staat in Gefahr bringen. Die Datenübermittlung sei deshalb im überwiegenden Allgemeininteresse erforderlich.

Als Rechtsgrundlage sehe es § 11 BrDSG an, wonach die Datenübermittlung innerhalb des öffentlichen Bereichs zulässig sei, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich sei. Soweit davon Beamte betroffen seien, finde dieses seine Stütze in den Vorschriften des Bremischen Beamtengesetzes über die allgemeinen Pflichten des Beamten, wonach er bei seiner Amtsführung auf das Allgemeinwohl Bedacht zu nehmen und sein Verhalten innerhalb und außerhalb des Dienstes so einzurichten habe, daß es der Achtung und dem Vertrauen gerecht werde, die sein Beruf erfordere, sowie in den Vorschriften, nach denen einem Beamten aus zwingenden dienstlichen Gründen die Führung seiner Dienstgeschäfte verboten werden könne und einem Polizeivollzugsbeamten das Tragen der Dienstkleidung und Ausrüstung, der Aufenthalt in Polizeidienstgebäuden und anderes verboten werden könne.

Den Einlassungen des Stadt- und Polizeiamtes vermag ich nicht zu folgen. Soweit eine Erlaubnis für die Übermittlung in der Vorschrift des § 11 BrDSG gesehen wird, ist darauf zu verweisen, daß das Bundesverfassungsgericht dargestellt hat, daß es für Eingriffe in das Recht auf informationelle Selbstbestimmung einer bereichsspezifischen Regelung bedarf und daß die allgemeinen Datenschutzgesetze dafür nur in Ausnahmefällen ausreichen. Ein solcher Ausnahmefall ist hier nicht gegeben. Das ergibt sich schon allein daraus, daß die hier praktizierte Datenübermittlung tief in das auch den öffentlich Bediensteten zustehende Grundrecht auf Schutz ihrer ureigenen privaten Sphäre eingreift. Es soll nicht verkannt werden, daß dieses Recht mit der Pflicht zu einem bestimmten außerdienstlichen Verhalten kollidiert. Da es sich bei dem Recht auf informationelle Selbstbestimmung ebenso um ein Recht mit Grundrechtscharakter handelt, kann die Auflösung dieser Kollision und die dabei notwendige Güterabwägung nicht dem Dienstherrn oder wie hier gar dem Dienstvorgesetzten überlassen bleiben. Dieses ist allein Aufgabe des Gesetzgebers. Er hat bisher keine Regelungen dazu getroffen.

Soweit man dem Dientherrn eine Kontrollmöglichkeit über außerdienstliches Verhalten durch Verarbeitung für andere Zwecke gewonnener personenbezogener Daten zugestehen will, kann dieses höchstens im Rahmen des „Übergangsbonus" hingenommen werden.

Da die Staatsanwaltschaft Herrin der im vorliegenden Fall übermittelten Daten ist und die Übermittlung von im Anzeigeverfahren gewonnener Daten an den Dienstherrn oder an Dienstvorgesetzte in der MiStra geregelt ist, muß jede über die darin vorgesehene Übermittlung hinausgehende als rechtswidrig angesehen werden.

Ich habe dem Stadt- und Polizeiamt meine Rechtsauffassung mitgeteilt und es aufgefordert, diese zu beachten und Übermittlungen nur noch im Rahmen der MiStra zuzulassen. Eine Antwort steht noch aus.

5.3 Inneres

5.3.1 Innere Sicherheit

5.3.1.1 Schwerpunkte, Handlungsbedarfsfälle

— Prüfungen im Stadt- und Polizeiamt

- **Staatsschutzprüfung/APIS**

  Ende 1987 habe ich mit einer Querschnittsprüfung der Arbeitsdatei PIOS — Innere Sicherheit = APIS (PIOS bedeutet Personen Institutionen Objekte Sachen) begonnen. APIS ist eine Verbunddatei des Bundes und der Länder. Hard- und Software werden bei dem Bundeskriminalamt (BKA) verwaltet und

gepflegt. Zugriff auf das System haben das BKA und die Landeskriminalämter (LKA), in Bremen ist diese Aufgabe der Inspektion 7 beim Stadt- und Polizeiamt Bremen übertragen worden. Dort sind auch die Kommissiariate zusammengefaßt, die Staatsschutzdelikte verfolgen.

Das System ermöglicht, daß bundesweit die zu einer Person im System vorhandenen polizeilichen Informationen zusammengeführt, abgerufen, ergänzt oder verändert werden können. Modernste Technik, neue Datenbankstrukturen und komfortable Recherche-Möglichkeiten machen APIS zu einem schnellen und in Zukunft bedeutsamen System. Deshalb habe ich mich frühzeitig bei seinem Aufbau eingeschaltet, um die bremische Praxis der Speicherung und Nutzung zu beeinflussen. In APIS werden Ermittlungserkenntnisse zu Straftaten der klassischen Staatsschutzdelikte, wie z. B. Hochverrat §§ 80 ff. StGB, Straftaten gegen ausländische Staaten oder gegen Verfassungsorgane §§ 102 ff. StGB gespeichert aber auch andere Straftaten, sofern sie wegen der Angriffsrichtung, dem Motiv des Täters oder dessen Verbindung zu einer Organisation politisch motiviert sind.

Bei der Prüfungsvorbereitung und der Einführung ins System fand ich trotz zeitlicher Engpässe von seiten der Inspektion die notwendige Unterstützung. Weil die Prüfung noch nicht abgeschlossen ist, werde ich die Prüfungsergebnisse insgesamt erst im nächsten Jahresbericht darstellen.

- **Speicherung von Volkszählungsgegnern**

Einen vorläufigen Abschluß hat die Prüfung hinsichtlich der Volkszählungsgegner, die in APIS gespeichert waren, genommen. Im Zuge der Prüfung hatte ich festgestellt, daß Personen, denen im Zusammenhang mit der Volkszählung die Begehung einer Straftat vorgeworfen wurde, in APIS gespeichert waren.

An dieser Stelle ist darauf hinzuweisen, daß im Gegensatz zu einzelnen anderen Bundesländern Bremen darauf verzichtet hat, erklärte Volkszählungsgegner und solche, die zu einem Boykott der Volkszählung aufgerufen haben, polizeilich zu erfassen und in APIS zu speichern. Hier wurde zurecht erkannt, daß die Nicht-Teilnahme an der Volkszählung sowie der Aufruf dazu keine Straftat, sondern lediglich eine Ordnungswidrigkeit darstellen.

Bei meiner Prüfung habe ich festgestellt, daß 15 Straftaten in APIS eingestellt wurden. In 9 Fällen wurde gegen Unbekannt ermittelt, in den übrigen 6 Fällen waren der Täter bzw. die Täter ermittelt. Der größere Teil der in APIS eingestellten Fälle stammte aus Bremerhaven.

Insgesamt wurden zu den Sachverhalten 11 vom Land Bremen gespeicherte Personendatensätze von mir in APIS festgestellt. Diese Zahl erklärt sich daraus, daß zum Teil die Taten gemeinschaftlich begangen wurden. In vielen Fällen handelt es sich um Erstspeicherungen in APIS.

Selbst wenn man der Argumentation des Stadt- und Polizeiamtes, das die Speicherung ursprünglich für zulässig hielt, folgte, muß festgestellt werden, daß auch hiernach einige Datensätze aus APIS zu löschen waren. So wurde z. B. anstelle des in einer Zeitschrift namentlich genannten Verfassers eines Artikels der Herausgeber dieser Zeitschrift gespeichert, obwohl dieser nur für namentlich nicht gekennzeichnete Artikel presserechtlich verantwortlich zeichnet. In zwei anderen Fällen hatte die Staatsanwaltschaft bereits das Verfahren eingestellt mit der Begründung, der von der Polizei ermittelte Sachverhalt sei unter keinem rechtlichen Gesichtspunkt strafbar. Dieses Ergebnis des Staatsanwaltes wurde zu dem Datensatz gespeichert, nicht hingegen wurde die umgehende Löschung veranlaßt.

Ich habe aber nicht nur die Löschung dieser Datensätze, sondern die Löschung aller Speicherungen in APIS, die im Zusammenhang mit der Volkszählung vorgenommen wurden, verlangt. Ich habe darauf hingewiesen, daß die Errichtungsanordnung eine Speicherung dieser Fälle in APIS nicht vorsieht.

Im übrigen ist klarzustellen, daß die Speicherung der sogenannten anderen Straftaten, die nicht zu den klassischen Staatsschutzdelikten zählen, sondern wegen ihrer Angriffsrichtung oder dem Motiv des Täters einen politischen Charakter tragen, nicht schon allein deswegen in APIS gespeichert werden dürfen, sondern es bedarf hier jeweils einer Einzelfallabwägung.

In der Bürgerschaft hat der Innensenator u. a. dazu erklärt, daß sich aus der

Tatsache des Volkszählungsboykotts eine staatsfeindliche Absicht, auch im Zusammenhang mit einer solchen Straftat, nicht begründen ließe.

Bei der Speicherung in APIS ist zu berücksichtigen, daß durch die bundesweite zur Verfügungstellung ein besonders schwerwiegender Eingriff in die Persönlichkeitsrechte des Betroffenen einhergeht und durch die Speicherung diese Personen in einen Topf z. B. mit Terroristen geworfen werden. Ich habe daher erklärt, daß in den von mir geprüften Fällen eine Speicherung in APIS auch unter dem Gesichtspunkt der Verhältnismäßigkeit unzulässig war.

Dieses Ergebnis mag folgender Sachverhalt verdeutlichen: Drei 17jährige Schüler schreiben mit Farbe auf einem Parkplatz das Wort „Volkszählungsboykott". Eine Polizeistreife ertappt die drei dabei. Ein Strafverfahren wegen Sachbeschädigung wird eingeleitet, eine Speicherung der Personendaten in APIS wird vorgenommen.

Hätten diese drei Schüler irgendein anderes Wort ohne politischen Bezug auf den Parkplatz geschrieben, wäre zwar auch der Tatbestand der Sachbeschädigung erfüllt, zu einer Speicherung in einem bundesweit verfügbaren polizeilichen Informationssystem wäre es jedoch nicht gekommen. Der Vorgang wäre in dem auf das Land Bremen begrenzte polizeiliche Informationssystem ISA gespeichert worden. Die Schüler dürfen daher nicht schlechter gestellt werden. Die Speicherung in APIS war daher zu löschen.

Meinem Verlangen auf Löschung all dieser Vorgänge wurde auf Anordnung des Innensenators entsprochen.

- **Einzelfälle**

Im letzten Jahr hatte ich eine Reihe von Eingaben besorgter Bürger, denen ich durch Prüfungen im Stadt- und Polizeiamt nachgegangen bin. Hierbei kontrolliere ich zunächst, ob Speicherungen in den polizeilichen Informationssystemen ISA, INPOL und APIS vorhanden sind. Im Falle einer Speicherung prüfe ich die Richtigkeit anhand des Akteninhalts, im übrigen die Einhaltung der Löschungsfristen, in geeigneten Fällen die Sammlung der erkennungsdienstlichen Behandlung auf Richtigkeit respektive auf Vernichtung. Die im letzten Jahr geprüften Fälle ließen sich alle aufklären, Beanstandungen mußten nicht ausgesprochen werden.

— Sicherheitsüberprüfung von Personal auf zivilen Flughäfen

Von Vertretern der Bremischen Luftfahrtbehörde bin ich gebeten worden, zu rechtlichen Fragen bei der Sicherheitsprüfung bei Personen im Rahmen des § 29 Luftverkehrsgesetz (LuftVG) Stellung zu nehmen.

Ausgangspunkt ist, daß die Betreiber ziviler Lufthäfen Ausweise an Personen aushändigen, die dann unkontrolliert den Sicherheitsbereich von Flughäfen betreten dürfen. Vor Aushändigung eines solchen Ausweises werden die nach den §§ 29 ff. LuftVG zuständigen Luftfahrtbehörden gefragt, ob Sicherheitsbedenken bestehen. Die Luftfahrtbehörden überprüfen die Personen, die einen Dauerausweis erhalten sollen, in den Informationssystemen der Polizei und des Verfassungsschutzes; bei der Ausgabe eines Tagesausweises werden nur die polizeilichen Informationssysteme abgefragt.

Bei meiner Beratung habe ich verschiedene datenschutzrechtliche Fragen angesprochen, u. a.:

— Differenzierung der Sicherheitszonen (Sicherheitsbereich, sicherheitsempfindlicher Bereich),

— Antragsverfahren (Fragebogen des Beschäftigten) und Verfahren bei Bedenken seitens der Luftfahrtbehörden,

— Überprüfungen (Kriterien-Katalog luftfahrtrelevanter Sicherheitsrisiken) und Verfahren,

— Ausweisausstellung, Gültigkeitsdauer und Verlängerungsverfahren,

— Dateien und Aufbewahrungsdauer bei den Luftfahrtbehörden,

— Möglichkeiten der Differenzierung nach verschiedenen Personenkreisen,

— Festlegung, welche Behörden bei der Durchführung der Sicherheitsüberprüfung beteiligt werden sollen,

— Wahrung des Grundsatzes der Verhältnismäßigkeit in der Zweckbindung, d. h. daß die beteiligten Stellen die Daten der Antragsteller nur für die Zwecke der Flugsicherheit verwenden,

— Prüfung der Notwendigkeit einer gesetzlichen Ausgestaltung des Verfahrens.

Der Vertreter der Luftfahrtbehörde des Landes Bremen hat zugesagt, mich über den Fortgang der Gespräche auf Bundesebene zu informieren.

— Prüfung beim Landesamt für Verfassungsschutz

- **Listenmäßige Überprüfung von Beschäftigten bei einem Berufsbildungswerk durch den Verfassungsschutz**

  Von einem Journalisten wurde mir eine Namensliste übergeben, die alle beim Berufsbildungswerk des Reichsbundes in Bremen (RBBW) bis zum 31. Januar 1979 Beschäftigten enthält. In dieser Liste befinden sich hinter den Namen einiger Beschäftigter handschriftliche Vermerke („pos"). Von seiten des Betriebsrates beim RBBW wurde der Verdacht geäußert, daß die Liste seinerzeit durch das Landesamt für Verfassungsschutz (LfV) überprüft worden sei und daß die Personen, über die Daten gespeichert sind, mit „pos" gekennzeichnet worden seien. Gemutmaßt wurde dabei, daß der Vermerk „pos" für das Wort „positiv" stünde und bedeute, daß die Daten dieser Personen beim LfV gespeichert seien.

  Aufgrund der öffentlich erhobenen Vorwürfe bin ich der Sache umgehend nachgegangen und habe eine Prüfung beim LfV durchgeführt. Dazu habe ich alle in der Liste mit „pos" gekennzeichneten Personen in dem Informationssytem der Verfassungsschutzämter des Bundes und der Länder NADIS geprüft und in den Fällen, in denen ich einen Bremer Vorgang feststellen konnte, habe ich mir die Akte vorlegen lassen.

  Aufgrund der erzielten Prüfergebnisse ließ sich keine Aussage mit hinreichender Sicherheit machen. Die Ergebnisse zusammen mit den aufgrund meiner Überprüfung beim RBBW gewonnenen Erkenntnissen (hier speziell die Erklärung der Geschäftsleitung beim RBBW, daß diese Liste dort über Jahre im Stahlschrank aufbewahrt worden sei, obwohl das dazu parallel laufende Stammbuch in der Personalabteilung offen geführt wurde) veranlaßten mich, eine Protokollauswertung der Zugriffe auf die Daten durch das LfV Bremen beim Bundesamt für Verfassungsschutz (BfV) zu verlangen.

  Da nicht jede Anfrage an NADIS protokolliert und über einen längeren Zeitraum aufbewahrt wird, sondern nur die Anfragen, die mit einem gespeicherten Personendatensatz korrespondieren, konnte ich nicht mehr überprüfen, ob tatsächlich die gesamte Liste seinerzeit überprüft worden ist. Ich habe mich daher auf eine Auswahl beschränkt und für diese Personen für einen Zeitraum nach dem 1. Februar 1979 die Protokollauswertung verlangt.

  Dabei ist festgestellt worden, daß über ein Terminal des LfV Bremen am 19. Februar 1979 nacheinander auf alle von mir benannten Personen zugegriffen worden ist. In welchem Umfang und auf welchem Wege entsprechende Mitteilungen an das RBBW gelangt sind, läßt sich heute nicht mehr mit Sicherheit feststellen, ein Zusammenwirken zwischen einer öffentlichen Stelle und der Geschäftsleitung des RBBW kann jedoch nicht ausgeschlossen werden.

  Auf die von mir geforderte Löschungsüberprüfung hin hat das LfV hinsichtlich der Bremer Datensätze bei 11 Personen eine vollständige Löschung der Datensätze in NADIS vorgenommen.

  Rechtlich habe ich die oben geschilderten Vorgänge wie folgt beurteilt:

  Unabhängig davon, ob das LfV selbst oder der Senator für Inneres damals personenbezogene Mitteilungen gemacht hat, steht fest, daß die Daten an das RBBW gelangt sind. Datenschutzrechtlich handelt es sich um eine Datenübermittlung, die aus nachfolgenden rechtlichen Gründen rechtswidrig ist.

  Eine Anwendung von § 6 des Bremischen Verfassungsschutzgesetzes in der damals gültigen Fassung (13. März 1974 — BremVerfassungsschutzG 1974 —) scheidet aus, da weder die Einwilligung des Senators für Inneres nachgewiesen wurde, noch der Schutz der freiheitlich demokratischen Grundordnung oder der Bestand und die Sicherheit des Bundes oder des Landes eine Überprüfung der zu diesem Zeitpunkt beim RBBW bereits eingestellten Beschäftigten erforder-

lich gemacht hätte. Auch eine Überprüfung der noch Einzustellenden wäre nach dieser Vorschrift unzulässig gewesen.

Da das BremVerfassungsschutzG 1974 keine weiteren bereichsspezifischen Regelungen für Datenübermittlungen in den nicht-öffentlichen Bereich enthält — das RBBW ist privatrechtlich organisiert —, beurteilt sich die Zulässigkeit der Datenübermittlung an das RBBW nach dem Bremischen Datenschutzgesetz in der Fassung vom 19. Dezember 1977 (BrDSG 1977). § 13 BrDSG 1977 regelt die Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs. Nach Abs. 1 ist die Übermittlung personenbezogener Daten an Personen und an andere Stellen als die in § 11 BrDSG 1977 bezeichneten zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist oder, soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Als Maßstab der Rechtmäßigkeit der Aufgabenerfüllung ist § 3 Abs. 2 BremVerfassungsschutzG 1974 heranzuziehen. Eine Mitwirkung des LfV nach § 3 Abs. 2 Nrn. 1, 3 und 4 scheidet bereits aufgrund ihres Wortlautes aus. Aber auch Nummer 2 ist nicht erfüllt, da das RBBW auch damals keine sicherheitsempfindliche Stelle einer lebens- und verteidigungswichtigen Einrichtung war.

Schließlich war eine Datenübermittlung in einigen Fällen der in der Liste verzeichneten Personen allein auch deshalb unzulässig, weil die Datenübermittlung gegen schutzwürdige Belange der Betroffenen verstoßen hat, denn, wie ich aufgrund der Aktenlage feststellen konnte, war hinsichtlich einiger Personen die Erkenntnislage beim LfV so qualifiziert, daß man allenfalls von einem „Anfangsverdacht" hätte sprechen können und ein Hinweis an das RBBW auch aus diesem Grunde hätte ausscheiden müssen.

Unabhängig davon, daß eine Datenübermittlung an die Geschäftsleitung des RBBW ohnehin rechtlich damals wie heute unzulässig gewesen ist, hätte eine Übermittlung an das RBBW auch deshalb unterbleiben müssen, weil bei der Überprüfung einer Liste von 160 Namen davon wenig mehr als 20 mit einem NADIS-Eintrag versehen waren. Eine vollständige Überprüfung einer Belegschaft dieses privaten Unternehmens durch das LfV ist unverhältnismäßig. Auch wenn sich aufgrund der Protokollage heute nicht mehr feststellen läßt, ob die Liste vollständig oder nur in Teilen mit dem Datenbestand in NADIS abgeglichen worden ist, so liegt doch die Vermutung nahe, daß der ganz überwiegende Teil der Personen einer Überprüfung unterzogen worden ist. Dies ergibt sich neben anderen Überlegungen daraus, daß nur bei einer vollständigen Überprüfung auch alle Personen entdeckt werden, denen der Abgleich galt.

Ich bin, wie dargestellt, insgesamt zu dem Ergebnis gekommen, daß die Überprüfung durch das LfV und die Übermittlung der positiv festgestellten Personen unter datenschutzrechtlichen Bewertungen unzulässig waren. Ich habe daher die unzulässige Überprüfung und Datenübermittlung gegenüber dem Innensenator beanstandet und ihn um Stellungnahme gebeten.

Der Senator für Inneres hat sich — entsprechend seiner Erklärung in der 10. Sitzung der Bremischen Bürgerschaft vom 18. Februar 1988 — mir gegenüber zu dem Vorgang wie folgt geäußert:

Die Überprüfung der gesamten Liste wäre als unverhältnismäßig unzulässig gewesen. Zu den bestehenbleibenden Unklarheiten gehöre es aber, daß nicht mehr festgestellt werden könne, ob die gesamte Liste oder Teile hiervon durch das LfV bearbeitet worden seien. Der Senator für Inneres vertritt die Auffassung, daß eine denkbare dosierte Übermittlung durch das LfV an das RBBW aus der Sicht des Jahres 1979 vertretbar gewesen wäre. § 6 BremVerfassungsschutzG in der 1979 geltenden Fassung und auch in der heute seit 1981 geltenden Fassung ergebe für ein pflichtgemäßes Ermessen des Senators für Inneres die Rechtsgrundlage, daß mit seiner Genehmigung dosiert, personenbezogene Informationen auch an andere als staatliche Stellen gegeben werden dürfen. Voraussetzung dafür sei gewesen und sei noch, daß diese Informationen den Schutz vor Bestrebungen gegen die freiheitlich demokratische Grundordnung dienen und an eine Institution gegeben werde, welche äußerst staatsnah ausgeprägt öffentliches Interesse verkörpere. Vorausgegangen sei der Übermittlung Anfang 1979, daß das Landesamt für Verfassungsschutz in der zweiten Jahreshälfte 1978 unmittelbar aus einem örtlichen KBW-Bezirk den Hinweis erhalten habe, es sei gelungen, daß beim RBBW bereits einige Mitglieder des KBW

FFD 12/163

eine Anstellung gefunden hätten und man habe das Ziel, „den Laden in die Hand zu bekommen". Diese Mitteilung sei dem Senator für Inneres vorgelegt worden.

Bei den mit „pos" 1979 gekennzeichneten Personen handele es sich überwiegend um Personen des Kommunistischen Bundes Westdeutschland (KBW) und Personen, die kleineren, dem KBW verwandten extremistischen Organisationen zuzurechnen waren.

Bei der damaligen Entscheidung der Datenübermittlung seien die politischen Ziele und der Aufbau des KBW zu berücksichtigen. Der KBW sei damals in der Bundesrepublik die mitgliederstärkste Organisation innerhalb der dogmatischen „neuen Linken" mit 2500 Mitgliedern, davon im bremischen Bereich 230, gewesen. An der extremistischen Zielrichtung, die im Programm auch Gewalt und bewaffneten Aufstand nicht ausschloß, habe kein Zweifel bestanden.

Zu berücksichtigen sei aber auch die besondere Stellung des RBBW. Das RBBW sei zwar eine GmbH, insoweit eine andere staatliche Stelle im Sinne des § 6 BremVerfassungsschutzG, integrativer Bestandteil des RBBW sei jedoch die Berufsschule für Behinderte, welche für Rehabilitanten die gleiche Aufgabenstellung habe, wie die staatlichen Berufsschulen für die Gesamtheit der Berufsschulpflichtigen. Schon dies sei eine öffentliche Aufgabe mit hohem Rang. Zum anderen habe das RBBW auch die Ausbildung für behinderte Jugendliche übernommen, die sonst unter den Bedingungen des Ausbildungsstellenmarktes keine Ausbildung erhalten würden. Dies sei ebenfalls eine öffentliche Aufgabe. Das RBBW unterliege in seiner Aufgabenerfüllung der vollen Fachaufsicht in der Weise, daß die Rechtsform der GmbH als eine reine Organisationsfrage für einen an sich sonst unabweisbaren staatlichen Betrieb erscheine.

Über den Fall hinaus weist der Innensenator darauf hin, daß auch künftig solche Fälle denkbar seien. Solche Entscheidungen müßten aber absoluten Ausnahmecharakter haben. Seit 1981 gelte zudem, daß der Senator für Inneres oder sein Vertreter im Amt diese Entscheidung zu treffen habe.

Auch nach den Ausführungen des Senators für Inneres halte ich an meiner Rechtsauffassung fest. Weil der Innensenator auch in Zukunft solche Datenübermittlungen nicht auszuschließen vermag, möchte ich mich mit seinen Argumenten im folgenden auseinandersetzen, um so künftig Datenschutzverstößen vorzubeugen:

1. Aus der Anordnung im Gesetzestext, der die Alternativen „Bestrebungen gegen die freiheitlich demokratische Grundordnung" und „Bestrebungen gegen den Bestand oder die Sicherheit des Bundes oder eines Landes" nennt, entnehme ich, daß der Gesetzgeber beabsichtigt hat, nur in Fällen vergleichbarer Schwere dürfe eine Mitteilung erfolgen. Eine diesen Voraussetzungen entsprechende Lage war in diesem Fall 1979 nicht gegeben.

2. Die allgemeinen gesetzlichen Regelungen zur Zulässigkeit von Datenübermittlungen (BrDSG, BDSG) differenzieren zwischen Datenübermittlung innerhalb des öffentlichen Bereichs und Datenübermittlungen an private Dritte; die Übermittlung an private Stellen knüpft an strengere, einschränkende Voraussetzungen. Dieser Grundsatz ist bei der Auslegung der Datenübermittlungsregelungen nach § 6 des BremVerfassungsschutzG entsprechend zu berücksichtigen.

3. Der frühere wie auch der neue § 6 BremVerfassungsschutzG knüpfen im Kerngehalt an dieselben Voraussetzungen an: Eine Datenübermittlung an private Stellen ist nur zulässig „zum Schutz vor Bestrebungen gegen die freiheitliche demokratische Grundordnung oder den Bestand und die Sicherheit des Bundes oder eines Landes". Daß die Mitteilung zum Schutze des Bestandes und der Sicherheit des Bundes oder eines Landes gemacht wurde, ist von keiner Seite behauptet worden. Demnach müßte die Mitteilung dazu dienen, Schutz zu bieten vor einer Bestrebung gegen die freiheitlich demokratische Grundordnung. Der KBW wurde als solche Bestrebung angesehen. Daß aber eine solche Mitteilung an das RBBW dem Schutz der freiheitlich demokratischen Grundordnung dienen konnte, ist vom Senator für Inneres nicht dargelegt worden. Die freiheitlich demokratische Grundordnung realisiert sich im wesentlichen einer entsprechenden Staatsform und der hieraus abgeleiteten Staatsmacht. Im Gegensatz dazu steht der totalitäre Staat. Das RBBW ist privat-rechtlich organisiert, also keine staatliche Institution. Nur

FFD 12/103

soweit von einem privaten Unternehmer für die freiheitlich demokratische Grundordnung unmittelbar Gefahren ausgehen, könnte eine Mitteilung gerechtfertigt sein. Dafür gab es hier keine Anhaltspunkte.

4. Man hat 1979 eine einzige Information zum Anlaß genommen, die gesamte Belegschaft oder aber doch wenigstens einen großen Teil einer Belegschaft zu überprüfen und das Ergebnis der Geschäftsleitung mitzuteilen. Es sind wesentlich höhere Anforderungen an die Sicherheit solcher Erkenntnisse zu stellen, bevor eine im übrigen zulässigen Mitteilung an Private erfolgen darf.

5. Aufgrund der Aktenlage habe ich festgestellt, daß, soweit „pos" über eine Person mitgeteilt würde, dies ohne Prüfung der tatsächlichen Vorgänge, die zu einer Speicherung der Betroffenen geführt haben, geschah. Eine Mitteilung ohne Prüfung, welche Relevanz eine Person für eine Organisation haben kann, ist unverhältnismäßig.

6. In der Liste des RBBW waren auch die einzelnen Abteilungen, in denen die Beschäftigten des RBBW tätig waren, vermerkt. Eine Differenzierung zwischen Lehrpersonal und sonstigem Betreuungs- oder Verwaltungspersonal bei den „pos"-Vermerken habe ich nicht feststellen können. Wenn es also dem Innensenator um eine einer staatlichen Ausbildung vergleichbaren Situation geht, hätte man sich auf eine Überprüfung des Lehrkörpers beschränken müssen. Aus der unterschiedslosen Kennzeichnung von Personen, die in verschiedenen Abteilungen tätig waren, schließe ich, daß das Küchenpersonal ebenso wie der Lehrkörper überprüft worden ist und entsprechende Mitteilungen erfolgten. Auch dies verstößt bei Anerkennung der Argumentation des Innensenators gegen den Verhältnismäßigkeitsgrundsatz.

7. Ich habe nicht erkennen können, daß durch andere Maßnahmen, die weniger eingreifend in die Persönlichkeitsrechte der Beschäftigten gewesen wären, versucht worden ist, dem Anliegen des Innensenators Rechnung zu tragen. Wenn, wie er hervorhebt, die volle Fachaufsicht gegenüber dem RBBW gilt, so hätte man dieses Instrument gezielt einsetzen können, um sicherzustellen, daß der Lehrkörper bei der Unterrichtsgestaltung den schulischen Anforderungen nachkommt.

8. Der Innensenator konstruiert eine Nähe zwischen der Ausbildung beim RBBW und der Ausbildung durch Berufsschullehrer an öffentlichen Schulen. Der Argumentation ist zu entnehmen, daß er dieselben Anforderungen an die Verfassungstreue von Lehrern des RBBW wie bei Lehrern an öffentlichen Schulen stellen will. Mit diesem Argument rechtfertigt er dann die personenbezogene Mitteilung an das RBBW. Diese Argumentation verkennt, daß es sich um unterschiedliche Verfahren handelt. Bei der Einstellungsüberprüfung in den öffentlichen Dienst wirkt der Betroffene mit. Ihm wird das Verfahren eröffnet, bei Ablehnung wird ihm bekannt, daß Bedenken an seiner Verfassungstreue bestehen. Hiergegen kann er sich in einem rechtsförmigen Verfahren wehren. Ganz anders hingegen bei dem gegenüber dem RBBW praktizierten Verfahren. Hier wird eine Mitteilung an die Geschäftsleitung gegeben, die hinter dem Rücken des Betroffenen erfolgt. Gegen die Richtigkeit einer solchen Mitteilung kann der Betroffene sich daher nicht wehren. Welche Auswirkungen diese Mitteilung auf sein Arbeitsverhältnis hat, ist ihm nicht bekannt, da nicht zu erwarten ist, daß ihm der wahre Grund mitgeteilt wird, sondern andere Gründe vorgeschoben werden. Schließlich kann er sich bei Bewerbungen bei anderen privaten Stellen nicht sicher sein, daß sein früherer Arbeitgeber diese Kenntnis auf Nachfrage nicht weitergibt.

Ich habe anhand des RBBW-Beispiels einige einschränkende Kriterien für die Anwendung des § 6 Abs. 2 Nr. 4 BremVerfassungsschutzG entwickelt, die verdeutlichen, daß nur in besonderen Fällen die Regelung einmal greifen kann.

Anhand der Protokollausdrucke habe ich festgestellt, daß das LfV nach der Umstellung auf eine erweiterte Protokollierung nicht alle Felder genutzt hat. So war deshalb nicht erkennbar, auf wessen Veranlassung eine Datenabfrage in NADIS erfolgte. Wenn aber nicht prüfbar ist, wer aus welchem Anlaß auf NADIS zugegriffen hat, ist nachträglich in der Regel nicht prüfbar, ob eine rechtmäßige Datenverarbeitung stattgefunden hat.

Diesen Verstoß gegen Grundsätze der Datensicherheit (vgl. § 6 BrDSG) habe ich beanstandet und das LfV aufgefordert, ein Verfahren zu entwickeln, das den

von mir genannten Anforderungen Rechnung trägt und die Möglichkeiten, die das System bietet, voll ausschöpft.

Der Senator für Inneres hat hierzu u. a. erklärt, daß sichergestellt sei, daß ab sofort das LfV neben dem Anfragenden und dessen Auftraggeber lückenlos auch das Aktenzeichen dokumentiert werde, so daß es künftig aus unterlassener Dokumentation keine Unklarheit mehr geben könne. Besonders sei jetzt auch angewiesen, daß etwaige weitere Entscheidungen nach § 6 BremVerfassungsschutzG schriftlich zu begründen seien und daß die Entscheidung der Gesetzeslage entsprechend die Unterschrift des Senators oder seines Vertreters im Amt tragen müßte.

- **Einzelfälle**

Außerhalb der vorgenannten Prüfungen im Zusammenhang mit den Vorgängen um das RBBW habe ich überwiegend aufgrund von Beschwerden 20 Einzelfallprüfungen durchgeführt. Bei der Mehrzahl der Fälle konnte ich keinen Eintrag in NADIS feststellen. Soweit es sich um Speicherungen handelte, die durch das Landesamt für Verfassungsschutz Bremen veranlaßt waren, habe ich die Rechtmäßigkeit dieser Speicherung anhand der dazugehörigen Akte überprüft. In den Fällen, in denen ich die Löschung und Vernichtung der Akte empfohlen habe, wurde nach Prüfung durch den zuständigen Sachbearbeiter meiner Empfehlung entsprochen.

Aus Anlaß der öffentlichen Auseinandersetzung um die Volkszählung hatte ich mich bereits Anfang des Jahres mit dem Leiter des Landesamtes für Verfassungsschutz in Verbindung gesetzt und dabei deutlich gemacht, daß ich eine Speicherung von Volkszählungsgegnern in NADIS aus diesem Anlaß für unzulässig halte. Mir wurde versichert, daß eine Ausforschung der Gegner der Volkszählung und ihrer Initiativen nicht beabsichtigt sei. Lediglich soweit deutlich werde, daß im Einzelfall die Volkszählungsbewegung benutzt werden solle, andere verfassungswidrige Ziele damit zu verfolgen, könnte dies ein Ansatzpunkt für den Verfassungsschutz darstellen. Ich habe in einer Stichprobe Anschriften von öffentlich bekannt gegebenen Volkszählungsboykottinitiativen und von einzelnen Personen, die sich öffentlich gegen die Volkszählung ausgesprochen haben und zum Boykott aufgerufen haben, in NADIS überprüft. Dabei habe ich keine Speicherungen aus Anlaß der Volkszählung feststellen können.

5.3.1.2 Datenübermittlung bei sozialen Notlagen

Aufgrund einer Eingabe sah ich mich veranlaßt, die Datenübermittlung der Polizei an den sozialpsychiatrischen Dienst gem. § 33 Abs. 1 Satz 4 BremPolG bei erheblicher sozialer Notlage zu prüfen.

Eine Bürgerin beschwerte sich darüber, daß ihre Nachbarin im Rahmen einer Sachbeschädigungsanzeige gegenüber Polizeibeamten sich über ihren Gesundheitszustand geäußert habe. Daraufhin haben die Polizeibeamten neben einer Klärung der strafrechtlichen Gegebenheiten eine medizinische Hilfeleistung für erforderlich gehalten und den sozialpsychiatrischen Dienst des Hauptgesundheitsamtes eingeschaltet.

Gemäß § 33 Abs. 1 Satz 4 BremPolG kann die Polizei, soweit sie im Rahmen ihrer rechtmäßigen Aufgabenerfüllung Anhaltspunkte für das Bestehen einer erheblichen sozialen Notlage feststellt, der zuständigen Behörde die erforderlichen personenbezogenen Informationen übermitteln. Die Mitarbeiter der Behörde, hier Gesundheitsamt, unterliegen im übrigen der Schweigepflicht gemäß § 203 StGB.

Der mit der Strafanzeige beschäftigte Polizist hat nach der von ihm vorgefundenen Sachlage Namen und Anschrift der Bürgerin dem Hauptgesundheitsamt mitgeteilt, damit dieses sich mit ihr in Verbindung setzen kann.

Der Polizeibeamte, der in der Regel weder sozial, medizinisch, psychologisch oder pädagogisch ausgebildet ist, kann in solchen Lagen sich kein eigenes Urteil bilden, daher ist es sinnvoll und vom Gesetzgeber so vorgesehen, daß die zuständigen Stellen sich in solchen Fällen mit dem Betroffenen in Verbindung setzen und ihm auf freiwilliger Basis Hilfe anbieten.

Ein Polizeibeamter muß selbstverständlich in den Fällen, in denen er erkennt, daß mutwillig verleumderische Aussagen gemacht werden, von einer Nachricht absehen. In anderen Fällen hingegen muß er aufgrund der sich ihm stellenden Sachlage entscheiden. Eine Überprüfung der Angaben durch die Polizei selbst ist zum

einem wegen der fachlichen Ausbildung und zum anderen wegen der tatsächlichen Gegebenheiten oft nicht möglich.

In der Ermessensausübung des Polizeibeamten habe ich in dem konkreten Fall keinen Verstoß gegen Datenschutzbestimmungen gesehen. Ich habe der Beschwerdeführerin von meiner datenschutzrechtlichen Beurteilung Kenntnis gegeben.

5.3.2 Meldewesen, Paß- und Ausweiswesen

5.3.2.1 Meldewesen

— Anpassung EDAS-Verfahren an das neue Melderecht

Das **Stadt- und Polizeiamt Bremen — Meldebehörde** — setzt seit Jahren ein automatisiertes Verfahren zur Unterstützung und Erledigung melderechtlicher Aufgaben in der Zentrale ein. Dieses sog. EDAS-Verfahren (EDAS = Einwohner-Datenbank-System), das auch die Verarbeitung von Gewerbemeldedaten ermöglicht, wurde Anfang der 70iger Jahre entwickelt und im Rahmen der laufenden Verfahrens- und Programmpflege vielfach geändert. Es entspricht schon lange nicht mehr den Anforderungen der dezentral und arbeitsteilig organisierten Meldebehörde Bremen sowie den systemtechnischen Möglichkeiten heutiger Rechner- und Datenverarbeitungssysteme. Außerdem haben sich das Melde- und Datenschutzrecht inzwischen so stark verändert, daß nach Auffassung aller Beteiligten das überkommene EDAS-Verfahren grundlegend überarbeitet bzw. durch ein neues Datenverarbeitungssystem ersetzt werden muß.

Der Gesetzgeber hat den Meldebehörden bei Verabschiedung des neuen Meldegesetzes zur Anpassung ihrer Verwaltungspraxis und der alten Datenverarbeitungsverfahren an die neue Rechtslage verschiedene Übergangsfristen eingeräumt, die inzwischen sämtlich abgelaufen sind. Auch die Frist zur Anpassung der automatisiert geführten Melderegister an das neue Melderecht, bereits einmal vom bremischen Gesetzgeber um zwei Jahre verlängert, ist inzwischen überschritten: Spätestens seit dem 01. 01. 1988 müssen die automatisiert geführten Melderegister den geänderten melderechtlichen Bestimmungen (Meldegesetz, Meldedatenübermittlungsverordnung) entsprechen.

Das EDAS-Verfahren des Stadt- und Polizeiamtes Bremen, das auch 1988 genutzt wird, entspricht den o. g. Anforderungen in wichtigen Punkten nicht. Es wurde zwar punktuell geändert (z. B. durch eine Änderung der Zugriffsbefugnisse auf den Einwohner- bzw. Gewerbemeldedatenbestand, durch eine Datenbereinigung, durch innerbetriebliche Änderungen im Arbeitsablauf, durch Änderungen im monatlichen Auswertungs- und Mitteilungsdienst, durch Aussonderung der grünen Geschäftskarten mit nicht mehr im Meldebestand zulässigen Gewerbemeldedaten in den örtlichen Meldestellen), doch die wesentlichen Mängel des alten EDAS-Verfahrens können ohne eine grundlegende Verfahrensänderung nicht beseitigt werden:

- Die Einwohnermeldedaten werden weiterhin gemeinsam mit den Gewerbemeldedaten in einer physischen Datenbank geführt. Dies entspricht nicht der Bestimmung des § 2 Abs. 4 Bremisches Meldegesetz, wonach das Melderegister nicht gemeinsam mit anderen Registern geführt werden darf. Ich hatte mich seinerzeit mit Blick auf die Übergangsregelung des § 38 Abs. 4 Bremisches Meldegesetz, d. h. der Pflicht zur Anpassung des automatisiert geführten Melderegisters an das neue Melderecht bis spätestens Ende 1987 mit organisatorischen Maßnahmen (Trennung Meldebehörde und Gewerbemeldestelle, Änderung der Zugriffsregelung) anstelle einer physischen Aufteilung der Datenbank einverstanden erklärt. Da die Übergangsfrist inzwischen abgelaufen ist und das EDAS-Verfahren weiter benutzt wird, kann ich meine damalige Zustimmung zu den organisatorischen Maßnahmen heute nicht mehr aufrecht erhalten.

- Die Datensätze des EDAS-Verfahrens entsprechen ebenfalls nicht der neuen Rechtslage. Zwar wurden Ende 1984 Bereinigungsläufe durchgeführt und dabei nicht mehr zulässige Meldedaten gelöscht. Die logische Datensatzstruktur des EDAS-Verfahrens wurde dabei jedoch nicht verändert. Es wurden lediglich die Inhalte bestimmter nicht mehr zulässiger Datenfelder gelöscht. Dies ist als Dauerzustand für ein laufendes zentrales Datenverarbeitungsverfahren jedoch nicht haltbar. Weder der Betroffene noch die Öffentlichkeit werden der Verwaltung eine dauerhafte Divergenz zwischen gesetzlicher Regelung und systemtechnischer Realisierung abnehmen, selbst dann nicht, wenn beide gutgläubig und voller Vertrauen in staatliches Handeln sind.

- Die Meldedatenübermittlungsverordnung (MeldDUV) des Landes ist ohne Übergangsregelung am 13. 05. 1987 in Kraft getreten. Die Umsetzung dieser Verordnung erzwingt eine grundlegende Anpassung der regelmäßigen und der automatisierten regelmäßigen Datenübermittlungen des EDAS-Verfahrens. Eine solche grundlegende Anpassung ist bis heute nicht erfolgt. Das Stadt- und Polizeiamt Bremen hat allerdings — beginnend im August des letzten Jahres — zur Umsetzung der MeldDUV eine Reihe von Änderungen im EDAS-Verfahren in Auftrag gegeben, die den monatlichen Auswertungs- und Mitteilungsdienst sowie den online-Anschluß des Senators für Bildung, Wissenschaft und Kunst an das bremische Melderegister betreffen. Diese Programmierarbeiten konnten im Berichtsjahr nur zum Teil erledigt werden. Der online-Anschluß des Senators für Bildung, Wissenschaft und Kunst wurde beispielsweise erst Ende Februar dieses Jahres aufgehoben, neun Monate nach Inkrafttreten der MeldDUV und zwei Monate nach Ablauf der Übergangsfrist des § 38 Abs. 4 BremMeldeG. Einige Arbeiten waren zum Erstellungszeitpunkt dieses Berichts noch nicht erledigt. Nicht in Auftrag gegeben und folglich auch nicht angepaßt wurden bisher z. B. die automatisierten Abrufverfahren der Finanzbehörden, der Landeshauptkasse, der Oberfinanzdirektion, der Polizei; die diesen Stellen im Rahmen des EDAS-Verfahrens zur Verfügung gestellten Bildschirmmasken sollen vor Einführung des neuen DV-Verfahrens nicht mehr geändert werden.

Seit Jahren bemüht sich das Stadt- und Polizeiamt Bremen, das alte EDAS-Verfahren durch ein neues Verfahren abzulösen. Ursprünglich war daran gedacht, ein eigenes vollständig neues Datenverarbeitungsverfahren, das sog. DEMOS-Verfahren selbst zu entwickeln (DEMOS = **D**ezentrales **E**inwohner-**M**elde-**O**nline-**S**ystem). Von diesem Vorhaben, d. h. der Eigenentwicklung ist man u. a. aus Zeit- und Kostengründen abgerückt. Statt dessen wurde beschlossen, ein fertiges laufendes Fremdverfahren zu übernehmen und auf bremische Verhältnisse zu übertragen. Zunächst wurde dabei das Einwohnerverfahren der Stadt Duisburg favorisiert; nach detaillierter Prüfung sowie einer Test- und Erprobungsphase in Bremen wurde dieses Verfahren jedoch wieder fallengelassen. Seit dem Spätherbst 1986 steht das neu entwickelte Einwohnerverfahren der Stadt Hamburg im Zentrum der Übernahme- und Anpassungsbemühungen.

Die Entwicklungsarbeiten an diesem neuen Datenverarbeitungsverfahren in Hamburg waren zum Zeitpunkt der Übernahmeentscheidung in Bremen noch nicht abgeschlossen. Es traten offensichtlich erhebliche Zeitverzögerungen ein. Die bremischen Arbeiten zur Anpassung und Übernahme der Hamburger Datenverarbeitungsprogramme verzögerten sich ebenfalls erheblich, so daß die Ablösung des alten EDAS-Verfahrens durch das neue DEMOS-Verfahren entgegen der gesetzlichen Vorschrift bis zum 31. 12. 1987 nicht eingehalten wurde.

Nach letzten Zeitschätzungen aus dem Hause des Senators für Inneres soll das neue automatisierte Verfahren in der Zentrale, d. h. im Stadt- und Polizeiamt Bremen bis etwa Februar/März 1989, in den einzelnen Meldestellen bis etwa Ende 1989 eingeführt werden. Dies bedeutet, daß entgegen der klaren melderechtlichen Bestimmung ein inzwischen nicht mehr haltbares automatisiertes Datenverarbeitungsverfahren fast zwei Jahre über den gesetzlich bestimmten Termin hinaus benutzt wird, obwohl die Übergangsfrist (31. 12. 1987) durch den Gesetzgeber bereits einmal verlängert wurde.

Ich habe die Mißachtung des Meldegesetzes und die nicht genügende Umsetzung der Meldedatenübermittlungsverordnung gegenüber dem Senator für Inneres beanstandet.

— Regelmäßige Übermittlung von Meldedaten an die Finanzämter in Bremen

Am 13. 05. 1987 ist die Bremische Verordnung zur Durchführung des Meldegesetzes, insbesondere zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden (MeldDUV) in Kraft getreten. § 5 Abs. 2 dieser Verordnung erlaubt u. a. eine regelmäßige Übermittlung enumerativ aufgeführter Meldedaten in der Form des automatisierten Datenabrufs an die Finanzämter der Stadt Bremen **(online-Zugriff der bremischen Finanzämter in der Stadt Bremen auf das Melderegister der Stadtgemeinde Bremen).** Als Zweckbestimmung für diese regelmäßige Datenübermittlung hat der Verordnungsgeber die „Personen- und Adressenfeststellung im Rahmen des Besteuerungsverfahrens" bestimmt. Folgende Daten hat der Verordnungsgeber zur Übermittlung zugelassen:

1. Familiennamen (Familienname, Namensbestandteile des Familiennamens, Ehename, Namensbestandteile des Ehenamens)

2. Frühere Namen (Geburtsnamen, Namensbestandteile des Geburtsnamens, Familienname vor der Namensänderung, Namensbestandteile des Familiennamens vor Änderung)
3. Vornamen (gebräuchliche[r] Vorname[n])
4. Tag der Geburt
5. Geschlecht
6. Anschriften (Anschrift-PLZ, Anschrift-Wohnort, Anschrift-Straße, Anschrift-Hausnummer, Anschrift-Hausnummernzusatz, Wohnungsstatus — einzige Wohnung / Hauptwohnung / Nebenwohnung / künftige Wohnung nach Angabe des Einwohners bei der Abmeldung/Wohnung, in die der Einwohner laut Rückmeldung tatsächlich verzogen ist, Datum Wohnungsstatuswechsel, Zuzug von -PLZ, Zuzug von -Wohnort, Zuzug von -Straße, Zuzug von -Hausnummer, Zuzug von -Adressierungszusätze zur Hausnummer, Zuzug von -Wohnungsstatus, Zuzug von außerhalb des Melderechtsrahmensgesetzes, Fortzug nach außerhalb des Melderechtsrahmensgesetzes)
7. Tag des Ein- und Auszugs (Datum des Beziehens der Wohnung, Datum des Auszugs aus der Wohnung)
8. Sterbetag.

Voraussetzung für die Übermittlung von Meldedaten an andere Behörden und damit an die Finanzämter ist nach den melderechtlichen Bestimmungen (§ 30 Bremisches Meldegesetz), daß die Datenübermittlung u. a. zur rechtmäßigen Erfüllung der Aufgaben des Datenempfängers erforderlich ist. Als Rechtsnorm für den Übermittlungsanspruch der Finanzämter wird § 136 Abgabenordnung (AO) angeführt, der besagt, daß die Meldebehörden dem zuständigen Finanzamt für die Personenstandsaufnahme die ihnen nach den melderechtlichen Vorschriften bekanntgewordenen Änderungen in den Angaben nach § 135 AO (insbesondere Namen, Familienstand, Geburtsdatum, Geburtsort, Religionszugehörigkeit, Wohnsitz, Erwerbstätigkeit oder Beschäftigung) mitzuteilen haben. Der hier genannte Datenkatalog weicht von dem in der Meldedatenübermittlungsverordnung genannten Datenkatalog ab.

Das gegenwärtig angewendete EDAS-Verfahren des Stadt- und Polizeiamtes Bremen — Meldebehörde — beinhaltet verschiedene Transaktionen/Bildschirmformate (E 101 Rechercheauskunft, E 103 Kurzauskunft, E 105 Wohnverhältnisse, E 107 Sammelnamenauskunft, E 201 Gebäudeauskunft), mit deren Hilfe die Finanzämter in Bremen, die Oberfinanzdirektion Bremen (OFD) und die Landeshauptkasse über die installierten Datensichtgeräte auf das Bremische Melderegister direkt, d. h. online zugreifen können. Diesen Behörden stehen dabei sämtliche Einwohnerdatensätze des Bremischen Melderegisters in den bereitgestellten Bildschirmformaten zum Abruf zur Verfügung. Der zur Verfügung gestellte Datenkatalog enthält auch das melderechtliche Ordnungsmerkmal, das nach der geltenden Rechtslage (§ 4 Bremisches Meldegesetz, § 5 Abs. 2 und 3 MeldDÜV) nicht übermittelt werden darf. Die OFD ist als Datenempfänger in der Meldedatenübermittlungsverordnung überhaupt nicht genannt. Im derzeitig praktizierten EDAS-Verfahren können die OFD, die Finanzämter in Bremen und die Landeshauptkasse zudem unabhängig von ihrer jeweiligen Zuständigkeit auf sämtliche Datensätze des Bremischen Melderegisters, also weit mehr als nach §§ 135, 136 AO vorgesehen, zugreifen. Darüber hinaus wird das Ordnungsmerkmal entgegen der Rechtslage online zum Abruf bereitgehalten.

Dieses Verfahren, das bis Ende 1987 trotz in Kraft getretener MeldDÜV vielleicht noch auf die Übergangsregelung des § 38 Abs. 4 Bremisches Meldegesetz (Anpassung der automatisierten Meldeverfahren an das neue Melderecht bis spätestens Ende 1987) gestützt werden konnte, ist seit Anfang 1988 nicht mehr haltbar.

Ich habe dem Senator für Finanzen und dem Senator für Inneres meine datenschutzrechtlichen Bedenken vorgetragen und um Mitteilung der dortigen Rechtsauffassung gebeten. Im Einvernehmen mit dem Senator für Inneres hat mir der Senator für Finanzen mitgeteilt, daß er meine Rechtsauffassung nicht teilt. Er hält lediglich eine Anpassung der Auskunftsformate an den in der Meldedatenübermittlungsverordnung zugelassenen Datenumfang für notwendig. Diese Anpassung soll erst mit der Einführung des neuen DEMOS-Verfahrens erfolgen, d. h. erst Mitte bis Ende 1989. Damit wird ein mindestens seit Anfang 1988 rechtswidriger Zustand unverändert fortgeführt. Ich habe dies gegenüber dem Senator für Inneres beanstandet.

FFD 121/163

— **Erweiterte Melderegisterauskunft**

Aufgrund einer Bürgereingabe hatte ich mich mit der Frage zu befassen, was als „berechtigtes Interesse" für die Erteilung einer erweiterten Melderegisterauskunft gemäß § 32 Abs. 2 Bremisches Meldegesetz gelten kann.

Für eine erweiterte Melderegisterauskunft ist nach der Befugnisnorm des § 32 Abs. 2 Bremisches Meldegesetz ein „berechtigtes Interesse" glaubhaft zu machen. Diesem unbestimmten Rechtsbegriff „berechtigtes Interesse" ist aufgrund einer umfangreichen Rechtsprechung und einer gesicherten kasuistischen Interpretation dann genüge getan, wenn es sich um ein tatsächliches Interesse handelt. Danach kann dieses Interesse rechtlicher, wirtschaftlicher oder ideeller Natur sein. Soweit ein berechtigtes Interesse glaubhaft gemacht wird und die angeführten Gründe wirklich ausreichen, darf eine erweiterte Melderegisterauskunft gem. § 32 Abs. 2 Bremisches Meldegesetz jedoch nur dann erfolgen, soweit nicht Schutzrechte des Betroffenen beeinträchtigt werden.

Die Prüfung, ob die Voraussetzungen für eine erweiterte Melderegisterauskunft vorliegen, hat nach einschlägiger Kommentierung unter Abwägung des berechtigten Interesses des Auskunftssuchenden und der schutzwürdigen Belange des Betroffenen hinsichtlich jedes einzelnen Merkmals zu erfolgen und wird sich auch darauf zu beziehen haben, ob die begehrte Auskunft für den genannten Zweck überhaupt erforderlich ist.

Das Gesetz unterscheidet zwischen einfacher, erweiterter und Gruppenauskunft aus dem Melderegister. Während die einfache Melderegisterauskunft neben der Beachtung der Schutzrechte und der besonderen Ausschlußgründe von keinen weiteren Voraussetzungen abhängig ist, verlangt der Gesetzgeber für die erweiterte Melderegisterauskunft und darüber hinaus für jedes weitere Datum die Glaubhaftmachung eines berechtigten Interesses. Hieraus folgt, daß zwar z. B. Gläubiger, Wirtschaftsauskunfteien oder Inkassobüros für eine erweiterte Melderegisterauskunft in Frage kommen können, aber für jedes einzelne zusätzliche Datum und für jede einzelne bestimmte Person ein berechtigtes Interesse glaubhaft dargelegt werden muß. Eine generelle erweiterte Melderegisterauskunft kann nicht damit begründet werden, daß es sich um ein Massengeschäft handele und die Daten angeblich von geringer Sensibilität seien. Eine solche Wertung widerspricht der Wertung des Gesetzgebers.

Eine hohe Häufigkeit von erweiterten Melderegisteranfragen kann ein Indiz dafür sein, daß diese Daten zum Aufbau von multifunktionalen privaten Informationssystemen genutzt werden. Die Folge ist die Entstehung bzw. Fortschreibung tendenziell umfassender Datenbestände, deren Existenz das Persönlichkeitsrecht des Betroffenen verletzt bzw. verletzen kann. Selbst wenn einzelne Datenübermittlungen jeweils für sich betrachtet durchaus im Rahmen der gesteckten Grenzen bleiben, beeinträchtigt bereits die Tatsache der Speicherung und das mit ihr verbundene Mißbrauchsrisiko beim Datenempfänger das grundrechtlich geschützte informationelle Selbstbestimmungsrecht des Betroffenen. Daraus ergibt sich auch die Notwendigkeit, jeden Einzelfall der Datenübermittlung, vor allem an die Handels- und Wirtschaftsauskunfteien und Inkassobüros zu prüfen.

Der Senator für Inneres schloß sich meiner Rechtsauffassung nicht an, so daß die bremischen Meldebehörden weiterhin z. B. den Wirtschafts- und Handelsauskunfteien und Inkassobüros erweiterte Melderegisterauskünfte erteilen.

Wie dargelegt, ist neben der rechtlichen Problematik das Zweckbindungsprinzip nach § 32 Abs. 4 BrMeldG dadurch beeinträchtigt, daß die genannten Stellen die erlangten Meldedaten nicht nur für den Einzelfall, sondern für den Aufbau ihrer multifunktionalen Informationssysteme verwenden. Ich erwarte, daß der Senator für Inneres seinen Standpunkt überprüft.

5.3.2.2 Paß- und Ausweiswesen

Am 1. April 1987 ist das neue Bundespersonalausweisgesetz und dazu als ergänzende Vorschrift für das Land Bremen das Gesetz zur Ausführung des Gesetzes über Personalausweise in Kraft getreten.

Damit wird der fälschungssichere und maschinenlesbare 10,5 × 7,4 cm große Personalausweis auch im Land Bremen eingeführt.

Ich hatte bereits in meinem letzten Jahresbericht (9. Jahresbericht, Pkt. 5.2.2.2) darauf hingewiesen, inwieweit meine Bedenken und meine Anregungen zu dem Landespersonalausweisgesetz mit aufgenommen worden sind.

Ende des Jahres 1987 wurde bekannt, daß bei der Vergabe der neuen Personalausweise Seriennummern auch im Lande Bremen doppelt vergeben wurden.

Die Ursache für die Doppelvergabe der Seriennummern waren vielfältig: Einmal wurden von Ausweisbehörden die Listen mit den Seriennummern, wie sie die Bundesdruckerei zur Verfügung stellt, versehentlich doppelt verwendet oder es wurde bei der manuellen Bearbeitung vergessen, die vergebenen Seriennummern zu kennzeichnen. Ein anderes Mal erfolgte — außerhalb Bremens — die Doppelvergabe der Seriennummern bei der Umstellung vom manuellen zum automatisierten Verfahren.

Letztlich hätten solche Pannen vermieden werden können, wenn die Seriennummern statt durch die örtlichen Ausweisbehörden direkt bei der Herstellung der Ausweise durch die Bundesdruckerei vergeben würden. Aus der Sicht des Datenschutzes bestehen hiergegen keine Bedenken, weil es nach den gesetzlichen Bestimmungen (§ 3 Abs. 3 Personalausweisgesetz) zulässig ist, daß die Bundesdruckerei die vergebenen Seriennummern — ohne sonstige Ausweisdaten — zentral und dauerhaft speichert. Die Bundesdruckerei verfügt derzeit jedoch über keine Kontrollmechanismen, die eine Doppelvergabe von Seriennummern bereits bei der Herstellung der Ausweise feststellt und korrigiert; es sind lediglich Mechanismen für eine nachträgliche Feststellung von Doppelvergaben vorhanden.

Für die betroffenen Bürger kann dies — neben den Unannehmlichkeiten im Zusammenhang mit der behördlichen Aufforderung zur Rückgabe seines Ausweises — gravierende Folgen haben; kann er doch in den Verdacht des Ausweisdiebstahls oder Ausweismißbrauchs geraten und sich als „Fall" bzw. „Vorgang" in den polizeilichen Informationssystemen wiederfinden.

Die Datenschutzbeauftragten des Bundes und der Länder verlangen deshalb unisono, die Mechanismen zur Kontrolle einer Doppelvergabe von Seriennummern sowohl bei der Bundesdruckerei in Berlin wie auch bei den Ausweisbehörden zu verbessern.

5.3.3 Kfz-Zulassung/Führerschein

5.3.3.1 Kfz-Zulassung

— Änderung Straßenverkehrsgesetz, Fahrzeugregisterverordnung

Am 15. Februar 1987 trat das **Gesetz zur Änderung des StVG** (28. Januar 1987 — BGBl. I S. 486) in Kraft. Damit wurde zum einen für die örtlichen Fahrzeugregister der Zulassungsstellen und zum anderen für eine der größten Datenbanken in der BRD, das **Z**entrale **V**erkehrs-**I**nformations-**S**ystem (ZEVIS) beim Kraftfahrtbundesamt (KBA) eine datenschutzrechtliche bereichsspezifische Grundlage geschaffen (§§ 31 bis 47 StVG).

Mit Hilfe dieser gesetzlichen Regelung können von den Polizeien des Bundes und der Länder, vom Zoll und Grenzschutz sowie von den örtlichen Zulassungsstellen rund um die Uhr im Wege des Direktabrufs (online-Betrieb) die Daten der Fahrzeuge und ihrer Halter, die im Zentralen Fahrzeugregister beim KBA enthalten sind, sowie darüber hinaus denjenigen Teil des Verkehrszentralregisters, der den Entzug von Führerscheinen betrifft, abgefragt werden.

Die Gesetzesänderung sieht darüber hinaus auch Regelungen über die Verarbeitung der bei der Kraftfahrzeugzulassung erhobenen Daten in den örtlichen Fahrzeugregistern vor.

In meinem letzten Jahresbericht unter Pkt. 5.2.3.2 hatte ich bereits auf die von den Datenschutzbeauftragten des Bundes und der Länder vorgetragenen Kritik hinsichtlich des unverhältnismäßigen Eingriffs des Staates in das informationelle Selbstbestimmungsrecht hingewiesen. Auf diese Ausführungen wird verwiesen.

Das StVG enthält in einer Reihe von Punkten keine abschließenden Regelungen, sondern überläßt diese der auf der Ermächtigungsgrundlage in § 47 I StVG geschaffenen und am 20. Oktober 1987 in Kraft getretenen Fahrzeugregisterverordnung (FRV).

Mit der Verabschiedung dieser neuen Regelung wurden in keiner Weise die datenschutzrechtlichen Bedenken, die vom BfD und den LfD dargelegt worden sind, berücksichtigt; vgl. hierzu Anlage 6. Kritisiert wurde vor allem:

- daß, obwohl in der Begründung des Vorentwurfs ausdrücklich davon gesprochen wurde, daß der Gesetzgeber den Empfängerkreis für die ZEVIS-Übermitt-

lungen bewußt auf den Polizeivollzugsdienst habe beschränken wollen, die automatisierte Abrufmöglichkeit aus dem ZEVIS auf, die bei den Innenministern der Länder eingerichteten Lagezentren erweitert wurde. Dies ist durch die gesetzliche Ermächtigung in § 36 II 1 und III StVG nicht gedeckt.

- Eine konkrete Angabe des Anlasses eines Abrufes für den großen Bereich der Straftaten und Verkehrsordnungswidrigkeiten entfällt. Obwohl der § 36 VII StVG ausdrücklich von einer Erstreckung der Aufzeichnung auf den Anlaß des Abrufes spricht. Die Nachprüfbarkeit eines Abrufes wird durch die vorgenommene Änderung nicht mehr gewährleistet.

- Auch die Änderung des Umfangs der vorgesehenen Auswahlprotokollierung zur Feststellung des konkreten Anlasses der Abrufe und der für die Abrufe verantwortlichen Personen von 5 Prozent auf 2 Prozent der Fälle ist nicht durch den § 36 VII StVG abgedeckt. Bei einer solch geringen Prozentzahl handelt es sich nicht mehr um den „ausgewählten Teil" im Sinne dieser Bestimmung, der eine systematische Überprüfung und wirksame Kontrolle des Abfrageverhaltens der abrufberechtigten Dienststellen ermöglichen muß.

Trotz dieser fundamentalen Kritik der Datenschutzbeauftragten wurde die Entwurfsfassung der FRV in Kraft gesetzt. Somit werden neben der jetzt rechtlich abgesicherten langjährig vollzogenen Verwaltungspraxis außerdem noch völlig neue Datenzugriffe bzw. Datenverarbeitungen eröffnet.

Der Deutsche Bundestag hat im Zusammenhang mit den Beratungen des Gesetzentwurfs zur Änderung des Straßenverkehrsgesetzes am 5. Dezember 1986 eine Entschließung verabschiedet, in der die Bundesregierung aufgefordert wird, spätestens vier Jahre nach Inkrafttreten des Änderungsgesetzes unter Beteiligung des Bundesbeauftragten für den Datenschutz über die Erfahrungen zu berichten, die mit

— dem automatisierten Abrufverfahren,

— der Aufzeichnungspflicht,

— der sog. P-Anfrage (Personen-Anfrage) und

— der Einsichtnahme in die örtlichen Fahrzeugregister

gemacht worden sind. Eine entsprechende Bitte hat auch der Bundesrat in seiner Sitzung am 19. Dezember 1986 gegenüber der Bundesregierung geäußert. Der Bundesbeauftragte für den Datenschutz hat die Datenschutzbeauftragten der Länder gebeten, ihn bei seiner Beteiligung an diesem Bericht zu unterstützen; hierzu wurde eine Arbeitsgruppe eingerichtet, an der ich mich aus Gründen meiner Arbeitskapazität nicht beteiligen kann. Ob der Gesetz- bzw. Verordnungsgeber dazu zu bewegen ist, auf der Grundlage des Berichts Änderungen am Straßenverkehrsgesetz bzw. der Fahrzeugregisterverordnung vorzunehmen, bleibt abzuwarten. Die Änderungswünsche der Datenschutzbeauftragten bleiben jedenfalls auf der Tagesordnung.

— Datenübermittlung aus Kraftfahrzeugzulassungsdateien zum Zwecke der Verfolgung von Schwarzarbeit

Im Berichtszeitraum hatte ich mich mit der Frage zu beschäftigen, ob Auskünfte aus der Kfz.-Zulassungsdatei einmalig oder regelmäßig an die mit der Ermittlung von Schwarzarbeit betrauten Stellen (z. B. Handwerkskammer, Senator für Arbeit) erteilt worden sind.

Bei der Prüfung stellte sich heraus, daß die Ortspolizeibehörde Bremerhaven keine Daten aus der Zulassungsdatei übermittelt. Das Stadt- und Polizeiamt Bremen — Kfz-Zulassung — hat dagegen aufgrund schriftlicher Anfragen Halteranschriften an die Handelskammer Bremen übermittelt; als Nachweis für das berechtigte Interesse wurde die Begründung „Verfolgung von Schwarzarbeit" als ausreichend anerkannt. Als Rechtsgrundlage wurde vom Stadt- und Polizeiamt Bremen früher der § 26 Abs. 5 StVZO, nach Inkrafttreten der neuen Bestimmungen über die Fahrzeugregister § 35 Abs. 1 StVG angeführt.

Ich habe das Stadt- und Polizeiamt Bremen darauf hingewiesen, daß ich diese Rechtsauffassung nicht teile. Nach § 35 Abs. 1 Nr. 3 StVG dürfen Fahrzeug- und Halterdaten an Behörden und sonstige öffentliche Stellen übermittelt werden, wenn diese Übermittlung zur Verfolgung von Ordnungswidrigkeiten jeweils erforderlich ist. Nach § 2a Gesetz zur Bekämpfung der Schwarzarbeit, der durch das

FFD 12.163

Artikelgesetz zur Bekämpfung der illegalen Beschäftigung geändert wurde, regelt Landesrecht, welche Stelle für die Verfolgung und Ahndung von Ordnungswidrigkeiten zuständig ist. Gemäß § 10 der Bremischen Verordnung über die Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten sind das Stadt- und Polizeiamt Bremen bzw. die Ortspolizeibehörde Bremerhaven zuständige Verfolgungsbehörden; die Handwerkskammer oder Handelskammer Bremen besitzen hierfür keine sachliche Zuständigkeit. Die Übermittlung von Fahrzeug- und Halterdaten zum Zwecke der Verfolgung von Ordnungswidrigkeiten aus den Kfz-Zulassungsdateien an die Kammern sind — auf der Grundlage des § 35 Abs. 1 StVG — daher wegen fehlender Zuständigkeit dieser Einrichtungen nicht erforderlich und daher unzulässig.

Das Stadt- und Polizeiamt Bremen hat sich inzwischen meiner Rechtsauffassung angeschlossen.

Unbedenklich hingegen sind Hinweise dieser Einrichtungen auf Schwarzarbeit an die zuständigen Verfolgungsbehörden. Gemäß der Neufassung der gemeinsamen Verwaltungsvorschrift des Senators für Arbeit, des Senators für Wirtschaft und Außenhandel, des Senators für das Bauwesen, zur Bekämpfung der Schwarzarbeit im Handwerk (in der Fassung vom 11. März 1987, BremABl. S. 71) sollen, soweit Behörden (einschließlich Handwerkskammern) im Rahmen ihrer Tätigkeit auf Anhaltspunkte für Schwarzarbeit stoßen — soweit möglich — diese den Sachverhalt durch Vorermittlungen aufklären. Die Handwerkskammern können sich bei ihren Kontrollmaßnahmen auf die Auskunfts- und Beratungsbefugnisse nach § 17 Handwerksordnung stützen.

5.3.3.2 Führerschein

— Automatisierte Datenverarbeitung bei der Führerscheinstelle Bremen

Vom Senator für Inneres bin ich zur geplanten Einführung der automatisierten Datenverarbeitung in der Führerscheinstelle Bremen um Stellungnahme gebeten worden. Geplant ist, ein Fremdverfahren, nämlich das der Stadt Iserlohn, zu übernehmen.

Ich habe in meiner Stellungnahme gegen die Einführung der automatisierten Datenverarbeitung in der Führerscheinstelle Bremen keine grundsätzlichen Bedenken erhoben. Hinsichtlich des automatisierten Zugriffs dieses Verfahrens auf das Melderegister habe ich jedoch die gleichen Vorbehalte, die ich seinerzeit beim sog. FAZID-Verfahren (Kfz-Zulassung) vorgetragen habe, geltend gemacht. Vgl. diesbezüglich meine Ausführungen im 9. Jahresbericht unter Pkt. 5.2.2.1 (Meldedatenzugriffe der Kfz-Zulassungsbehörden).

Für Meldedatenzugriffe und -abrufe der Führerscheinstelle gilt, daß gegenwärtig weder das Bremische Melderecht noch die straßenverkehrsrechtlichen Vorschriften eine regelmäßige Übermittlung von Meldedaten durch automatisierten Direktzugriff bzw. -abruf zulassen. Aus der Sicht des Datenschutzes sind allein Einzelanfragen bei der Meldebehörde im Zusammenhang mit der Bearbeitung von Führerscheinanträgen unbedenklich, sofern bei der Führerscheinstelle Zweifel an der Identität oder an der Anschrift des Antragstellers bestehen. Automatisierte Lösungen, wie sie in Bremen geplant sind, stammen aus einer Zeit, als es noch kein Datenschutzrecht und kein neues Melderecht gab und als Integration und integrierte Datenverarbeitung Ziel aller Datenverarbeitungsentwicklungen war, funktionelle Trennung der Behörden und ihrer Datenverarbeitungsvorgänge sowie Zweckbindung der Daten hingegen noch keine große Rolle spielten.

Inzwischen sind aufgrund der Rechtsentwicklung integrierte Systemlösungen, wie sie das Iserlohner Verfahren darstellt, ohne weiteres nicht mehr möglich, obwohl die technologische Entwicklung in diese Richtung drängt. Derartige Lösungen werden im übrigen nur in Großstädten oder in kommunalen Gemeinschaftsrechenzentren realisiert, wo die Datenbestände sozusagen räumlich und/oder organisatorisch unter einem Dach verfügbar sind. Man muß hier auch berücksichtigen, daß die Führerscheindaten nicht nur innerhalb der Verkehrsbehörden ausgetauscht werden, sondern viele andere Stellen, z. B. Kraftfahrtbundesamt Flensburg, Polizei- und Sicherheitsbehörden, evtl. Kfz-Versicherungen, Private ebenfalls Auskünfte erhalten. Die technische Entwicklung birgt die große Gefahr in sich, daß die o. g. Stellen direkt auf öffentliche Datenbestände zugreifen können. Zugriffe des automatisierten Führerscheinverfahrens auf das Melderegister aktualisieren nicht nur die örtliche Führerscheindatei, sondern auch die Dateien der übrigen Stellen, die automatisiert auf das Führerscheinregister zugreifen können. Dem Zweckbindungsgedanken des Melde- und Datenschutzrechts würde dies zuwiderlaufen.

Ich habe in meiner Stellungnahme darauf hingewiesen, daß die Erforderlichkeit eines Zugriffs auf das Melderegister durch das Führerscheinverfahren bzw. durch die Führerscheinstelle kritisch zu prüfen ist. Führerscheinanträge können auch ohne Direktzugriff auf das automatisierte Melderegister und höchstens in Zweifelsfällen durch Rückfrage bei der Meldebehörde bearbeitet werden (z. B. durch Vorlage amtlicher Identitätspapiere).

— Interne Führerscheinkartei

Einige Bürger baten mich um Stellungnahme zu der Frage, ob nach 20 Jahren der Vermerk über den Entzug der Fahrerlaubnis nicht aus der internen Führerscheinkartei, die bei der Führerscheinstelle Bremen geführt wird, zu löschen sei.

Ungeachtet eines etwaigen Verwertungsverbotes ist schon die Speicherung dieser Angaben unzulässig. Sinn und Zweck der internen Führerscheinkartei nach § 10 StVZO ist eine Übersicht über alle Inhaber von Führerscheinen zu gewährleisten. Dem Sinn und Zweck widerspricht es, wenn über Name, Anschrift und ggf. Aushändigungsdatum hinaus weitere Angaben gemacht werden.

Intention des Gesetzgebers bei der Konzeption des Verkehrszentralregisters war es, die Masse der „örtlichen Verkehrssünderdateien" durch ein zentrales überregionales Register zu ersetzen.

Dementsprechend hätte die Behörde vor ihrer Entscheidung auf Erteilung einer Fahrerlaubnis die dafür notwendigen Auskünfte über vorhandene Eintragungen aus dem Verkehrszentralregister anfordern müssen. Die vorliegenden Fälle zeigen, daß die Tilgungsregelungen und damit die Verwertungsverbote durch die zusätzlichen Eintragungen in die interne Führerscheinkartei umgangen werden.

Ich halte diese Praxis für rechtswidrig und habe dies dem Stadt- und Polizeiamt Bremen mitgeteilt.

Das Stadt- und Polizeiamt Bremen will im Benehmen mit dem Senator für Inneres bis zur Klärung auf Bund-Länder-Ebene am bisher praktizierten Verfahren festhalten. Ich halte dies für unzulässig.

— Führerscheinakte

Immer wieder beklagen sich Bürger darüber, daß ihnen im Verfahren auf Wieder- bzw. Neuerteilung der Fahrerlaubnis sogenannte „alte Sünden" vorgeworfen werden.

Die alten Verkehrsstrafen, die zum Teil über 20 Jahre zurückliegen, die gemäß den Verjährungsfristen nach dem Bundeszentralregistergesetz aus dem Bundeszentralregister getilgt sind, die aber immer noch Bestandteil der örtlichen Führerscheinakte sind, werden von der Verwaltungsbehörde weiterhin für die Erteilung einer Fahrerlaubnis verwendet.

Dies widerspricht einem auf mein Betreiben hin ergangenen Erlaß des Senators für Inneres aus dem Jahre 1983, wonach der Bearbeiter einer Führerscheinakte bei jedem Ziehen dieser Akte tilgungsreife Vorgänge zu entfernen und zu löschen bzw. zu vernichten hat; sofern dies ausnahmsweise wegen der besonderen Art der Speicherung nicht möglich ist, hat der Bearbeiter die tilgungsreifen Daten z. B. durch Schwärzen unleserlich zu machen (vgl. hierzu meinen 5. Jahresbericht unter Pkt. 5.2.5.2 sowie die Stellungnahme des Senats vom 12. Juli 1983 zu meinem 5. Jahresbericht).

Der Datenschutzausschuß der Bremischen Bürgerschaft hat in seinem von der Bremischen Bürgerschaft zustimmend zur Kenntnis genommenen Bericht zu meinem 5. Jahresbericht (vgl. Drucksache 10/1173 vom 2. August 1983) zu dieser Angelegenheit wie folgt formuliert:

„Die beabsichtigte Verfahrensregelung für die Tilgung bzw. Nichtverwertung von Eintragungen bei den Führerscheinstellen wird begrüßt und sollte so bald wie möglich durch eine vollständige Bereinigung der Akten abgelöst werden."

Ich stelle fest, daß weder der Erlaß des Innensenators beachtet wird noch die vollständige Aktenbereinigung durchgeführt ist.

Ich prüfe gegenwärtig, ob ich — erstmals — von der neuen Möglichkeit des § 38 BrDSG (Einleitung eines OWI-Verfahrens) Gebrauch machen soll.

5.3.4 Amtliche Statistik

5.3.4.1 Volkszählung 1987

Herausragendes Ereignis im Berichtsjahr — und mit erheblicher Arbeitsbelastung für meine Dienststelle verbunden — war die Durchführung der Volkszählung 1987. Vor allem nach Beginn der sogenannten Haupterhebung setzte ein Sturm von schriftlichen, mündlichen und vor allem telefonischen Anfragen und Eingaben bei mir ein. In den Tagen vor und nach dem Erhebungsstichtag waren alle meine Mitarbeiter einzig und allein mit der Beantwortung derartiger Anfragen und Eingaben beschäftigt. Die meisten dieser Anfragen und Eingaben beschäftigten sich mit der Rechtmäßigkeit der Zählung, mit den Fragen in den Erhebungsbögen, mit dem Zählereinsatz, mit der Art und Weise der Auskunftserteilung, mit der Aushändigung der Erhebungsunterlagen an Nachbarn oder minderjährige Kinder, mit den Folgen einer etwaigen Auskunftsverweigerung und mit der Gewährleistung des Datenschutzes (Anonymität) und der Datensicherung.

Zu einigen dieser Fragen möchte ich mich hier äußern. Das Volkszählungsgesetz 1987 erfüllt nach meiner Auffassung die Anforderungen, die das Bundesverfassungsgericht in seinem Urteil zum Volkszählungsgesetz 1983 aufgestellt hat. Verschiedene Verfassungsbeschwerden gegen das Volkszählungsgesetz 1987 wurden vom Bundesverfassungsgericht nicht zur Entscheidung angenommen, weil sie keine Aussicht auf Erfolg hätten. Dabei hat das Verfassungsgericht zu erkennen gegeben, daß es die in der Öffentlichkeit erhobenen verfassungsrechtlichen Bedenken gegen das Volkszählungsgesetz 1987 für unbegründet hält. Besondere Bedeutung kommt dem Hinweis des Gerichts zu, daß es Aufgabe der unabhängigen Datenschutzbeauftragten und der Verwaltungsgerichte sei, den Bürger vor unzulässigen Maßnahmen bei der Durchführung der Volkszählung zu schützen. Wichtig ist auch der Hinweis des Gerichts, daß die statistischen Ämter für jede einzelne Erhebungsunterlage den frühestmöglichen Zeitpunkt der Vernichtung bzw. Löschung zu bestimmen haben und entsprechend verfahren müssen. Die von den statistischen Ämtern festgelegte Organisations- und Ablaufstruktur für die Datenerhebung und Datenaufbereitung seien nicht als verbindliche Vorgabe zu betrachten.

Sehr viele Bürgereingaben und -beschwerden richteten sich gegen den Zählereinsatz in unmittelbarer Wohnungsnähe. Ich habe eine Vielzahl derartiger Eingaben sowohl in Bremerhaven als auch in Bremen überprüft und festgestellt, daß die von den Statistikern selbst gesetzte Bedingung, wonach zwischen der Wohnung eines Auskunftspflichtigen und derjenigen des Zählers mindestens ein Zählbezirk (= ein Straßenabschnitt/Baublock) liegen muß, offensichtlich nicht abgewichen wurde. Dem Senator für Inneres und den beiden Erhebungsstellen habe ich jedoch mitgeteilt, daß ich die Auffassung der Petenten teile, daß der Abstand von einem Zählbezirk zwischen Zähler und Gezähltem in einer städtischen Verdichtungsituation zu gering sei, um die Absicht des Gesetzgeberes bei der Regelung des § 10 Abs. 5 Volkszählungsgesetz 1987 zu erfüllen. Besser wäre gewesen, als Abstandskriterium den Arbeitsbezirk zu wählen, der sich in der Regel aus mehreren Zählbezirken zusammensetzt. Den Petenten habe ich meine Auffassung ebenfalls mitgeteilt. Einen Anlaß für eine förmliche Beanstandung habe ich in dieser Sache nicht gesehen.

Viele Beschwerden richteten sich auch gegen die Aushändigung der Zählunterlagen an Nachbarn, minderjährige Kinder oder unbeteiligte Besucher von Auskunftspflichtigen. Einen Datenschutzverstoß habe ich hierin nicht gesehen. Gleichwohl habe ich Verständnis für die besorgten Bürger gehabt, die als Auskunftspflichtige selbst die Erhebungsunterlagen entgegennehmen und dem Zähler die erforderlichen Angaben machen wollten.

Einige Beschwerden erhielt ich auch wegen eines behaupteten Verstoßes gegen das Adoptionsgeheimnis. Eltern, die ein Kind mit dem Ziel der Adoption in Pflege nehmen, vertrauen darauf, daß das vom Bundesgesetzgeber sehr stringent geregelte Adoptionsgeheimnis von den beteiligten Behörden beachtet wird. Im Melderegister wird in solchen Fällen beim Kind eine sogenannte Auskunftssperre eingetragen, die verhindern soll, daß in diesen Fällen eine Melderegisterauskunft erteilt wird (§ 32 Abs. 7 Bremisches Meldegesetz). Diese Bestimmung verhindert allerdings nicht, daß innerbehördlich Daten weitergegeben werden, die Schlüsse auf eine Adoptionspflegschaft zulassen. Die Regelung betrifft lediglich die Datenübermittlung an Personen und private Stellen.

Die Meldebehörden waren gemäß § 11 Abs. 1 Volkszählungsgesetz 1987 verpflichtet, auf Anforderung den Erhebungsstellen zur Organisation der Zählung Einwoh-

nerdaten zu übermitteln. In **Bremen** wurden zu diesem Zweck im Rechenzentrum der bremischen Verwaltung stichtagsbezogene Magnetbandabzüge mit den zulässigen Einwohner- und Gewerbemeldedaten erstellt und diese Bandabzüge für Zwecke der Erhebungsstelle Bremen bereitgehalten. Die Erhebungsstelle Bremen hat die für ihre Zwecke erforderlichen Listen (Begehungslisten, Stichtagslisten) aufbereiten und drucken lassen. Bei Adoptionspflegefällen wurde das Merkmal „Auskunftssperre" überlesen mit der Folge, daß diese Fälle sowohl in der Stichtagsliste als auch in den Begehungslisten ohne speziellen Hinweis enthalten waren. Aus den übermittelten Namen konnten die Erhebungsstelle bzw. die eingesetzten Zähler nicht eindeutig erkennen, daß es sich um eine Adoptionspflegschaft handelt. Namensunterschiede — auch bei Kleinkindern — können viele Ursachen haben und müssen nicht unbedingt auf eine Adoptionspflegschaft hindeuten. Obwohl aus der Sicht der betroffenen Eltern diese „Durchbrechung" des Adopitionsgeheimnisses mehr als ärgerlich war, vor allem, wenn ein bekannter Zähler vor der Tür stand, habe ich diesen Vorgang für Bremen nicht als Datenschutzverstoß beanstandet. Gleichwohl zeigt dieser Vorgang, daß das vom Bundesgesetzgeber im Bürgerlichen Gesetzbuch sehr restriktiv geregelte Adoptionsgeheimnis im Melderecht nur unzulänglich umgesetzt worden ist. Deshalb werde ich dem Gesetzgeber empfehlen, das Adoptionsgeheimnis auch bei der innerbehördlichen Übermittlung von Meldedaten zu verwirklichen.

In **Bremerhaven** enthielt die Begehungsliste in diesen Fällen zusätzlich den Hinweis „A" (= Auskunftssperre), ohne daß die Zähler über die Bedeutung dieses Hinweises aufgeklärt wurden. Die Übermittlung des Merkmals „A" = Auskunftssperre an die Erhebungsstelle war nach dem Volkszählungsgesetz 1987 nicht zulässig, da dieses Merkmal in § 11 Abs. 1 Volkszählungsgesetz nicht genannt ist. Formal liegt damit ein Verstoß gegen § 11 Abs. 1 Volkszählungsgesetz 1987 vor. Im Hinblick auf den Schutzzweck, den das Merkmal „A" in diesen Fällen erfüllen soll, stellt sich die Frage, ob die unzulässige Übermittlung dieses Merkmals als Datenschutzverstoß beanstandet werden muß. Angesichts der Tatsache, daß in Bremerhaven ebenso wie in Bremen die Zähler durchweg zu dicht an ihrer Wohnung eingesetzt wurden und vielfach nachbarschaftliche Bekannschaften zwischen Zähler und Gezähltem vorhanden waren, ist dies als Datenschutzverstoß zu behandeln.

Im Herbst des letzten Jahres fand in Bremen und Bremerhaven eine Wiederholungsbefragung zur Volkszählung 1987 statt (0,2 Prozent Stichprobe). Eine solche Wiederholungsbefragung hat der Gesetzgeber zur Prüfung der Zuverlässigkeit der Ergebnisse zugelassen (§ 1 Abs. 4 Volkszählungsgesetz 1987). Als Zähler wurden hierbei Mitarbeiter des Statistischen Landesamtes eingesetzt; die Durchführung dieser Befragung entsprach weitgehend der Durchführung der Haupterhebung. In Bremen waren vier Arbeitsbezirke à 80 Haushalte (Wohnheime und Anstalten ausgenommen) betroffen, in Bremerhaven 60 Haushalte. Bei der Wiederholungsbefragung wurden ein Haushaltsmantelbogen und ein Personenbogen mit einem eingeschränkten Fragenkatalog verwendet.

Die Wiederholungsbefragung hat das Ziel, die Zuverlässigkeit der Volkszählungsergebnisse zu prüfen. Sie hat nicht das Ziel, die Angaben der betroffenen Auskunftspflichtigen bei der Haupterhebung zu kontrollieren und im Abweichungsfall womöglich ein Bußgeldverfahren einzuleiten. Um dies zu erreichen, haben die statistischen Ämter zugesichert, daß vor dem Vergleich der Ergebnisse der Wiederholungsbefragung mit denjenigen der Haupterhebung die Erhebungsunterlagen der Wiederholungsbefragung einschließlich der Hilfsmerkmale (Name, Vorname, Ordnungsnummer) gelöscht bzw. vernichtet werden.

Die Zählung ist in Bremen und Bremerhaven noch nicht abgeschlossen. In Bremen läuft gegenwärtig (März 1988) die Erinnerungs- und Mahnaktion für die eigentliche Volkszählung (Arbeitsstättenzählung zunächst ausgenommen). Im Rahmen dieser Aktion wurden über 75 000 Erinnerungs- und Mahnschreiben verschickt, die in einem rein manuellen Verfahren aufbereitet und versandfertig gemacht wurden. Das speziell für diesen Zweck entwickelte Datenverarbeitungsverfahren wurde nicht angewendet. Erinnert und gemahnt wurden alle diejenigen Fälle, bei denen nach der Begehungs- und Stichtagsliste die Erhebungsunterlagen, d. h. ausgefüllte Haushaltsmantelbögen, Personenbögen, Wohnungsbögen noch fehlten.

In diesem Zusammenhang erreichten mich wiederum eine ganze Reihe von Eingaben und Beschwerden, in denen die Betroffenen erklärten, die Erhebungsunterlagen bereits ausgefüllt und zurückgeschickt oder noch nie derartige Unterlagen erhalten zu haben. Diese Eingaben, die ich zum Teil in der Erhebungsstelle Bremen

überprüft habe, bringen mich zu der Feststellung, daß die Durchführungsorganisation der Volkszählung in Bremen höchst fehleranfällig und pannenträchtig gestaltet ist und sich hieraus auch Datenschutzprobleme für den Bürger ergeben (z. B. korrekte Verbuchung der eingehenden ausgefüllten Erhebungsunterlagen mit Entlastung des Bürgers von seiner Auskunftspflicht, richtige Zuordnung dieser Unterlagen zu den Zähl- und Arbeitsbezirken, Kontrolle der Zähler hinsichtlich der termingerechten und vollständigen Rückgabe der Zählungspapiere). Dies bestätigt auch der Fall eines „säumigen" Zählers, der in der örtlichen Presse ausführlich und im wesentlichen richtig dargestellt wurde. Meine Prüfung dieses Falles hat ergeben, daß der Zähler tatsächlich erst Anfang März dieses Jahres die bei ihm befindlichen Zählungsunterlagen bei der Erhebungsstelle Bremen abgegeben hat, mehr als sieben Monate nach Ablauf des Abgabezeitraums. Die vom Zähler verspätet abgelieferten Zählungsunterlagen fehlten in der Zählungsmappe des entsprechenden Arbeitsbezirks, ohne daß dies der Erhebungsstelle Bremen aufgefallen ist. Auch bei der Abrechnung der Zählerentschädigung ist dies der Erhebungsstelle nicht aufgefallen, eine Rückfrage beim „säumigen" Zähler war nicht vorgenommen worden. Bei der Erhebungsstelle Bremen sind — wie dieser Fall exemplarisch nochmals deutlich macht — bei der Durchführung der Zählung, insbesondere bei der Rücklaufkontrolle der Erhebungsunterlagen und der Überwachung der Zählertätigkeit erhebliche Pannen und Probleme aufgetreten. In diesem Fall hat die Erhebungsstelle Bremen § 3 der bremischen Verordnung zur Durchführung der Volkszählung nicht sorgfältig beachtet. Der Zähler hat gegen seine Pflichten (§ 10 VZG 1987, § 6 Durchführungsverordnung) verstoßen, was sich die Erhebungsstelle Bremen zurechnen lassen muß. Das Statistische Landesamt Bremen beabsichtigt, gegen den „säumigen" Zähler Strafantrag zu stellen. Ich werde nach Vorlage der schriftlichen Stellungnahme der Erhebungsstelle Bremen zu entscheiden haben, ob ich von meinen datenschutzrechtlichen Sanktionsmöglichkeiten Gebrauch mache.

Das Erinnerungs- und Mahnverfahren für die Arbeitsstättenzählung soll in Bremen erst nach dem Verschicken der Heranziehungsbescheide (sofern es dazu kommt) bzw. nach Abschluß der laufenden Erinnerungs- und Mahnaktion erfolgen. In Bremerhaven wurde die Erinnerungs- und Mahnaktion sowohl für den Bereich der eigentlichen Volkszählung als auch für den Bereich der Arbeitsstättenzählung bereits im Januar 1988 abgeschlossen. Heranziehungsbescheide wurden bisher (März 1988) in Bremen und Bremerhaven nicht verschickt. Praktisch bedeutet dies, daß die Datenerhebung bei den Bürgern bis heute noch nicht abgeschlossen ist. Datenschutzrechtlich stellt sich deshalb die Frage, wie lange die stichtagsbezogene Auskunftspflicht eines Bürgers noch andauert und inwieweit inzwischen Erinnerungslücken und Veränderung der tatsächlichen Verhältnisse dazu führen, daß etwas Unmögliches vom Bürger verlangt wird und die Auskunftspflicht deshalb verwirkt sein kann.

Das Volkszählungsgesetz 1987 bietet den Erhebungsstellen in § 11 Abs. 1 Satz 2 mit der sogenannten Ersatzvornahme ein Instrument, um zumindest für die Personenzählung von allen gemeldeten auskunftspflichtigen Personen die statistischen Grunddaten zu erlangen. Für die anderen Zählungsteile hat der Gesetzgeber ein solches Instrument nicht für notwendig erachtet. Ich habe Zweifel, ob die Auskunftspflicht des Volkszählungsgesetzes 1987 (von Wiederholungsbefragungen gem. § 1 Abs. 4 Volkszählungsgesetz abgesehen) wesentlich über den Zeitraum eines Jahres nach Zählungsstichtag noch andauert.

5.3.4.2 Bevölkerungsfortschreibung nach der Volkszählung 1987

Nach dem Gesetz über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes haben die Statistischen Ämter des Bundes und der Länder den Bevölkerungsstand auf der Grundlage der jeweils letzten allgemeinen Zählung der Bevölkerung fortzuschreiben. Der Bevölkerungsstand selbst wird aufgrund der Statistik der natürlichen Bevölkerungsbewegung (z. B. Geburten, Todesfälle, Eheschließungen) sowie der Wanderungsstatistik (z. B. An- und Abmeldungen, Zu- und Fortzüge) ermittelt und kontinuierlich amtlich festgestellt.

Die Fortschreibung des Bevölkerungsstandes dient dazu, die Ergebnisse der Bevölkerungsstatistik und der Volkszählung 1987 zahlenmäßig anzugleichen.

Die Wanderungsstatistik speist sich aus den Durchschlägen der Meldescheine, die nach der bestehenden Rechtslage an das Statistische Landesamt zu übersenden sind. Zur korrekten Fortschreibung der statistischen Zahlenwerte beabsichtigt das Statistische Landesamt Bremen, durch die Meldebehörde zusätzliche Daten für

statistische Zwecke auf freiwilliger Grundlage erheben zu lassen. Auf einem Beiblatt zu den Meldeformularen sollen bei der An-, Ab- oder Ummeldung folgende zusätzliche Daten vom meldepflichtigen Bürger erhoben werden:

„Wenn schon vor dem 1. Mai 1983 (Zeitpunkt der Einführung des neuen Meldegesetzes) mehrere Wohnungen bestanden und wenn seit diesem Zeitpunkt keine Veränderung (An- oder Abmeldung, Wechsel der Hauptwohnung) eingetreten ist, dann bitte ausfüllen.

1. Wenn Sie verheiratet sind und nicht dauernd getrennt leben: Welches war die vorwiegend benutzte Wohnung der Familie?
2. Für alle übrigen Personen: Welches war Ihre vorwiegend benutzte Wohnung?"

In meiner Stellungnahme zu dieser neuen Datenerhebung für statistische Zwecke im Zusammenhang mit einem Meldevorgang habe ich darauf hingewiesen, daß die der Wanderungsstatistik und der Bevölkerungsfortschreibung zugrundeliegende statistische Rechtsvorschrift die Anforderungen des Volkszählungsurteils aus dem Jahre 1983 nicht erfüllt und dringend novelliert werden muß. Die Auffassung vertrete ich seit Jahren (vgl. meine diesbezüglichen Ausführungen in meinem 7. Jahresbericht unter Pkt. 5.2.1.1).

Für besonders problematisch halte ich die Tatsache, daß bei dieser statistischen Datenerhebung Verwaltungsvollzug (Meldeangelegenheiten) und Statistik „vermischt" sind, also keine klare Trennung zwischen diesen Bereichen besteht. Eine solche klare Trennung wird aber vom Bundesverfassungsgericht zur Gewährleistung des Statistikgeheimnisses und zur Sicherung des Rechts auf informationelle Selbstbestimmung für unerläßlich gehalten (informationelle Gewaltenteilung). Grundsätzlich ist für die Übermittlung von personenbezogenen Daten an die amtliche Statistik für statistische Zwecke eine normenklare, präzise gesetzliche Grundlage erforderlich. An einer solchen Rechtsgrundlage mangelt es in diesem Fall.

In der Erwiderung auf meine Stellungnahme teilte der Senator für Inneres mir mit, daß er meine datenschutzrechtlichen Bedenken hinsichtlich der Durchführung dieser zusätzlichen Datenerhebung für statistische Zwecke bei den genannten Meldevorgängen nicht teilt.

Diese Antwort des Senators für Inneres ist nach der Rechtsprechung des Bundesverfassungsgerichts nicht haltbar. Sollte diese Statistik unverzichtbar sein, so ist eine verfassungskonforme Rechtsgrundlage erforderlich.

5.3.5 Personenstandswesen

Änderung Personenstandsgesetz

Nach der derzeitigen Rechtslage und Verwaltungspraxis übermitteln die Standesämter öffentlichen Stellen in einer Vielzahl von Fällen Personenstandsdaten. Grundlage hierfür ist die Allgemeine Verwaltungsvorschrift zum Personenstandsgesetz (Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden; Stand: 23. November 1987). Gerade die Übermittlung personenbezogener Daten aus dem Bereich des Personenstandswesens stellt i. d. R. einen Eingriff in die grundrechtlich geschützte Sphäre der Betroffenen dar. Seit langem fordern die Datenschutzbeauftragten für diese Eingriffe in das informationelle Selbstbestimmungsrecht eine präzise gesetzliche Grundlage.

Unter Federführung des BMI wird derzeit eine umfassende Novellierung des Personenstandsgesetzes vorbereitet.

Gegenüber dem geltenden Recht enthält der Vorentwurf eines Fünften Gesetzes zur Änderung und Ergänzung des Personenstandsgesetzes (5. PStÄndG) deutliche datenschutzrechtliche Verbesserungen.

Als positiv zu bewerten ist insbesondere die Absicht,

— die Mitteilungspflichten des Standesbeamten gesetzlich zu verankern (§ 66),

— die Einsicht in der Personenstandsbücher und die Erteilung von Auskünften und Urkunden präziser zu regeln (§§ 61 ff.), insbesondere eigenständige Vorschriften über die Auskunft bzw. Einsicht für Zwecke wissenschaftlicher Forschung zu schaffen (§ 61 b),

— das öffentliche Aufgebot wegfallen zu lassen (Streichung des geltenden § 3 PStG, Änderung des Ehegesetzes durch Art. 2 des Entwurfs).

Ein von den Datenschutzbeauftragten des Bundes und der Länder eingesetzter Arbeitskreis Personenstandswesen hat sich mit dem Vorentwurf dieses Gesetzes befaßt und in einer Stellungnahme folgende wesentliche Punkte hervorgehoben:

— Eine standesamtliche Herausgabe personenbezogener Daten zur Veröffentlichung von Personenstandsfällen darf der Standesbeamte grundsätzlich nur dann vornehmen, wenn der Betroffene eingewilligt hat.

— Auf die Eintragung des Berufes des Eheschließenden und der Zeugen ins Heiratsbuch soll verzichtet werden.

— Eine Gewährung von Auskunft und Einsicht darf nicht routinemäßig erfolgen, sondern nur auf Ersuchen im Einzelfall, ein Direktzugriff auf Personenstandseintragungen ist dementsprechend auszuschließen.

— Die Gewährung von Informationen an Behörden und bestimmte sonstige Stellen sollte an die gleichzeitige Benachrichtigung des Betroffenen gebunden werden.

— Die Gewährung von Informationen zum Zwecke wissenschaftlicher Forschung sollte durch gesetzliche Vorschriften bereichsspezifisch geregelt werden.

— Die Sterbeurkunden sollten so gefaßt werden, daß sie Dritten keinen Anlaß zu Spekulationen über die näheren Umstände des Todes geben. Für Orts- bzw. Zeitangaben in Urkunden, namentlich Sterbeurkunden, sollte eine Regelung vorgesehen werden, durch die Peinlichkeiten für die Betroffenen vermieden werden.

— Es sollte eine verordnungsmäßige Regelung etwaiger regelmäßiger automatisierter Datenübermittlungen zur Erfüllung der gesetzlich festzulegenden Mitteilungspflichten erfolgen.

— Ein Schutz von Informationen über Adoption bei Mitteilungen an Meldebehörden sollte sichergestellt werden (Wahrung des Adoptionsgeheimnisses).

Wichtig erscheint, daß die Rahmenbedingungen für die Einwilligung gesetzlich festzulegen sind und klarzustellen ist,

— in welchen Fällen,

— in welchem Umfang,

— unter welchen Voraussetzungen

die Veröffentlichung von Personenstandsdaten in Betracht kommen.

Ich erwarte, daß der Gesetzgeber die Anregungen des Arbeitskreises berücksichtigt.

5.3.6 Datenverarbeitung bei der Beitragserhebung durch die Deichverbände

Die Deichverbände haben im Einvernehmen mit dem Senator für Inneres und mir die notwendige Auslegung von Beitragsbuch und Hebeliste für die Beitragserhebung satzungsrechtlich so geregelt, daß die Offenlegung fremder Daten ausgeschlossen ist. Danach gewähren die Deichverbände ihren Mitgliedern nur noch insoweit eine Einsichtnahme in das Beitragsbuch, als es die sie selbst betreffenden Daten angeht. Die personenbezogenen Daten anderer Mitglieder werden während der Einsichtnahme abgedeckt.

Nachdem sich jedoch einige Verbandsmitglieder dagegen beschwert haben, daß ihnen eine Einsicht in die Daten anderer Mitglieder verwehrt worden ist, habe ich auf Bitten der Deichverbände eine datenschutzrechtliche Stellungnahme folgenden Inhalts abgegeben:

Das von einzelnen erbetene Recht, das gesamte Beitragsbuch einzusehen oder aber Auszüge aus dem Beitragsbuch zu bekommen, stellt eine Übermittlung personenbezogener Daten an Dritte durch eine öffentliche Stelle dar, die nach dem Volkszählungsurteil des Bundesverfassungsgerichts nur aufgrund einer den verfassungsgemäßen Prinzipien der Normenklarheit, Zweckbindung und Verhältnismäßigkeit entsprechenden bereichsspezifischen Rechtsgrundlage zulässig ist, da sie das Recht des Betroffenen auf informationelle Selbstbestimmung einschränkt.

Als bereichsspezifische Regelungen kommen das Gesetz über Wasser- und Bodenverbände vom 10. Februar 1937 und die dazu ergangene Erste Wasserverbandsordnung vom 3. September 1937 in Frage. Das Gesetz über Wasser- und Boden-

verbände enthält weder datenschutzrechtliche Vorschriften noch eine Ermächtigung für den Verordnungsgeber, in einer Verordnung entsprechende Vorschriften aufzunehmen. Der 7. Abschnitt dieser Ersten Wasserverbandsordnung enthält Vorschriften über die Festsetzung der Beiträge von Mitgliedern und Nutznießern und Verfahrensvorschriften für die Festsetzung und Hebung dieser Beiträge. In der Kommentierung und Rechtsprechung zum 7. Abschnitt der Ersten Wasserverbandsordnung werden die darin enthaltenen Verfahrensvorschriften, die ein zweistufiges Verfahren vorsehen, nämlich die Erstellung eines Beitragsbuches und einer Hebeliste dahingehend ausgelegt, daß diese den Mitgliedern Gelegenheit geben sollen zu kontrollieren, ob die für sie ferstgesetzten Beiträge in einem Verhältnis zu denen der übrigen Verbandsmitglieder veranlagt worden sind, das in etwa den tatsächlich erlangten Vorteilen entspricht, und ob ihre Daten und ihr Beitragsverhältnis zutreffend ausgeworfen sind.

Ebenso sollen sie eine Kontrollmöglichkeit bieten, um offensichtliche Unrichtigkeiten (z. B. Rechenfehler) feststellen zu können. Daraus wird der Schluß gezogen, daß den einzelnen Mitgliedern das gesamte Beitragsbuch und die gesamte Hebeliste, also auch die personenbezogenen Daten der übrigen Verbandsmitglieder, zur Einsichtnahme zur Verfügung stehen müssen.

Bei dem Gesetz über Wasser- und Bodenverbände und der Ersten Wasserverbandsverordnung handelt es sich um vorkonstitutionelles Recht, das durch die Bestimmungen des Art. 123 GG fortgilt. Das Bundesverfassungsgericht hat in ständiger Rechtsprechung zu solchem Recht entschieden, daß einzelne Vorschriften solchen Rechts dann als nichtig angesehen werden müssen, wenn einzelne Vorschriften in so krassem Widerspruch zu der heutigen Rechtsordnung stehen, daß ihre Rechtsfolgen als Unrecht anzusehen sind. Davon ist grundsätzlich auszugehen, wenn es sich um Vorschriften handelt, die einen Eingriff in ein Recht von Verfassungsrang, wie hier dem informationellen Selbstbestimmungsrecht, beinhalten. Das gilt insbesondere, wenn wie hier eine untergesetzliche Norm einen Eingriff in Grundrechtspositionen darstellt. Sollte hier das Entstehen eines rechtsfreien Raumes gesehen werden, kann dieses nicht dazu genutzt werden, der Verwaltung eine so weitgehende Eingriffsmöglichkeit in das informationelle Selbstbestimmungsrecht zu gewähren, zumal dieses im vorliegenden Falle auch nicht unerläßlich für den Schutz öffentlicher Interessen ist. Es kann auch nicht außer Acht bleiben, daß der Gesetzgeber inzwischen ausreichend Gelegenheit hatte, diese Vorschriften unserer heutigen Rechtsordnung anzugleichen.

Will man dem nicht folgen, ist die mit der totalen Offenlegung von Beitragsbuch und Hebeliste verbundene Übermittlung personenbezogener Daten von einer öffentlichen Stelle an dritte nicht-öffentliche Stellen oder Personen auch aus anderen Gründen unzulässig. Die vorher zitierten Vorschriften der Ersten Wasserverbandsordnung erfüllen nämlich nicht das vom Bundesverfassungsgericht geforderte Gebot der Normenklarheit. § 87 der Ersten Wasserverbandsordnung bestimmt lediglich, daß der Vorsteher des Wasser- und Bodenverbandes den beitragspflichtigen Mitgliedern das ermittelte Beitragsverhältnis (Beitragsbuch) in der nach der Satzung vorgeschriebenen Weise bekannt gibt. Für die Hebeliste gilt diese Vorschrift entsprechend. Die Betroffenen können der Vorschrift nicht erkennbar entnehmen — auch nicht aus dem Gesetzeszusammenhang, in dem dieser Text steht —, ob und inwieweit ihre personenbezogenen Daten an Dritte übermittelt werden.

Diese Vorschriften der Ersten Wasserverbandsordnung erfüllen nicht den Grundsatz der Verhältnismäßigkeit. Nach diesem Verfassungsgrundsatz darf der Gesetzgeber das informationelle Selbstbestimmungsrecht nur soweit beschränken, als es zum Schutz öffentlicher Interessen unerläßlich ist. Dabei müssen die personenbezogenen Daten, deren Verarbeitung als zulässig bestimmt wird, für die Erreichung des Zweckes geeignet und erforderlich sein.

Wie bereits erwähnt, soll die totale Offenlegung von Beitragsbuch und Hebeliste der verbandsinternen Kontrolle dienen. Das einzelne Verbandsmitglied soll feststellen können, ob es im Verhältnis zu den übrigen Verbandsmitgliedern richtig veranlagt worden ist, ob die Berechnungen offensichtliche Unrichtigkeiten (z. B. Rechenfehler) enthalten und ob seine Daten zutreffend ausgeworfen worden sind. Die Offenlegung aller personenbezogenen Daten der übrigen Mitglieder ist für die Erreichung dieser Zwecke weder geeignet noch erforderlich.

Die mangelnde Eignung dieser Form der Datenübermittlung für den Zweck der Kontrolle der Angemessenheit des Beitrages ergibt sich allein daraus, daß den

Deichverbänden in Bremen ca. 80 000 Mitglieder angehören. Es wird dem einzelnen Mitglied in aller Regel praktisch unmöglich sein, sich für eine so große Zahl von Grundstücken hinreichende Informationen zu beschaffen, die eine gesicherte Erkenntnis über den Vorteil zulassen, der diesen Mitgliedern aus der Aufgabe des Deichverbandes erwächst.

Die Offenlegung der personenbezogenen Daten aller Mitglieder ist für diesen Zweck auch nicht erforderlich.

Die von Kommentierung und Rechtsprechung verlangte Binnenkontrolle kann für diesen Zweck mit anderen Mitteln, die eine so weitgehende Einschränkung des informationellen Selbstbestimmungsrechts der Mitglieder nicht erfordert, zumindest ebenso gut erreicht werden. Denkbar ist z. B., daß alle Berechnungen, die der Deichverband zur Festsetzung des Beitragsmaßstabes (Beitragsbuch) und der Beiträge (Hebeliste) durchgeführt hat, zum Inhalt von Betragsbuch und Hebeliste gemacht werden, soweit sie nicht ohnehin schon bekannt sind, die dann von jedem Mitglied eingesehen werden können. Ggf. kann dabei je nach Notwendigkeit die Summe der der Berechnung zugrundeliegenden Einheitswerte nach Grundstücksgruppen, z. B. nach Nutzungsarten oder Grundstücksgrößeklassen u. ä. aufgeschlüsselt werden. Hinsichtlich der Hebeliste können Haushaltsplan und Haushaltsrechnung und ggf. weitere Aufschlüsselungen der darin enthaltenen Einnahme- und Ausgabepositionen zum Inhalt gemacht werden. Bei solchen oder ähnlichen Verfahren hätte das einzelne Mitglied auch ausreichend Gelegenheit, offensichtliche Unrichtigkeiten bei der Berechnung von Beitragsmaßstab oder Beitrag festzustellen. Das einzelne Mitglied kann ohne Offenlegung der personenbezogenen Daten der übrigen Mitglieder durchaus feststellen, ob die ihn betreffenden Daten zutreffend ausgeworfen worden sind, indem es in diesen Teil des Beitragsbuches Einblick nimmt.

Nicht außer Acht bleiben kann, daß bei der Offenlegung vorstehend genannten Materials dem einzelnen Mitglied die Kontrolle auch insoweit erleichtert wird, als diese vom Vorstand des Verbandes erarbeiteten Zahlenwerte bereits durch den von den Mitgliedern gewählten Ausschuß geprüft worden sind.

Es soll nicht verkannt werden, daß es im öffentlichen Interesse liegen mag, durch die Kontrollmöglichkeiten für das einzelne Mitglied die Akzeptanz der Pflichtmitgliedschaft im Deichverband zu erhöhen und den Mitgliedern demokratische Rechte der Kontrolle von Verwaltungshandeln einzuräumen. Dem steht jedoch das aus den Grundrechten abgeleitete Recht der Betroffenen auf Wahrung der informationellen Selbstbestimmung gegenüber. Bei der Bedeutung, die dem allgemeinen Freiheitsanspruch des Bürgers gegenüber dem Staat bei dem sich insoweit wandelnden Verfassungsverständnis zukommt, wäre eine Einschränkung dieses Rechts zugunsten des möglichen öffentlichen Interesses nicht verfassungskonform, zumal das öffentliche Interesse auch mit anderen als das Recht der Betroffenen auf informationelle Selbstbestimmung einschränkenden Mitteln erreicht werden kann.

Da Grundlage für die Ermittlung des Beitragsverhältnissses der Einheitswert des die Mitgliedschaft begründenden Grundstückes ist und dieser deshalb bei Einsichtnahme in das Beitragsbuch offengelegt wird, ist eine Offenbarung der Daten aller Mitglieder zugunsten einzelner Mitglieder unzulässig. Das ergibt sich insbesondere aus den Vorschriften der §§ 30 und 31 der Abgabenordnung (AO). Nach § 30 AO (Steuergeheimnis) dürfen in einem Steuerverfahren erhobene Daten nur offenbart werden, wenn ein Gesetz dieses ausdrücklich zuläßt. Eine solche Vorschrift ist für den vorliegenden Fall nicht in Sicht. § 31 AO läßt zwar eine Mitteilung von Besteuerungsgrundlagen an Körperschaften des öffentlichen Rechts zu. Die Verwendung der so übermittelten Daten ist jedoch begrenzt auf den Zweck: Festsetzung von Abgaben, die an diese Besteuerungsgrundlagen anknüpfen. Eine Verwendung, die wie hier die verbandsinterne Kontrolle über diesen Zweck hinausgeht, ist unzulässig. Wenn die Rechtsprechung der Verwaltungsgerichte die Bedeutung des Steuergeheimnisses für die Verpflichtung der Deichverbände auf Offenlegung aller Daten des Beitragsbuches und der Hebeliste für unbedeutend gehalten hat, mag dieses seine Ursache darin haben, daß sein Zweck ursprünglich als im Interesse der Verwaltung liegend angesehen wurde, weil man davon ausging, daß Personen, die das Steuergeheimnis kennen, eher bereit sein würden, Verhältnisse zu offenbaren.

Inzwischen ist der Zweck des Steuergeheimnisses jedoch primär auf den Schutz des Rechtes der Auskunftspflichtigen auf informationelle Selbstbestimmung ge-

richtet. Der Gesetzgeber hat dem zuletzt durch Aufnahme weiterer datenschutzrechtlicher Vorschriften in § 30 AO durch das Steuerbereinigungsgesetz vom 17. 12. 1985 Rechnung getragen. Auch in der Rechtsprechung hat dieses entsprechend Niederschlag gefunden. Der vom Bundesverfassungsgericht in seinem Volkszählungsurteil 1983 aufgestellte Grundsatz, nach dem zwangsweise erhobene Daten nur für den im Gesetz verwendeten Zweck (hier: Besteuerung) verwendet werden dürfen, gilt somit auch für die im Besteuerungsverfahren erhobenen personenbezogenen Daten. Soweit die Verwaltungsgerichte bei ihrer Entscheidung die Abgabenordnung und die Erste Wasserverbandsordnung als in dieser Frage miteinander kollidierenden Normen und dabei die Erste Wasserverbandsordnung als bevorzugt anzuwendende Spezialnorm hinsichtlich der Auslegung der personenbezogenen Daten in Beitragsbuch und Hebeliste angesehen haben sollten, ist diese Position im Hinblick auf das gewandelte Verfassungsverständnis und die Fortentwicklung des Rechtes nicht mehr haltbar. Dabei ist auch zu bedenken, inwieweit eine vorkonstitutionelle untergesetzliche Norm, nämlich die Erste Wasserverbandsordnung, in der Lage sein kann, die laufend fortentwickelten Vorschriften des § 30 der AO und der damit verbundenen Anpassung dieser Vorschriften an die Fortentwicklung des Rechtes auf informationelle Selbstbestimmung zurückzudrängen.

Die Erste Wasserverbandsordnung erfüllt nicht die Anforderungen, die das Bundesverfassungsgericht an eine Norm, die das Recht auf informationelle Selbstbestimmung einschränkt, gestellt hat. Das bedeutet, daß nach diesen Vorschriften jede Verarbeitung personenbezogener Daten als unzulässig angesehen werden muß. Sie kann höchstens noch vorübergehend unter Inanspruchnahme des Übergangsbonus hingenommen werden. Der Gesetzgeber bleibt hier aufgerufen, die notwendigen gesetzlichen Vorschriften für unumgängliche Verarbeitung personenbezogener Daten zu schaffen.

5.3.7 Ausländerangelegenheiten

5.3.7.1 Weitergabe von Sozialdaten über Klienten des Sozialpsychiatrischen Dienstes an die Einbürgerungsbehörde

Die Einbürgerungsbehörde beim Senator für Inneres hat im Rahmen der Prüfung des „unbescholtenen Lebenswandels" von Einbürgerungsbewerbern nach § 8 Abs. 1 Nr. 1 Reichs- und Staatsangehörigkeitsgesetz (RuStAG) den Sozialpsychiatrischen Dienst beim Hauptgesundheitsamt um Auskunft ersucht, ob dort Erkenntnisse über eine Sucht oder Suchtgefährdung des jeweiligen Einbürgerungsbewerbers bekannt sind. Die Einbürgerungsbewerber haben vorher in das Auskunftsersuchen eingewilligt. Soweit Erkenntnisse über eine Sucht oder Suchtgefährdung des Einbürgerungsbewerbers bekannt waren, hat der Sozialpsychiatrische Dienst zur Beurteilung der Einbürgerungsvoraussetzungen einen Vermerk/Bericht für die Einbürgerungsbehörde angefertigt.

Auf meine Anfrage hat der Senator für Inneres (Einbürgerungsbehörde) ausgeführt, die Einbürgerung eines Ausländers in die deutsche Staatsangehörigkeit setze nach § 8 RvStAG als gesetzliche Einbürgerungsvoraussetzung voraus, daß der Einbürgerungsbewerber einen „unbescholtenen Lebenswandel" geführt hat. Dieser unbestimmte Rechtsbegriff sei nach herrschender Rechtsauffassung nicht ausschließlich unter strafrechtlichen Gesichtspunkten zu beurteilen; vielmehr umfasse er das gesamte Verhalten des Einbürgerungsbewerbers in sittlicher und rechtlicher Beziehung. Der Einbürgerungsbewerber müsse in seinem Lebenswandel und den sich daraus ergebenden charakterlichen Eigenschaften gewisse Mindestvoraussetzungen erfüllen, die in ihm einen wünschenswerten Bevölkerungszuwachs sehen und damit ein öffentliches Interesse an der Einbürgerung begründen lassen. Dieses könne jedoch bei Bestehen einer Alkohol- oder Rauschmittelsucht nicht bejaht werden. Eine Verweigerung der Auskunftserteilung hätte demnach zur Folge, daß eine bundesrechtliche Regelung nicht mehr gesetzeskonform durchgeführt werden könne. Die Anfrage sei auch verhältnismäßig, weil nur so vermieden werden könne, daß den Gesundheitsbehörden bekannte Personen, die süchtig oder suchtgefährdet sind und bei denen ein öffentliches Interesse an der Einbürgerung nicht bejaht werden könne, dennoch eingebürgert würden.

Aus der Sicht der Einbürgerungsbehörde sei darüber hinaus an dem Auskunftsersuchen und der Auskunftserteilung auch deshalb nichts auszusetzen, weil der Einbürgerungsbewerber zusammen mit seinem Einbürgerungsantrag die Ärzte des Hauptgesundheitsamtes ausdrücklich von ihrer ärztlichen Schweigepflicht entbunden und sich mit der Auskunftserteilung einverstanden erklärt habe. Diese Einwil-

FFD 12.163

ligungserklärung entspreche den Anforderungen, die § 64 SGB X an eine Befugnis zur Offenbarung des Sozialgeheimnisses stelle.

Die Frage, ob die Einwilligung durch den Einbürgerungsbewerber tatsächlich „freiwillig" erfolgt, wurde von der Einbürgerungsbehörde bejaht. Danach stünden sämtliche Erklärungen des Einbürgerungsbewerbers, die für die Durchführung des Einbürgerungsverfahrens erforderlich sind und von ihm im Rahmen seiner Mitwirkungsobliegenheiten nach § 26 Abs. 2 Bremisches Verwaltungsverfahrensgesetz (BremVwVfG) abgegeben werden, in einem untrennbaren Zusammenhang mit seinem Einbürgerungsantrag. Die Entscheidung, einen solchen Antrag zu stellen, sei ausschließlich eine Entscheidung des Bewerbers; auf die Entscheidung würde staatlicherseits keinerlei Zwang ausgeübt. Die Entscheidung sei deshalb immer als eine „freiwillige" anzusehen, in die der Einbürgerungsbewerber seine eigenen Überlegungen des „für und wider" einbezogen habe. Hierbei sei im Einzelfall nicht auszuschließen, daß sich der Einbürgerungsbewerber auch aus Gründen zu einem Einbürgerungsantrag veranlaßt oder motiviert sehe, die mit der staatsangehörigkeitsrechtlichen Idealbezeichnung der „freiwilligen Hinwendung zu Deutschland" nichts oder nur wenig zu tun hätten, der Einbürgerungsbehörde aber naturgemäß nicht mitgeteilt oder bekannt würden. So erscheine es ihr nicht ausgeschlossen, daß der Bewerber seine Einbürgerung vorwiegend aus wirtschaftlichen Gründen betreibe, die für ihn subjektiv eine Zwangslage für seine Entscheidung zugunsten der Deutschen und zu Lasten seiner bisherigen Staatsangehörigkeit darstelle.

Nach allem halte sie es lediglich aus philosophischer Sicht wohl für interessant, in solchen Zusammenhängen über die Freiwilligkeit menschlichen Handelns im allgemeinen und besonderen nachzudenken, für die Lösung der Interessenlage bringe das jedoch wenig. So sei davon auszugehen, daß das Antragsprinzip im Einbürgerungsrecht das Moment der Freiwilligkeit berücksichtige.

Ich habe dem Senator für Inneres (Einbürgerungsbehörde) meine gegenteilige Auffassung dargelegt. Insbesondere habe ich bezweifelt, daß es verhältnismäßig ist, von einem Einbürgerungsbewerber die Einwilligung zu verlangen, daß Auskünfte über eine bestehende Sucht bei der Suchtberatungsstelle eingeholt werden. Es muß dabei abgewogen werden zwischen dem öffentlichen Interesse, von ausländischen Mitbürgern zu erfahren, ob Tatsachen zur Verneinung eines unbescholtenen Lebenswandels vorliegen und dem Grundrecht des Einbürgerungsbewerbers auf informationelle Selbstbestimmung hinsichtlich seiner Privat- und Intimsphäre. Zur Auslegung des Begriffes „unbescholtener Lebenswandel" besagt die einschlägige Kommentierung, daß nach herrschender Meinung dieser Begriff den Wandlungen der Zeit ausgesetzt ist. Danach kann das Staatsangehörigkeitsgesetz insoweit nur dann gesetzeskonform durchgeführt werden, wenn der Begriff des „unbescholtenen Lebenswandels" zeitgemäß ausgelegt wird. Aus datenschutzrechtlicher Sicht kann eine gesetzeskonforme Anwendung dann nicht gegeben sein, wenn bei allen nur denkbaren Stellen Auskünfte eingeholt werden.

Mit dem Ziel einer bundeseinheitlichen Anwendung des Staatsangehörigkeitsgesetzes und zur Wahrung des Gleichheitsgrundsatzes hat der Bundesminister des Innern im Einvernehmen mit den Ministern/Senatoren der Länder am 01. 07. 1977 Einbürgerungsrichtlinien erlassen, die den damaligen Wertvorstellungen in öffentlicher und rechtlicher Hinsicht entsprechen sollten und dabei den Begriff des „unbescholtenen Lebenswandels" ausformulieren. Die unter Nr. 3.3.4 dieser Richtlinien dargelegten „Fehlentwicklungen der Persönlichkeit" (Alkohol- oder Rauschmittelsucht, fortdauernde Verletzung der Unterhaltspflicht, Arbeitsunwilligkeit), die eine Einbürgerung ausschließen, lassen erkennen, daß im wesentlichen Fehlentwicklungen gemeint waren, die nach damaliger sittlicher Auffassung vorwerfbar waren. Damals wurden Alkohol- oder Rauschmittelsucht noch weitgehend den charakterlichen Eigenschaften zugeordnet, die der einzelne selbst zu verantworten hat. Ob es sich bei Alkohol- oder Rauschmittelsucht um eine von den Betroffenen selbst zu verantwortende Fehlentwicklung der Persönlichkeit handelt, ist zumindest unter den neuesten Erkenntnissen der medizinischen Wissenschaft höchst zweifelhaft. Danach wird inzwischen allgemein anerkannt, daß es sich um eine Suchterkrankung handelt, die wie jede andere Krankheit in jeder sozialen Schicht auftritt und einer Therapie bedarf. Insoweit beinhaltet der Begriff „notorische Trunksucht und dergleichen", wie er seinerzeit in Literatur verwandt wurde, Wertvorstellungen aus einer Zeit, in der noch nicht erkannt worden war, daß es sich hier um Suchtkrankheiten handelt.

Unter Berücksichtigung des inzwischen allgemein anerkannten medizinischen Erkenntnisstandes ist ein unbescholtener Lebenswandel wohl nicht zu verneinen,

wenn ein Einbürgerungsbewerber an einer Suchtkrankheit leidet. Aufgrund dieser Erkenntnisse ist die Beantwortung der Frage, ob ein Einbürgerungsbewerber an einer Suchtkrankheit leidet, für die Beurteilung des unbescholtenen Lebenswandels nicht mehr erforderlich.

Wenn jedoch trotz dieser neueren Erkenntnisse der Begriff des „unbescholtenen Lebenswandels" ohne Rücksicht auf die Wandlungen der Zeit ausgelegt werden würde, wäre zu prüfen, inwieweit das informationelle Selbstbestimmungsrecht zur Prüfung der Voraussetzung nach § 8 Nr. 2 RuStAG eingeschränkt werden darf.

Dem Einbürgerungsbewerber wird abverlangt, in die Auskunftseinholung durch die Einbürgerungsbehörde gegenüber dem Sozialpsychiatrischen Dienst einzuwilligen. Verweigert er diese Einwilligung, wird die Einbürgerung versagt.

Die Einwilligung einer schriftlichen Einverständniserklärung vermag nur dann eine verfassungskonforme Einschränkung des Rechts auf informationelle Selbstbestimmung darzustellen, wenn das Prinzip der „Freiwilligkeit" gewahrt bleibt. Freiwillig wird diese Einverständniserklärung nicht abgegeben. Der Einbürgerungsbewerber wird von sich aus eine solche Erklärung — ob er tatsächlich will oder nicht — unterschreiben, möchte er doch deutscher Staatsbürger werden. Aus diesem Grunde kann die wohl nicht freiwillig abgegebene Einverständniserklärung die Voraussetzung nach § 67 Nr. 1 SGB X nicht erfüllen.

Außerdem kann nicht davon ausgegangen werden, daß das Antragsprinzip im Einbürgerungsrecht das Moment der Freiwilligkeit berücksichtigt. Der Betroffene hat im bisherigen Verfahren zwei Erklärungen abgegeben, nämlich den Einbürgerungsantrag und daraufhin nach Aufforderung durch die Einbürgerungsbehörde die Einwilligung in das Auskunftsersuchen gegenüber dem Sozialpsychiatrischen Dienst. Insoweit stehen zwar beide Erklärungen in einem gewissen Zusammenhang, stellen jedoch jeweils für sich eigenständige Erklärungen dar.

Die Einwilligung des Betroffenen in das Auskunftsersuchen und damit die Einschränkung seines informationellen Selbstbestimmungsrechts hat für ihn existentielle Bedeutung. Willigt er in die Auskunftseinholung nicht ein, muß er nach dem bisherigen Verfahren mit der Ablehnung seines Einbürgerungsantrages rechnen. Die Abverlangung seiner Einwilligungserklärung und einer Entbindung von der ärztlichen Schweigepflicht kann jedoch nur dann verhältnismäßig und damit zulässig sein, wenn die Auskünfte zur Beurteilung des unbescholtenen Lebenswandels geeignet und erforderlich sind.

Die gleichen Grenzen ergeben sich aus § 26 Abs. 2 i. V. m. mit § 26 Abs. 1 BremVwVfG. Die Mitwirkungspflicht endet dann, wenn sie nicht mehr dem Verhältnismäßigkeitsgrundsatz entspricht. Daraus folgt, daß die Verweigerung einer erbetenen Mitwirkung — soweit sie unverhältnismäßig ist — nicht dazu führen kann, den Einbürgerungsantrag abzulehnen.

Abgesehen davon hängt die Intensität des Eingriffes in Persönlichkeitsrechte des Betroffenen auch davon ab, welche Folgen für ihn und seine persönliche Weiterentwicklung zu erwarten sind, wenn der von der Einbürgerungsbehörde angeforderte Vermerk/Bericht des Sozialpsychiatrischen Dienstes angefertigt und entsprechend weitergeleitet wird.

Es ist inzwischen nicht nur unter Medizinern allgemeine Erkenntnis, daß für die Arbeit einer Suchtberatungsstelle, wie dem Sozialpsychiatrischen Dienst, die Bildung eines Vertrauensverhältnisses zwischen Berater und Klienten unabdingbare Voraussetzung ist. Dies gilt sowohl für die Anbahnung der Berater-Klienten-Beziehung als auch für deren Aufrechterhaltung. Muß der Klient damit rechnen, daß seine während der Beratung gemachten Äußerungen und die dabei mitgeteilten Tatsachen aus seinem persönlichen Lebensbereich Dritten zugänglich werden, so wird er regelmäßig gar nicht erst bereit sein, von der Möglichkeit, sich beraten zu lassen, Gebrauch zu machen. Die rückhaltlose Offenbarung von Angelegenheiten des privaten Lebensbereiches ist im Hinblick auf die Ursachen und Motive notwendig, die für den Drogenmißbrauch bestimmend sind und oft in tieferen Schichten der Persönlichkeit wurzeln. Das sich entwickelnde Vertrauensverhältnis zwischen Berater und Klienten für eine erfolgreiche Therapie ist somit unabdingbar. Daraus folgt, daß die Weiterleitung von Informationen aus Beratungsgesprächen — besonders, wenn der Betroffene nicht oder nicht vollständig freiwillig darin einwilligt — das Therapieziel erheblich gefährden würde.

Allein schon aus diesen Gründen greift die Abverlangung einer Einwilligungserklärung von den Einbürgerungsbewerbern, die sich in Sozialtherapeutischen

FFD.12.163

Beratungsstellen einer Therapie unterziehen, so tief in das Recht auf informationelle Selbstbestimmung ein, daß eine Gesundheitsgefährdung des Betroffenen bzw. eine erhebliche Störung des Heilungsprozesses nicht auszuschließen ist. Die Persönlichkeitsrechte sind demnach höher zu bewerten als das öffentliche Interesse nach § 8 Abs. 2 RuStAG.

Darüber hinaus stellt sich die Frage, ob ein Auskunftsersuchen gegenüber dem Sozialpsychiatrischen Dienst überhaupt geeignet ist, die notwendigen Feststellungen zur Beurteilung des unbescholtenen Lebenswandels vorzunehmen. Es gibt keinen Anhaltspunkt dafür, daß sich alle bzw. der überwiegende Teil der Alkohol- oder Drogenabhängigen beim Sozialpsychiatrischen Dienst in Therapie befindet. Experten gehen davon aus, daß es sich hier um eine kleine Minderheit der Suchtkranken handelt.

Darüber hinaus befinden sich die drogenabhängigen Einbürgerungsbewerber, die sich beim Sozialpsychiatrischen Dienst einer Therapie unterziehen und der Einbürgerungsbehörde im Rahmen dieses Auskunftsverfahrens bekannt werden, in einer positiv zu bewertenden Situation, die einem Abbau der Sucht zuträglich ist. Insgesamt erreicht die Einbürgerungsbehörde mit dem bisher praktizierten Verfahren ohnehin nur die Einbürgerungsbewerber, die auf absehbare Zeit vermutlich nicht mehr drogenabhängig sein werden. Aus diesem Grunde muß die Abverlangung der Einwilligungserklärung und die Auskunftserteilung als nicht geeignet und damit unverhältnismäßig angesehen werden, wenn das Ziel verfolgt werden soll, alkohol- oder rauschmittelabhängige Einbürgerungsbewerber von der Einbürgerung abzuhalten.

Der Senator für Inneres (Einbürgerungsbehörde) ist inzwischen meiner Auffassung im wesentlichen beigetreten und wird keine Auskunftsersuchen mehr an den Sozialpsychiatrischen Dienst beim Hauptgesundheitsamt richten.

5.3.7.2 Datenverarbeitung bei Ausländerbehörden und beim Ausländerzentralregister

Bei der Durchführung des Ausländergesetzes und einer Reihe weiterer Ausländer betreffende Gesetze sammeln und verarbeiten die Ausländerbehörden eine Fülle personenbezogener Daten der Betroffenen. Ein großer Teil der von den Ausländerbehörden gesammelten Daten wird an ein beim Bundesverwaltungsamt geführtes Ausländerzentralregister übermittelt. Einer Vielzahl von Behörden, aber auch nicht-öffentlichen Stellen werden aus diesem Register Auskünfte erteilt.

Die bereichsspezifischen Datenschutzvorschriften in den die Ausländer betreffenden Gesetzen erfüllen zum großen Teil nicht die Anforderungen, die das Bundesverfassungsgericht an Normen gestellt hat, die das Recht auf informationelle Selbstbestimmung einschränken. Das gilt insbesondere auch für die Datenverarbeitung beim Ausländerzentralregister.

Wie ich in meinem 9. Jahresbericht unter Pkt. 5.2.6.1 berichtet habe, haben deshalb die Innenminister/Senatoren unter Federführung des Bundesinnenministers Entwürfe zur Neukonzeption des Registers vorgelegt.

Die Datenschutzbeauftragten des Bundes und der Länder haben mit dem Beschluß in ihrer Konferenz vom 4./5. Mai 1987 (vgl. Anlage) dazu Stellung genommen.

Im übrigen haben sie den aus diesem Anlaß gebildeten Arbeitskreis beauftragt, die notwendig werdenden Änderungen im Ausländerrecht datenschutzrechtlich zu begleiten.

5.4 Justiz und Verfassung

5.4.1 Schwerpunkte, Handlungsbedarfsfälle

5.4.1.1 ADV-Einsatz bei Gerichten, Staatsanwaltschaften und im Strafvollzug

Ich hatte bereits im letzten Jahresbericht unter Pkt. 5.3.1.2 auf die beabsichtigte breite Einführung von ADV in der Justizverwaltung wie auch in der Verwaltung des Strafvollzugs ausführlich hingewiesen. Auf eine Wiederholung der Darstellung von bereits realisierten Verfahren möchte ich an dieser Stelle verzichten.

Bei der Automatisierung allgemeiner Geschäftstellentätigkeiten, wie z. B. die Vergabe der Aktenzeichen, Registratur oder ähnliches waren, soweit damit keine Änderungen des bisher praktizierten manuellen Verfahrens einhergingen, in der Regel nur die allgemeinen Datensicherungsmaßnahmen zu gewährleisten. Die jetzt sichtbar werdenden Tendenzen deuten aber auf einen viel intensiveren Ein-

satz der ADV in Rechtspflege und Strafvollzug hin, der mir Anlaß gibt zu einigen generellen Bemerkungen.

Die Gerichte, die Staatsanwaltschaften und der Strafvollzug erhoffen sich eine spürbare Entlastung durch den Technikeinsatz und sind daher leicht, zum Teil unkritisch, für solche Entscheidungen zu gewinnen. Im Vordergrund der Betrachtung z. B. bei Gerichten stehen daher häufig wirtschaftliche Gesichtspunkte, nicht so sehr die Auswirkungen moderner Technologien auf den Rechtsuchenden und seine Rechte wie auch die Wirkungen, die auf den Prozeß der Rechtsanwendung selbst ausstrahlen können. Eine gewisse Anpassung der Richter an systematisierte Arbeitsweisen wird notwendig und ist man bereit in Kauf zu nehmen.

An dieser Stelle möchte ich z. B. darauf hinweisen, daß die Verwendung von Textbausteinen in gerichtlichen Entscheidungen rechtsstaatliche Probleme unter dem Gesichtspunkt der Notwendigkeit der Einzelentscheidung und der Erhaltung richterlichen Entscheidungsfreiheit aufweisen können. Die Massenverfahren, wie die in einem Jugendzentrum in Nürnberg durchgeführten Verhaftungen oder die eines Verwaltungsgerichts in Rheinland-Pfalz, das bei Volkszählungsentscheidungen sich rühmen konnte, dank des Technikeinsatzes im Verlauf von nur wenigen Wochen mehrere 100 Verfahren entschieden zu haben, wobei zwischen Antragstellung und Entscheidung des Antrages nur wenige Tage gelegen haben und die in den Medien darauf eingetretenen kritischen Reaktionen machen das Problem deutlich. Werden solche Techniken zur Verfügung gestellt, sind Gerichte angesichts des Termindrucks wenigstens in solchen Fällen geneigt, davon Gebrauch zu machen; anstatt individueller Entscheidungen besteht die Gefahr, daß der Einfachheit halber vorhandene Textbausteinvarianten genutzt werden. In solchen Verfahren, in denen auf unterschiedlichstes Vorbringen mit einigen wenigen Textbausteinen pauschal geantwortet wird, ohne daß die Entscheidung sich an dem gegebenen Fall orientiert, ist das justizielle Grundrecht auf rechtliches Gehör in Frage gestellt.

Um die Systeme „bürokommunikationsfähig" zu machen, d. h. den Datenaustausch zwischen Gerichten und Instanzen zu ermöglichen, geht die Einführung einher mit der Vereinheitlichung des Geschäftsbetriebes. Regionalen Besonderheiten kann mit Mehraufwand zwar noch in gewissem Umfang entsprochen werden, als Tendenz ist aber die bundesweite Vereinheitlichung der Geschäftsgänge zu verzeichnen. Die Vernetzung nicht nur innerhalb einzelner Gerichte, sondern ganzer Gerichtszweige und dies bundesweit ist ebenso denkbar, wie die diskutierte Verknüpfung der Staatsanwaltschaften untereinander (SISY). Durch die Vernetzung der PC's untereinander wird ein in weiten Teilen nicht mehr zu kontrollierender Datenaustausch ermöglicht.

Diese Tendenzen gilt es bei der Einführung der ADV-Systeme zu berücksichtigen. Die nachfolgend aufgelisteten Entscheidungen zur Einführung von ADV-Verfahren zum Einsatz von Arbeitsplatzrechnern und der Einsatz von Textverarbeitungssystemen sind Einzelschritte. Um die datenschutzrechtlichen Bewertungen sinnvoll vorzunehmen, ist es aber wichtig, auch diese Teilschritte unter dem Gesichtspunkt von vernetzten Systemen zu betrachten.

— Der Senator für Rechtspflege und Strafvollzug beantragte in Abstimmung mit dem Senator für Inneres die Übernahme des beim Stadt- und Polizeiamtes Bremen und der Staatsanwaltschaft Bremen bereits installierten ADV-Verfahrens ISA/CANASTA für die Ortspolizeibehörde Bremerhaven und die Staatsanwaltschaft Bremerhaven. In einem Gespräch mit Vertretern der Staatsanwaltschaft in Bremen habe ich die mit der Übernahme des Verfahrens verbundenen datenschutzrechtlichen Fragestellungen erörtert. Nach dessen Erklärung handelt es sich um eine identische Übernahme des bereits vorhandenen ADV-Verfahrens ISA/CANASTA, zu dem ich bereits 1985 Stellung genommen hatte. Mir wurde versichert, daß über das Geschäftszeichen sichergestellt ist, daß die Staatsanwaltschaft in Bremerhaven nur auf Daten der eigenen Dezernate zugreifen kann, um dort Datenerfassungen und -änderungen durchzuführen. Zum Lesen hingegen steht der gesamte in CANASTA gespeicherte Datensatz zur Verfügung. Weiter wurde mir erklärt, daß die Übernahme der polizeilichen Daten aus der Zwischendatenbank in die Datenbank CANASTA sowie die Rückmeldung über den Ausgang des Verfahrens an die Polizei technisch so organisiert ist, daß die Polizeibehörde in Bremerhaven nur Daten aus dem Bereich der Staatsanwaltschaft Bremerhaven erhalten.

  Unter Zugrundelegung meiner bereits früher abgegebenen Stellungnahme (vgl. den 7. Jahresbericht unter Pkt. 5.2.1.5) habe ich keine datenschutzrechtlichen Bedenken gegen die geplante Übernahme des ADV-Verfahrens erhoben.

Dieses Verfahren sichert zwar, daß der Ausgang des Strafverfahrens den Polizeidienststellen mitgeteilt wird. Dies führt in der Regel auch zu einer Berücksichtigung bei der Speicherung der Falldaten in polizeilichen Informationssystemen. Bei der Polizei nicht aktualisiert werden hingegen die tatsächlichen Feststellungen, die im Verlauf eines Verfahrens oft durch die Staatsanwaltschaft oder durch die Gerichte ergänzt oder korrigiert werden. In dieser Zwischenzeit ist es durchaus möglich, daß in polizeilichen Informationssystemen strafrechtlich nicht gesicherte Daten gespeichert sind. Die Erkenntnisse, die bei der Polizei im Rahmen der Strafverfolgung anfallen, sind nur vorläufiger Natur. Staatsanwaltschaften und Gerichte können zu anderen tatsächlichen Feststellungen oder zu einer anderen Bewertung von Strafbarkeit und Verschulden kommen. Bei Strafverfahren, die sich über einen gewissen Zeitraum erstrecken, kann dies im Einzelfall eine erhebliche Beeinträchtigung schutzwürdiger Belange der Betroffenen darstellen. Polizeiliche Datensammlungen können nämlich mehr als Datensammlungen anderer Behörden das verfassungsrechtlich geschützte Persönlichkeitsrecht der betroffenen Bürger beeinträchtigen. Aus diesem Anlaß verweise ich auf den von den Datenschutzbeauftragten des Bundes und der Länder gefaßten Beschluß zur Rückmeldung von der Justiz an die Polizei, den ich als Anlage 1 abdrucke. Dies gilt um so mehr, wenn die Daten in polizeilichen Informationssystemen gespeichert werden, die bundesweit genutzt werden können.

— Der Senator für Justiz und Verfassung hat Ende 1987 eine Reihe von ADV-Anträgen auf Einsatz von PC in Schreibdiensten gestellt. Im einzelnen handelt es sich dabei um den

- ADV-Antrag auf Einsatz von PC im Schreibdienst der Staatsanwaltschaft Bremen (StA) und die Ersatzbeschaffung von PC für einen abschreibungsfähigen Schreibautomaten;
- ADV-Antrag auf PC-Einsatz zur Unterstützung der Textverarbeitung im Landgericht Bremen (Strafkammer und Verwaltungsbereich);
- ADV-Antrag auf Einsatz von PC im Schreibdienst des Sozialgerichts Bremen und der Ersatzbeschaffung von PC für einen abschreibungsfähigen Schreibautomaten;
- ADV-Antrag auf PC-Einsatz zur Unterstützung der Textverarbeitung im Landessozialgericht Bremen.

Die Anträge wurden mir mit einer außergewöhnlich kurzen Frist zur Stellungnahme übersandt. Die zugrundeliegenden Unterlagen ließen wenige datenschutzrechtliche Ansatzpunkte für den tatsächlichen Einsatz der zu beschaffenden Geräte erkennen. Auf dieser Grundlage sah ich mich nicht in der Lage, Empfehlungen abzugeben, wie datenschutzrechtlichen Anforderungen Rechnung getragen werden könnte. Aufgrund der mir zur Verfügung gestellten Unterlagen vermutete ich, daß die für die Staatsanwaltschaft zu beschaffenden PC mit einer Schnittstelle zu CANASTA ausgestattet werden sollten. Bei den anderen Stellen war nicht deutlich, inwieweit die Beschaffung bereits eine Weichenstellung zur Einführung von SOJUS (nunmehr SIJUS) bedeutete. Auch zu den Fragen, wie technische und organisatorische Maßnahmen nach § 6 BrDSG zur Datensicherheit getroffen werden sollten und wie die Zweckbindung nach § 12 BrDSG sichergestellt werden soll, konnte den Anträgen nicht entnommen werden. In aller Regel ist vor Abgabe einer datenschutzrechtlichen Stellungnahme daher ein die verschiedenen Fragen klärendes Gespräch erforderlich.

Aus diesem Anlaß habe ich den Senator für Justiz und Verfassung darauf hingewiesen, daß gem. § 27 Abs. 4 BrDSG ich über die Planung zum Aufbau automatisierter Informationssysteme rechtzeitig zu unterrichten bin, sofern in dem System personenbezogene Daten verarbeitet werden sollen. Da der Stand der Unterlagen ein zwei bis drei Monate zurückliegendes Datum auswies, habe ich bedauert, daß, obwohl bereits seit einiger Zeit an der Vorbereitung des Antrages gearbeitet wurde, ich in diesem Stadium nicht über die Planungen informiert worden bin. Weiter habe ich den Senator in diesem Zusammenhang darauf hingewiesen, daß es nicht so sehr darum geht, der Nr. 4 der Richtlinien des ADV-Ausschusses vom 1. März 1987 zu entsprechen, sondern vielmehr unter Wirtschaftlichkeitsgesichtspunkten dienlich ist, wenn eine datenschutzrechtliche Stellungnahme dem ADV-Antrag beigefügt werden kann. Datenschutzrechtliche Gesichtspunkte können nämlich durchaus zu einer Kostensteigerung des geplanten ADV-Einsatzes führen und wären somit auch unter

wirtschaftlichen Gesichtspunkten für die Entscheidung des ADV-Ausschusses von Belang.

Schließlich habe ich hervorgehoben, daß ich in erster Linie ein Kontroll- und Beratungsorgan bin; die datenverarbeitenden Stellen haben daher zunächst selbst den Bestimmungen mit datenschützenden Charakter Rechnung zu tragen. Ich erwarte daher von den datenverarbeitenden Stellen, daß sie bereits bei der Planung des Einsatzes von ADV ein Datenschutzkonzept entwickeln, basierend auf einer Schwachstellenanalyse, das dann Grundlage einer Datenschutzberatung sein kann.

Diese allgemeinen Überlegungen sind von ganz grundsätzlicher Art und daher von den anderen Ressorts zu berücksichtigen.

In den mittlerweile geführten Gesprächen habe ich die Probleme des PC-Einsatzes im Schreibdienst hinreichend diskutieren können. Mir wurde dabei erklärt, daß der Einsatz der PC zur Fertigung von Schriftstücken (z. B. Anklageschriften, Strafanträge etc.) dienen soll und nur zur vorübergehenden Nutzung bis zur Einführung des SIJUS-Verfahrens beschafft werden. Bis dahin handelt es sich um Einzelplätze, die nicht miteinander vernetzt sind und auch keinen Anschluß zu CANASTA aufweisen. Da keine Adreßdateien verwendet werden und das Schriftgut nur bis zum Zeitpunkt der endgültigen Korrektur gespeichert wird, ist eine Dateimeldung nicht notwendig. Eingesetzt werden soll eine spezielle Textsoftware, mit der jedoch auch Geschäftsverteilungspläne und Telefonverzeichnisse geschrieben werden sollen. Sicherzustellen ist auch, daß die vom RbV erarbeitete „PC-Systemakte" verwendet wird und gem. § 7 BrDSG ein Geräteverzeichnis geführt wird. Damit sichergestellt ist, daß keine weitere unkontrollierte Verarbeitung erfolgt, ist eine Zugriffsschutz-Software je Arbeitsplatzrechner einzusetzen.

— Automatisierte Datenverarbeitung in den Vollzugsgeschäftsstellen

Bereits frühzeitig wurde ich darüber informiert, daß beabsichtigt ist, die Datenverarbeitung im Strafvollzug zu automatisieren (vgl. 9. Jahresbericht unter Pkt. 5.3.1.2). Anläßlich eines Informationsgesprächs über den Sachstand im Herbst des Berichtsjahres wurde mir erklärt, daß auf Bundesebene im September 1986 eine Fachgruppe „ADV im Strafvollzug" gebildet wurde. Diese setzt sich aus drei Arbeitsgruppen zusammen; nämlich der Arbeitsgruppe I: Arbeitsverwaltung, der Arbeitsgruppe II: Wirtschaftsverwaltung und der Arbeitsgruppe III: Vollzugsgeschäftsstelle.

Das Land Bremen beteiligt sich an der Entwicklung der Automation der Vollzugsgeschäftsstellen. Geplant ist, mit dem Verfahren Automation der Datenabläufe in den Vollzugsgeschäftsstellen (ADIV) die Datenverarbeitungsvorgänge bei den Vollzugsgeschäftsstellen zu automatisieren. Federführend in diesem Projekt ist das Land Berlin. Dort soll bereits ein Verfahren zur Automation der Verwaltungsabläufe in der Vollzugsgeschäftsstelle getestet werden.

Der Umfang und der Inhalt der Dienstgeschäfte der Vollzugsgeschäftsstellen ist im einzelnen in der bundeseinheitlich geltenden Vollzugsgeschäftsordnung (VGO) geregelt. Alle Daten, die für oder im Geschäftsstellenbetrieb bereits in Form von Karteikarten oder Formblättern vorhanden sind (vgl. VGO Band II) und für eine Vielzahl von Arbeitsbereichen benötigt werden, sollen übernommen und auf automatisierte Datenträger gespeichert werden

Mit den derzeitigen Arbeitsabläufen in den Vollzugsgeschäftsstellen soll es bei größeren Vollzugsanstalten nicht mehr möglich sein, die Dienstgeschäfte ordnungsgemäß zu erledigen. Dies soll insbesondere für die verwaltungsmäßige Abwicklung bei Urlaub, Ausgang, Strafunterbrechung, Anfragen, Verschubung und Verlegung der Fall sein.

Jede Willensäußerung des Insassen und jede hierauf getroffene Entscheidung ist lückenlos zu dokumentieren. Das Schriftgut soll deshalb einen noch kaum zu bewältigenden Umfang angenommen haben. Gefangenenpersonalakten mit ca. 1000 Blatt (3 Bände) seien deshalb heute keine Seltenheit mehr. Nach den Bestimmungen über die Aufbewahrungsfristen sind die Justizvollzugsanstalten verpflichtet, die Personalakten der Gefangenen 30 Jahre aufzubewahren, zu verwalten und gegebenenfalls zu aktualisieren.

Anfragen an die Vollzugsgeschäftsstelle sollen derzeit aus einer manuell geführten Gefangenenkartei beantwortet werden. Diese Kartei soll in Bremen

zwischenzeitlich einen Umfang von über 100 000 Karten mit durchschnittlich 50 Informationen pro Karte angenommen haben.

Nach Auskunft der Arbeitsgruppe ist zu erwarten, daß voraussichtlich Ende 1988 ADIV auch in Bremen eingeführt und getestet wird.

Bei der Entwicklung und Einführung von ADIV werde ich darauf dringen, daß Fragen der Datensicherheit in ausreichendem Maße Berücksichtigung finden.

Daneben ist aber aus datenschutzrechtlicher Sicht zu berücksichtigen, daß der Gesetzgeber selbst den zulässigen Umfang der Datenverarbeitung, wenigstens deren Rahmenbedingungen festzulegen hat. Mithin darf die Ausgestaltung des Verfahrens nicht allein der Verwaltung überlassen bleiben. Eingriffe in das Recht auf informationelle Selbstbestimmung sind präzise zu bestimmen. Weiter ist eine Transparenz in Bezug auf Verwendungszusammenhänge, bei Datenweitergabe auch beim Datenempfänger, zu fordern.

Die Datenschutzbeauftragten des Bundes und der Länder hatten mit Blick auf das Volkszählungsurteil des Bundesverfassungsgerichts darauf hingewiesen, daß auch im Strafvollzug die Datenverarbeitung einer bereichsspezifischen Normierung bedarf. Das Bundesministerium arbeitet daher an einer Novelle des Strafvollzugsgesetzes. Dementsprechend ist zu erwarten, daß auch Regelungen der Vollzugsgeschäftsordnung geändert oder angepaßt werden müssen. Die durch die Novellierung dann geschaffene neue Rechtslage läßt sich bei der Entwicklung von ADIV jetzt nicht antizipieren. Es kann daher schon bald nach Einführung von ADIV bei den Vollzugsgeschäftsstellen zu größeren, durch die Novellierung verursachte Umstellungen kommen. Auf diese Gefahr und die damit verbundenen Kosten habe ich bereits hingewiesen. Es sollte deshalb überlegt werden, ob die Automatisierung so dringlich ist, daß sie vor Verabschiedung der Novellierung durchgeführt werden soll.

— SIJUS

Ich hatte im letzten Jahresbericht unter Pkt. 5.3.1.2 auf das Bürokommunikationssystem SOJUS (**S**oftwaresystem zur Unterstützung operativer Hilfsaufgaben in der **Ju**stiz) hingewiesen. Dieser Name ist nunmehr in SIJUS — dem Namen eines großen deutschen Elektrokonzerns folgend — geändert worden. Ich habe eine Probevorführung von SIJUS besucht und mir kursorisch unter datenschutzrechtlichen Gesichtspunkten die Möglichkeiten von SIJUS erläutern lassen. SIJUS ist ein Verfahren, das die Arbeiten der Geschäftsstellen in den Staatsanwaltschaften und Gerichten automatisiert. Mit SIJUS kann die Aktenanlage vorgenommen werden, es können Vorlagen, Urteile, Strafanträge und anderes erstellt werden. Die Software wurde von der Gesellschaft für Mathematik und Datenverarbeitung (GMD) entwickelt und dann vom Vertreiber übernommen. Eingesetzt wird die Software auf PC als Mehrplatzsystem (Betriebssystem SINIX, Server, Streamer zur Datensicherung). Der PC hat keinen Peripheriespeicher.

Die Terminals sind weder mit Schloß noch mit Chipkarte gesichert. Dies könnte allerdings nachgerüstet werden. Nach Anmeldung und offener Eingabe des Namens des Benutzers erfolgt eine verdeckte Paßwortprüfung des Benutzers. Ein horizontaler Zugriffsschutz ließe sich durch Aufgliederung in verschiedene sachliche Gebiete herstellen, z. B. Abschottung der Bereiche Geschäftszimmer, Kanzlei usw. Ein Zugriffsschutz durch die Einführung hierarchischer Berechtigungsstufen, wie Auskünfte, Ändern, Systemverwaltung usw. läßt sich realisieren. Eine Protokollierung ist nicht vorgesehen. Zugriffe können einzeln nicht nachgewiesen werden. Ebenso sind Übermittlungen nicht nachvollziehbar.

Aus meiner Sicht wird es erforderlich sein, für jeden PC (Arbeitsplatz) eine Datensicherheitsschale vorzusehen, um zu vermeiden, daß Betriebssystemfunktionen benutzt werden, Sachbearbeiter eigene Programme schreiben und nutzen und unerlaubte Zugriffe durch Protokollierung erkannt werden können.

Bei der Erarbeitung eines Datenschutzkonzeptes wird es vonnöten sein, eine Vorlage zu erstellen, die die beabsichtigte Vernetzung ausweist. Es sind Überlegungen anzustellen, wie die Löschungsfristen für personenbezogene Texte gefaßt werden können, wie dem datenschutzrechtlichen Auskunftsanspruch Rechnung getragen werden kann, wie die Nutzung der Systemakte je Arbeitsplatz sichergestellt werden kann und anderes mehr. Diese Fragen werden in 1988 eingehend zu behandeln sein.

5.4.1.2 Datenübermittlung zur Erstellung eines privaten bundesweiten Handelsregisters

Der Senator für Justiz und Verfassung war an mich herangetreten, ob datenschutzrechtliche Bedenken bestehen, einer Privatfirma das von den Amtsgerichten zu führende Handelsregister vollständig zu überlassen. Die Firma wollte die Handelsregister bundesweit verfilmen und für Auskunftszwecke vermarkten.

Ich habe daraufhin erklärt, daß die Übermittlung personenbezogener Daten das informationelle Selbstbestimmungsrecht der Betroffenen berührt und daher einer hinreichenden Rechtsgrundlage bedarf.

Für die Übermittlung von Daten aus dem Handelsregister enthält § 9 Handelsgesetzbuch (HGB) eine bereichsspezifische Regelung. Hiernach ist die Einsicht in das Handelsregister jedermann ohne Nachweis eines berechtigten Interesses gestattet. Alle Änderungen des Inhalts der Handelsregister werden regelmäßig im Bundesanzeiger veröffentlicht.

Der § 9 HGB vermag eine Übermittlung des gesamten Datenbestandes im Wege der Verfilmung des Registers indessen nicht zu tragen. Die Abnahme des gesamten Registerinhalts zur Gewinnung eines vermarktbaren Produkts kann begrifflich nicht mehr als Einsicht im Sinne von § 9 Abs. 1 HGB angesehen werden.

Durch die Überlassung der Handelsregisterdaten würden damit die örtlichen öffentlichen Handelsregister faktisch in private Hand überführt und zentral zusammengefaßt werden. Diese zentrale Zusammenfassung und die Auswertungsmöglichkeiten nach den verschiedensten Kriterien bilden eine neue Qualität, die vom Gesetzgeber derzeit nicht beabsichtigt ist. Dies gilt auch für die Verfahren der Berichtigung, Überprüfung und Löschung der Daten bei der privaten Firma. Außerdem hat der Gesetzgeber in § 8 HGB zum Ausdruck gebracht, daß das Handelsregister dezentral von den Gerichten geführt wird. Die Errichtung eines zentralen privaten Nebenhandelsregisters entspricht nicht dem Willen des Gesetzgebers.

Die ins Auge gefaßte Verfilmung des Handelsregisters der Amtsgerichte durch eine private Firma ist damit mangels hinreichender Rechtsgrundlage für die Datenübermittlung aus datenschutzrechtlicher Sicht nicht zulässig.

Auf meine Nachfrage über die Handhabung im Lande Bremen erklärte mir der Senator, daß das Amtsgericht Bremen bereits das vollständige Register der Firma überlassen habe.

Ich habe daher diesen Vorgang gegenüber dem Senator beanstandet und ihn gebeten, daß in Zukunft sichergestellt wird, daß vor der Übermittlung solcher umfangreichen Datenbestände an Dritte meine Stellungnahme abgewartet bzw. eingeholt wird.

Ich halte es für selbstverständlich, daß die unzulässig übermittelten Daten weder für das zentrale Handelsregister noch für andere Zwecke genutzt werden und an das Amtsgericht Bremen, soweit Unterlagen versandt wurden, zurückübermittelt werden bzw. daß die Daten bei der Firma gelöscht werden.

5.4.1.3 Wahl von ehrenamtlichen Richtern

Der Senator für Inneres hat mich gebeten, die Vorbereitung der Wahl der ehrenamtlichen Richter am Verwaltungsgericht bzw. Oberverwaltungsgericht unter datenschutzrechtlichen Aspekten zu prüfen.

Nach § 28 Verwaltungsgerichtsordnung (VwGO) stellen die Stadtgemeinde Bremen und die Stadt Bremerhaven je eine Vorschlagsliste auf. Dabei muß § 20 VwGO beachtet werden. § 20 VwGO schreibt vor, daß die ehrenamtlichen Richter die deutsche Staatsangehörigkeit besitzen müssen. Sie sollen das 30. Lebensjahr vollendet und während des letzten Jahres vor der Wahl den Wohnsitz innerhalb des Gerichtsbezirks, also im Lande Bremen, gehabt haben.

Bei der Auswahl der ehrenamtlichen Richter muß darauf geachtet werden, daß keine gesetzlichen Ausschlußgründe vorliegen. Nach der Rechtsprechung des Oberverwaltungsgerichts Bremen dürfen z. B. diejenigen, die ehrenamtlich im öffentlichen Dienst tätig sind, z. B. in Ortsamtsbeiräten, nicht gewählt werden. Mit Rücksicht auf die in § 21 VwGO enthaltenen Anforderungen müssen für jede(n) Bewerber(in) Strafregisterauszüge eingeholt werden.

Vom Statistischen Landesamt (Wahlamt) werden Verbände und Organisationen angeschrieben, Personen für eine Wahlvorschlagsliste zu benennen. Werden nicht

genügend Wahlvorschläge unterbreitet, ist vorgesehen, Bürger aus dem Einwohnermeldebestand mittels einer Stichprobe zu ziehen und in die Vorschlagsliste aufzunehmen.

Das Wahlamt reicht eine Vorschlagsliste über den Senator für Inneres und den Senat an die Stadtbürgerschaft. Die dort beschlossene Vorschlagsliste wird an den Präsidenten der Verwaltungsgerichte geleitet, der gleichzeitig Vorsitzender des Wahlausschusses gemäß § 26 VwGO ist. Danach wählt der Wahlausschuß aus der Vorschlagsliste die ehrenamtlichen Richter.

Ich bin vom Statistischen Landesamt — Wahlamt — gebeten worden, das Verfahren unter datenschutzrechtlichen Gesichtspunkten zu prüfen. Dabei ging es insbesondere um das Verfahren der Erhebung der Daten, die Eingrenzung des Umfanges der Daten und das Überprüfungsverfahren zur Erstellung der Vorschlagsliste. Prinzipiell bin ich von folgenden Voraussetzungen ausgegangen:

— Bei den zu erstellenden Vorschlagslisten gelten datenschutzrechtlich die Prinzipien der Freiwilligkeit. Auch wenn der einzelne Bürger, soweit keine Ausschlußgründe vorliegen, prinzipiell verpflichtet ist, ein solches Ehrenamt anzunehmen, so ist die Gewinnung der Daten bei Organisationen doch nicht mit einer Stichprobe aus dem Melderegister vergleichbar. Das Vorschlagsverfahren muß daher den Grundsätzen der Freiwilligkeit entsprechend ausgestaltet werden.

— Bereits bei der Gewinnung der Daten durch die Organisationen müssen die datenschutzrechtlichen Anforderungen sichergestellt sein.

— Dem Betroffenen müssen alle Stationen der Datenweitergabe und staatlich veranlaßten Überprüfungen (wie z. B. Bundeszentralregisterauszug) vorher bekannt sein.

— Das Verfahren ist nach Möglichkeit so auszugestalten, daß keine Unterschiede erkennbar sind zwischen den auf freiwilliger Basis vorgeschlagenen Bürgern und der aus dem Melderegister gezogenen Stichprobe.

Im einzelnen habe ich darauf hingewiesen, daß bei der Wahl der ehrenamtlichen Richter folgende Punkte zu beachten sind:

— Verfahren der Gewinnung von Kandidaten bei Verbänden und Organisationen.

Da die Kandidatur auf Vorschlagslisten einer Organisation auf freiwilliger Basis beruht, ist bei den Organisationen und Verbänden sicherzustellen, daß bereits hier die datenschutzrechtlichen Anforderungen eingehalten werden. Über die grundsätzliche Freiwilligkeit der Datenangabe muß daher aufgeklärt werden. Dem Betroffenen muß vor seiner Kandidatur klar sein, welches Prüfungsverfahren seitens des Wahlamtes vorgenommen wird.

— Angabe der Berufsbezeichnung

Die Angabe der Berufsbezeichnung ist vom Gesetz nicht zwingend vorgeschrieben. Anders als bei der Schöffenwahl nach § 42 Abs. 2 GVG findet sich in der VwGO keine Bestimmung, nach der bei der Wahl darauf geachtet werden soll, daß alle Gruppen der Bevölkerung nach Geschlecht, Alter, Beruf und sozialer Stellung angemessen berücksichtigt werden müssen. Die Berufsangabe geschieht daher auf freiwilliger Basis. Bei von Organisationen vorgeschlagenen Personen sind diese auf die Freiwilligkeit der Berufsangabe hinzuweisen. Entsprechendes gilt für die Stichprobe aus dem Melderegister.

— Angabe der Anschriften

Die Angabe der Anschriften wird in § 28 VwGO nicht genannt. Diese Angabe ist aber erforderlich, um die Vorgeschlagenen ggf. über ihre Wahl zu unterrichten. Insoweit ist diese Angabe nur für das Wahlamt und den Wahlausschuß erforderlich. Eine Weitergabe der Adressen an den Senat, die Bürgerschaft und den Wahlausschuß ist nicht zwingend erforderlich und daher datenschutzrechtlich nur auf freiwilliger Basis der Einwilligung der Betroffenen zulässig.

— Angabe des Arbeitgebers

Eine Rechtsgrundlage für die Angabe des Arbeitgebers gibt es nicht. Die generelle Frage nach der Beschäftigungsstelle ist daher nicht zwingend vorgeschrieben, vielmehr würde es ausreichen, den Betroffenen zu befragen, ob er im öffentlichen Dienst oder einer der sonst in § 22 VwGO genannten Stellen angehört oder eine ehrenamtliche Beschäftigung im öffentlichen Dienst bekleidet.

FFD 121,163

Diese Angaben sind nur vom Wahlamt zu erheben und nicht an die Bürgerschaft oder den Wahlausschuß weiterzugeben, andernfalls ist die Freiwilligkeit der Angabe sicherzustellen.

— Angabe des Vorschlagträgers

Eine Rechtsgrundlage für die Angabe des Vorschlagträgers gibt es nicht. Der Umstand, daß die Vorschlagsträger bei der Wahl ungleichmäßig berücksichtigt werden könnten, rechtfertigen die Angabe nicht. Im Gegensatz zur Schöffenwahl gemäß § 42 Abs. 2 GVG findet der Ausgewogenheitsgrundsatz über einen repräsentativen Querschnitt der Bevölkerung keine Anwendung; erforderlich ist nur, daß eine Wahl und keine Auslosung stattfindet. Auch ist fraglich, ob die Angabe des Vorschlagträgers dazu führen würde, daß alle Vorschlagsträger gleichmäßig berücksichtigt werden. Um eine gewisse repräsentative Streuung zu erreichen, reicht die Angabe von Beruf und Alter durchaus aus.

— Gestaltung der Vorschlagslisten

Bei den Vorschlagslisten, die dem Wahlausschuß zugeleitet werden, ist darauf zu achten, daß die mittels einer Stichprobe aus dem Melderegister gewonnenen Personen nicht gekennzeichnet werden. Für eine solche Differenzierung besteht kein Anlaß.

— Einholung der Bundeszentralregisterauskünfte gemäß § 41 Abs. 1 Nr. 1 BZRG

Zunächst war geplant, daß das Wahlamt über den Senator für Inneres die Bundeszentralregisterauskünfte einholt, um festzustellen, ob die von den Organisationen Vorgeschlagenen auch wählbar sind.

Eine beschränkte Auskunft aus dem Bundeszentralregister (BZRG) ist nicht möglich, weil gemäß § 21 Nr. 1 VwGO vom Amt des ehrenamtlichen Richters diejenigen Personen ausgeschlossen sind, die wegen einer vorsätzlichen Tat zu einer Freiheitsstrafe von mehr als 6 Monaten verurteilt wurden. Unter bestimmten Voraussetzungen werden hingegen gemäß § 32 Abs. 2 Nrn. 6 und 7 BZRG Freiheitsstrafen bis zu zwei Jahren in das Führungszeugnis nicht aufgenommen. Daraus folgt, daß die Führungszeugnisse gemäß § 31 BZRG nicht in jedem Fall vollständige Auskunft über das Vorliegen der Voraussetzungen des § 21 VwGO geben.

Um den Gerichten zur Vorbereitung der Wahl eine unbeschränkte Registerauskunft zu ermöglichen, wurde durch das zweite Änderungsgesetz in § 42 Abs. 1 Nr. 1 BZRG das Wort „Gerichtsvorstände" eingefügt (vgl. BT-Drs. 10/319).

In einer Besprechung mit dem OVG-Präsidenten und Vertretern des Senators für Justiz und Verfassung und des Senators für Inneres habe ich Übereinstimmung dahingehend erzielt, daß die vom Wahlamt zu erstellenden Vorschlagslisten — soweit vom Betroffenen angegeben — folgende Daten enthalten dürfen: Familienname (ggf. Geburtsname), Vorname, Geburtsdatum, Geburtsort, Anschrift, ausgeübter Beruf, Arbeitgeber, Bezeichnung der vorschlagenden Institution.

Der Senator für Inneres wird ein Formular erarbeiten. In dieses Formular können alle Interessenten die o. g. Daten freiwillig eintragen. Ferner wird in dieses Formular ein Passus aufgenommen, wonach der Interessent sich damit einverstanden erklärt, daß die fraglichen Daten im weiterem Verfahrensablauf den Beteiligten (dem Senator für Inneres, dem Senat, der Stadtbürgerschaft, dem Wahlausschuß) mitgeteilt werden und daß zur Prüfung der Ausschlußgründe gemäß § 21 VwGO eine unbeschränkte Bundeszentralregisterauskunft eingeholt wird.

Dazu ist vereinbart worden, daß die zuständigen Präsidenten die unbeschränkte Auskunft aus dem Bundeszentralregister einholen und die Auskünfte auswerten. Soweit dies dazu führt, daß ein vorgeschlagener Kandidat nicht wählbar ist, wird das Ergebnis dem Wahlamt mitgeteilt, damit die entsprechende Person aus der Vorschlagsliste gestrichen werden kann. Die Auszüge sind unmittelbar nach Auswertung zu vernichten.

Wegen des Verfahrens der Auskünfte aus dem Bundeszentralregister habe ich mich an den Bundesbeauftragten für den Datenschutz gewandt. Zur Überprüfung der Voraussetzung nach § 21 VwGO benötigen die Gerichtspräsidenten lediglich die Information, ob Ausschlußgründe vorliegen oder nicht. Da die Vorschrift kein Ermessen vorsieht, benötigen sie hingegen nicht eine vollständige Auflistung aller Einträge. Ich habe den Bundesbeauftragten daher gebeten, sich beim Bundeszentralregister dafür zu verwenden, daß für diese Belange ein gesondertes, den datenschutzrechtlichen Anforderungen entsprechendes Verfahren eingerichtet wird.

5.4.1.4 Bekanntgabe von Grundbuchdaten bei Miteigentum an Grundstücken

Immer wieder beschweren sich Grundstückseigentümer, die Miteigentum an Grundstücken haben (z. B. Eigentumswohnungen), daß bei einem neuen Eintrag in das Grundbuch oder bei der Neuanlegung eines Grundblattes die Nachbarn durch die Übersendung eines vollständigen Auszuges auch über die finanziellen Belastungen des Grundstückes Kenntnis erhalten.

Ich halte das bisher geübte Verfahren, das sich auf § 55 Grundbuchordnung (GBO) stützt, für unbefriedigend.

§ 55 GBO ist zwar eine spezielle Rechtsnorm, die den allgemeinen Vorschriften der Datenschutzgesetze vorgeht, § 55 GBO ist aber auch im Lichte des Rechts auf informationelle Selbstbestimmung auszulegen. Nach dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz, der bei jedem Eingriff in die Rechtsphäre des Betroffenen zu beachten ist, müssen sich die Beteiligten nach § 55 GBO bei zu übersendenden Mitteilungen auf diejenigen Eintragungen beschränken, die die Rechte dieses Beteiligten betreffen. Uberlegungen, die im Hinblick auf § 12 GBO darauf hinweisen, daß dem Miteigentümer ohnehin ein Einsichtsrecht in das Grundbuch zustehe, liegen neben der Sache, denn § 12 GBO gibt nur bei Vorliegen eines berechtigten Interesses dem Verfahrensbeteiligten das Recht auf Einsicht in das Grundbuch bzw. auf einen Grundbuchauszug. Mit dieser Vorschrift wird jedoch nicht die Versendung eines vollständigen Auszuges von Amts wegen begründet.

Nach meiner Kenntnis wird derzeit beim Bundesjustizministerium an einer Novellierung der Grundbuchordnung gearbeitet, die auch datenschutzrechtliche Aspekte berücksichtigen soll. Solange eine entsprechende Regelung aber nicht in Kraft ist, empfehle ich eine verfassungskonforme Anwendung des § 55 GBO.

5.4.2 Kurze Darstellung von Problemen und Beschwerden

5.4.2.1 Forschungsvorhaben

Wie in den Jahren zuvor bin ich auch im letzten Jahr um datenschutzrechtliche Stellungnahme zu verschiedenen Forschungsprojekten im Justizbereich gebeten worden. Hierbei geht es in der Regel um den Zugang zu Akten und Urteilen. Je nach Ausgestaltung des einzelnen Forschungsprojektes sind verschiedene Datenschutzmaßnahmen möglich. Die Justizbehörden können die Gewährung von Akteneinsicht von Auflagen abhängig machen. Die neue Regelung des § 21 BrDSG, die den Datenschutz bei Forschungsvorhaben regelt, ist erst seit kurzem in Kraft, inwieweit sie den Interessenkonflikt zwischen Forscher und Betroffenen hinreichend ausgleicht, wird sich erst in Zukunft in der Anwendung beweisen.

5.4.2.2 Verwendung von Paketmarken in der Justizvollzugsanstalt

Mit der Verwendung von Paketmarken in Justizvollzugsanstalten hatte ich mich aufgrund einer Eingabe erneut auseinanderzusetzen. Ein Häftling beschwerte sich darüber, daß er bei einer Bücherbestellung über einen Fachverlag eine von der Vollzugsanstalt ausgegebene Paketmarke gleichzeitig mit seiner Bestellung absenden muß. Er hält eine solche Verfahrensweise, durch das der Buchverlag über seine Inhaftierung Kenntnis erlangt, für außerordentlich bedenklich.

Bereits in meinem 7. Jahresbericht unter Pkt. 5.3.2 hatte ich die ausnahmslose Verpflichtung zur Verwendung von Paketmarken für datenschutzrechtlich bedenklich gehalten. Paketmarken werden in anderen gesellschaftlichen Bereichen nicht verwandt, somit ist der Strafgefangene in der Regel gezwungen, bei Bestellungen o. ä. gegenüber Dritten seine Identität als Insasse einer Vollzugsanstalt preiszugeben.

Darüber hinaus kommt hinzu, daß einerseits die Vollzugsanstalt keinerlei Auskünfte über den Gefangenenstatus eines Betroffenen geben darf, andererseits der Gefangene aber selbst gezwungen wird, Dritten seinen Status preiszugeben.

Aufgrund meiner Initiative wurde damals darauf verzichtet, für den Bezug von Zeitungen und Zeitschriften über den Postzeitungsdienst oder im Abonnement Paketmarken zu erheben.

Beim Senator für Justiz und Verfassung hatte ich nunmehr aufgrund der erneuten Eingabe angeregt, bei den Bezug von Büchern ebenso zu verfahren.

Er teilte mir in einer Stellungnahme mit, daß auf der Anstaltsleiterkonferenz vom 25. 09. 1987 die Angelegenheit nochmals ausführlich erörtert worden ist. Es wurde ergänzend darauf hingewiesen, daß bei dem Verzicht auf Paketmarken im Falle

der Zusendung von Büchern durch Versandhäuser häufig Bestellungen von Gefangenen aufgegeben würden, die dann von diesen nicht bezahlt werden können. Unter Berücksichtigung, daß die Verwendung von Paketmarken rechtlich zulässig sei und unter Beachtung der Bedenken sieht er sich nicht in der Lage, meiner Anregung zu folgen.

5.4.2.3 Datenschutz und Öffentlichkeit in der Gerichtsverhandlung

Ein Bürger hat sich mit der Bitte an mich gewandt zu prüfen, ob es sich mit den Datenschutzgesetzen vereinbaren läßt, wenn er als Angeklagter im Strafprozeß vor der Öffentlichkeit seinen Namen, Adresse, Geburtsdatum bekanntgeben muß, wenn er nach seinen Einkommens- bzw. Vermögensverhältnissen gefragt wird und dazu noch offenbaren soll, wie hoch das Einkommen der Ehefrau ist oder ob nicht auf Antrag die Öffentlichkeit von der Gerichtsverhandlung ausgeschlossen werden kann.

Die aufgeworfenen Fragen beurteilen sich nach den Vorschriften der §§ 169 ff. Gerichtsverfassungsgesetz (GVG), die die Öffentlichkeit der Hauptverhandlung bei Straf- und Zivilgerichten zum Gegenstand haben. Nach diesen Vorschriften ist die Öffentlichkeit der Hauptverhandlung zur Kontrolle des Gerichtsverfahrens durch die Allgemeinheit zwingend vorgesehen. Die Öffentlichkeit der Verhandlung ist eine wesentliche Bedingung des öffentlichen Vertrauens zur Rechtsprechung der Gerichte, sie soll verhindern, daß die Tätigkeit der Gerichte hinter verschlossenen Türen ohne demokratische Kontrolle stattfinden kann. Die Öffentlichkeit des Verfahrens gehört daher zu den grundlegenden Einrichtungen des Rechtsstaates.

Das GVG sieht in einigen Fällen Ausnahmen von diesem Grundsatz vor, so daß gemäß § 172 Nr. 2 GVG die Öffentlichkeit ausgeschlossen werden kann, wenn Umstände aus dem persönlichen Lebensbereich eines Prozeßbeteiligten oder Zeugen zur Sprache kommen, durch deren öffentliche Erörterung überwiegende schutzwürdige Interessen der Betroffenen verletzt werden würden. Diese Ausschließungsmöglichkeit sucht einen Kompromiß zwischen dem hohen rechtsstaatlichen Wert der Öffentlichkeit der Verhandlung einerseits und dem gebotenen Schutz der persönlichen Würde des einzelnen andererseits. Durch die vom Verfahrensrecht her gebotene Erörterung in der Öffentlichkeit ist der Betroffene daher nicht schutzlos der öffentlichen Neugier und der sich daraus zusätzlich leicht ergebenden nachteiligen Folgen für sein Ansehen oder seine persönliche Entfaltung ausgeliefert. Bei dem Ausschluß der Öffentlichkeit muß es sich aber um Umstände handeln, die für die Beeinträchtigung der Privatsphäre von einem erheblichen, über das allgemein übliche und notwendige hinausgehendem Gewicht sind (z. B. die Aussage eines Opfers eines Sexualdeliktes).

Inwieweit im Verfahren das Einkommen der Ehefrau des Angeklagten offenbart werden muß, hängt davon ab, ob diese Angabe zur Entscheidungsfindung für das Gericht von Bedeutung ist.

Die Vorschriften über die Öffentlichkeit bestehen im öffentlichen Interesse und sind daher den Parteien und damit auch dem Angeklagten der Disposition entzogen (weitere Überlegungen zu diesem Thema habe ich im 9. Jahresbericht in Anlage 4 Pkt. 2.3 abgedruckt). Ich habe den Bürger darauf hingewiesen, daß das Gericht über den Antrag zum Ausschluß der Öffentlichkeit entscheidet.

5.4.2.4 Telefonische Datenerhebung im Strafverfahren durch Gerichte bei unbeteiligten Dritten

Anläßlich einer Beschwerde hatte ich mich mit der Frage zu beschäftigen, ob und inwieweit ein Strafrichter berechtigt ist, Auskünfte über einen ehemaligen Mitarbeiter einer Bildungsgemeinschaft vom Personalsachbearbeiter im Zuge eines Prozesses wegen Verletzung der Unterhaltspflicht telefonisch zu erfragen.

Der Richter wollte wissen, warum der ehemalige Beschäftigte seine auf ein Jahr abgeschlossene Arbeitsbeschaffungsmaßnahme nicht fortgesetzt hat bzw. warum keine Verlängerung durch den Arbeitgeber beantragt worden ist. Ferner wurde er gefragt, ob der frühere Beschäftigte sich arbeitslos gemeldet habe.

Der Mitarbeiter der Bildungsgemeinschaft hat die telefonische Beantwortung der Frage abgelehnt und eine schriftliche Anfrage seitens des Gerichts verlangt. Weiter hatte er im Telefonat darauf hingewiesen, daß für Einstellungen und Entlassungen er nicht zuständig sei., sondern vielmehr dies Sache der Geschäftsleitung bzw. des Vorstandes der Einrichtung sei.

Gemäß § 24 BDSG trifft den Arbeitgeber die Verpflichtung bei der Übermittlung von Arbeitnehmerdaten an Dritte zu prüfen, ob diese ein berechtigtes Interesse

FFD 12/1 A 63

an der Kenntnis der Daten geltend machen und ob durch diese die schutzwürdigen Belange des Betroffenen an einer Geheimhaltung zurückgedrängt werden können. Um dieser Verpflichtung nachzukommen ist Voraussetzung, daß sich der Arbeitgeber davon überzeugen kann, wer Daten von ihm erfahren will und ob dieser Person ein Fragerecht zusteht.

Es ist in Gerichtsverfahren durchaus üblich, daß ein Richter — im Wege einer Vorabklärung — zunächst prüft, ob ein in Frage kommender Zeuge, der ggf. geladen werden soll, prozeßrelevante Tatsachen mitteilen kann.

Zum Umfang der Auskunftspflicht des Arbeitgebers gehört es, dem Gericht gegenüber Fragen zu beantworten, die zur Klärung eines Tatvorwurfes z. B. bei einer Straftat gemäß § 170 b StGB (Verletzung der Unterhaltspflicht) erforderlich sind. In der Regel geht es in diesem Zusammenhang darum, daß das Gericht beurteilen muß, ob der Täter sich seiner Leistungspflicht entzieht.

Ob ein ehemaliger Arbeitnehmer sich arbeitslos gemeldet hat, entzieht sich meist der Kenntnis des Arbeitgebers, darüber hinaus betrifft diese Tatsache ein Verhältnis Arbeitnehmer zum Arbeitsamt. Die Arbeitsämter sind gemäß § 76 f. SGB X den Gerichten gegenüber auskunftspflichtig, gegenüber dem ehemaligen Arbeitgeber u. a. gemäß § 35 SGB I zur Geheimhaltung dieser Tatsachen verpflichtet.

Unter datenschutzrechtlichen Gesichtspunkten ist es nicht nur wünschenswert, sondern zur Vermeidung eines Verstoßes gegen datenschutzrechtliche Vorschriften unerläßlich, daß in den Fällen, in denen ein Anrufer dem Betroffenen nicht bekannt ist oder sonst z. B. die Zuständigkeit des Anrufers in der Sache nicht überprüfen kann, keine telefonischen Auskünfte erteilt werden, sondern auf eine schriftliche Anforderung von dem zuständigen Organ die Fragen beantwortet werden.

Ich habe dem Betroffenen meine Ausführungen dargelegt.

5.4.2.5 Aktenvernichtung bei den ordentlichen Gerichten

Aufgrund einer Anfrage der Präsidialabteilung des Amtsgerichtes Bremen hatte ich zu prüfen, welche Anforderungen an eine Aktenvernichtungsanlage zu stellen sind.

Derzeit erfolgt eine Vernichtung beim Landgericht auf einer Anlage, die gemeinsam vom Amts- und Landgericht sowie der Staatsanwaltschaft genutzt wird. Bei einer Inaugenscheinnahme dieser Anlage, die sich im Keller des Landgerichts befindet, habe ich festgestellt, daß die räumlichen Gegebenheiten verschließbar waren und die Anlage von einem vorherbestimmten Personenkreis zu bedienen ist. Nach Auskunft der Beschäftigten fallen jährlich ca. 60 Tonnen Altpapier an. Die Zerreißergebnisse fallen so fein aus, daß sie einen datenschutzgerechten Standard erreichen.

Eine neue Aktenvernichtungsanlage soll im Amtsgericht aufgestellt werden. Ein Zerreißmuster dieser Anlage konnte ich in Augenschein nehmen. Die Schnipselgröße habe ich für ausreichend klein erachtet, zumal ein Schrägschnitt der Akten dazu führt, daß niemals ganze Zeilen nach dem Vernichtungsvorgang noch lesbar sind.

5.4.2.6 Telefonische Auskünfte der Staatsanwaltschaft an Dritte

Ein Rechtsanwalt bat mich, den nachfolgend geschilderten Geschehnissen nachzugehen.

Sein Mandant erhielt ein Schreiben, in dem er von einem Kreditinstitut als Täter eines Scheckdiebstahls bezeichnet und von ihm Schadensersatz gefordert wurde. Da der Mandant aus verschiedenen Gründen unmöglich der Täter sein konnte, wies er die Vorwürfe unverzüglich zurück und verlangte von dem Kreditinstitut Aufklärung darüber, wer ihn als Täter benannt hatte. Das Kreditinstitut teilte mit, von der Staatsanwaltschaft sei sein Name telefonisch auf Anfrage zu dem diesbezüglichen Aktenzeichen mitgeteilt worden.

Die Prüfung durch die Staatsanwaltschaft hat folgenden Verfahrensverlauf ergeben:

Das Kreditinstitut hatte sich als Geschädigte nach dem Stand eines Ermittlungsverfahrens erkundigt und dabei ein bei der Staatsanwaltschaft nicht vorhandenes Geschäftszeichen angegeben. Die Anfrage war deshalb der zentralen Namenskartei (CANASTA) vorgelegt worden. Dabei wurde das Aktenzeichen im Bestand unter einem anderen Jahrgang als von dem Kreditinstitut angegeben aufgefunden.

FFD.12/163

Dies Aktenzeichen wurde dann als vermeintlich richtiges Aktenzeichen der Geschäftsstelle mitgeteilt. Dem Dezernenten sind dann die Akten vorgelegt worden, er hat die Anfrage des Kreditinstituts fernmündlich beantwortet, ohne sich zu vergewissern, ob ihm tatsächlich die richtigen Akten vorgelegt worden waren.

Das Kreditinstitut hat inzwischen anerkannt, daß der Betroffene als Täter nicht in Frage kommt, das Verfahren, insbesondere eine telefonische Auskunft, erschien dem Rechtsanwalt unter datenschutzrechtlichem Aspekt jedoch bedenklich.

Aufgrund der Auswertung der eingeholten Stellungnahmen kam ich zu dem Ergebnis, daß es bei der Staatsanwaltschaft zu einer bedauerlichen Verwechslung der Aktenzeichen gekommen ist und es sich um ein Versehen im Einzelfall handelt. Dadurch, daß die Staatsanwaltschaft gegenüber der Sparkasse den Namen genannt hat, hat sie gleichzeitig zu erkennen gegeben, daß dieser im zentralen Nachweissystem der Staatsanwaltschaft CANASTA gespeichert ist.

Grundsätzlich beurteilt sich die telefonische Auskunft in solchen Fällen nach § 406e Abs. 5 StPO. Danach kann bei Vorliegen eines berechtigten Interesses dem Verletzten Auskünfte und Abschriften aus den Akten erteilt werden. Nr. 185 Abs. 4 RiStBV konkretisiert dazu, daß einfach und schnell zu erledigende Auskünfte Privatpersonen, insbesondere den Geschädigten oder privaten Einrichtungen erteilt werden können, wenn ein berechtigtes Interesse an einer Auskunftserteilung dargelegt ist und wenn sonst keine Bedenken bestehen.

Diesen Vorgang habe ich zum Anlaß genommen, die Staatsanwaltschaft darauf hinzuweisen, daß bei entsprechenden telefonischen Auskünften unbedingt sichergestellt sein muß, daß nur zum Empfang solcher Mitteilungen wirklich berechtigte Personen entsprechende telefonische Auskünfte aus der Akte erhalten. Dies ist in der Regel durch telefonischen Rückruf zu gewährleisten.

Dem Rechtsanwalt habe ich mitgeteilt, daß, wenn der Sparkasse als Verletzte (Scheckdelikt/Diebstahl) vom zuständigen Dezernenten der Staatsanwaltschaft die Auskunft aus der Akte mit dem richtigen Aktenzeichen gegeben worden wäre, ich gegen eine solche Übermittlung keine Bedenken erhoben hätte.

5.5 Bildung, Wissenschaft und Kunst

5.5.1 Änderung des Bremischen Hochschulgesetzes

Gegenwärtig wird vom Senator für Bildung, Wissenschaft und Kunst eine umfangreiche Novellierung des Bremischen Hochschulgesetzes vorbereitet. Geplant ist dabei auch, die Vorschrift des § 37 Abs. 2 Nr. 1 Bremisches Hochschulgesetz zu streichen, wonach die Immatrikulation eines Studienbewerbers versagt werden kann, wenn er die Erhebungsbögen für die Hochschulstatistik (Studentenstatistik) nicht ausgefüllt vorlegt. Begründet wird diese Streichung mit der geplanten Umstellung des Erhebungsverfahrens bei der Studentenstatistik: Nicht mehr die Studienbewerber bzw. Studenten sollen die statistischen Bögen ausfüllen, d. h. auskunftspflichtig sein, sondern die einzelnen Hochschulen (Umstellung der statistischen Datenerhebung von einer Primärerhebung auf eine Sekundärerhebung).

Derzeit ist nicht absehbar, wann der Bundesgesetzgeber das Hochschulstatistikgesetz ändert, das den Anforderungen, die das Bundesverfassungsgericht in seinem Urteil zum Volkszählungsgesetz 1983 aufgestellt hat, nicht entspricht und dringend der Novellierung bedarf; vgl. hierzu die Ausführungen im 8. Jahresbericht unter Pkt. 5.2.4.5. Im Hinblick auf das Volkszählungsurteil des Bundesverfassungsgerichts ist es — auch nach der Novellierung des Bremischen Datenschutzgesetzes — dringend erforderlich, spezifische Datenschutzregelungen im Bremischen Hochschulgesetz vorzusehen. Diese Regelungen sollten insbesondere den Umfang der Datenerhebung und die Übermittlung studentischer Daten sowie der Daten anderer Hochschulpersonen beinhalten. Der Senator für Bildung, Wissenschaft und Kunst hat in dem bisher vorliegenden Entwurf zum Bremischen Hochschulgesetz keine Datenschutzregelungen aufgenommen. Ich gehe allerdings davon aus, daß dies nachgeholt wird.

5.5.2 Aufbewahrung und Vernichtung von Datenmaterial aus Forschungsvorhaben

Aufgrund von Beschwerden und Presseveröffentlichungen wurde mir bekannt, daß personenbezogenes Datenmaterial aus einem Forschungsprojekt der Universität Bremen nicht ordnungsgemäß aufbewahrt und zur Vernichtung gegeben worden ist. Das Datenmaterial war in die Hände unbefugter Personen (Studenten) gelangt. Nach Überprüfung des Vorgangs mußte ich dies als Verstoß gegen beste-

hende Datenschutzvorschriften beanstanden und die Universität Bremen auffordern, umgehend interne Anweisungen zur Aufbewahrung und Vernichtung personenbezogenen Datenmaterials aus Forschungsprojekten zu erlassen.

Die Universität Bremen hat inzwischen — gestützt auf § 9 Abs. 2 BrDSG — eine Dienstanweisung zur Durchführung von Projekten/Forschungsvorhaben mit personenbezogenen Daten und zur Aufbewahrung und Vernichtung personenbezogenen Datenmaterials erarbeitet und Anfang 1988 in Kraft gesetzt. Ich habe zu dem Entwurf Stellung genommen; meinen Anregungen wurde weitgehend gefolgt.

Die Dienstanweisung sieht im wesentlichen folgende Regelungen vor:

— Anzeigepflicht von Forschungsvorhaben beim Datenschutzbeauftragten der Universität,

— Regelungen zur Aufbewahrung und Verwaltung von Daten und Unterlagen,

— Regelungen zur Vernichtung von Unterlagen und Löschung von Daten sowie

— Regelungen zur Verantwortlichkeit.

5.6 Jugend und Soziales

5.6.1 Programmierte Sozialhilfe (PROSOZ)

Mit dem Projekt „Programmierte Sozialhilfe — PROSOZ —", ein dialogorientiertes Sozialhilfeberechnungsverfahren über Arbeitsplatzrechner in Verbindung mit dem Zentralrechner im RbV, habe ich mich auch im Berichtszeitraum weiter befaßt. Auf die besonderen Probleme und Gefahren im Hinblick auf den Datenschutz habe ich in den vergangenen Jahresberichten wiederholt hingewiesen (vgl. 8. und 9. Jahresbericht unter Pkt. 5.7.1.1 und 5.5.1.2).

Zwischenzeitlich ist innerhalb der Projektgruppe PROSOZ eine Arbeitsgruppe eingerichtet worden, an der ich beratend beteiligt bin. Ziel dieser Arbeitsgruppe ist es, auf der Basis zweier Gutachten ein Datenschutzkonzept zu erstellen. Die Arbeitsgruppe hat bisher besondere Elemente für ein Datenschutzkonzept ausgearbeitet. Dabei hat sie über die bereichsspezifischen Regelungen hinaus die weitergehenden Intentionen des Bremischen Datenschutzgesetzes berücksichtigt. Es bestand insoweit Einigkeit auch mit den Vertretern des Senators für Jugend und Soziales. Bisher wurden u. a. folgende Schwerpunkte bzw. Details festgelegt:

— Alle für PROSOZ verwendeten personenbezogenen Dateien werden auf dem Host-Rechner gespeichert. Der PC beinhaltet lediglich den letzten bearbeiteten Fall. Dieser wird überschrieben, sobald ein neuer Fall bearbeitet wird.

— Für die Zuteilung der Zugriffsberechtigung ist ein zentraler Koordinator vorgesehen.

— Es wird nach Stadtregionen je ein betrieblicher Datenschutzbeauftragter benannt, der allerdings diese Funktion in Kooperation zu anderen Aufgaben ausführen wird.

— Der einzelne PC erlaubt keine weitere Bearbeitung neben PROSOZ. Die Sachbearbeitung wird über ein festes Menue gesteuert.

— Es wird noch geklärt, wie Programmodifikationen bzw. Änderungen dem Einzel-PC zugeführt werden. Es kommen dafür entweder Disketten in Frage, die vom Koordinator geladen und dann wieder eingezogen werden oder aber feste sogenannte Disk-Packs (transportable Platten, die in ihrer Identifizierung mit dem Einzelgerät koordiniert sind). D. h. im letzteren Falle kann die Abnahme eines Packs nicht dazu führen, daß dessen Inhalt unbefugt auf anderen Geräten verwendet bzw. verarbeitet werden kann.

— Es wird überlegt, ob eine Datenschutz-Software sozusagen als Schale über das Betriebssystem je Rechner installiert wird.

— Ein Mailbox-System ist für PROSOZ nicht geplant, so daß eine Kommunikation der einzelnen Sachbearbeiter über ihren PC bzw. über den Host-Rechner nicht erfolgt.

— Eigene Programme (private) können am PC nicht verwendet werden, da die Möglichkeit des Disketteneinschubs verhindert werden soll (Abschließen des Diskettenlaufwerkes bzw. Verwendung von Disk-packs).

— Besonderer Regelung bedarf die Aufbereitung und Auswertung personenbezogener Dateien für statistische Zwecke.

Die Arbeitsgruppe befindet sich noch im Diskussionsprozeß. Ein vorläufiger Gliederungsentwurf für das Datenschutzkonzept wird erörtert. Ich gehe davon aus, daß das Konzept bis zum Beginn des Probelaufs fertiggestellt und mit mir abgestimmt ist.

5.6.2 Kurze Darstellung von Problemen und Beschwerden

— Ein Beschwerdeführer wandte sich dagegen, daß im Rahmen einer beim Sozialamt Bremerhaven beantragten Hilfe für ein orthopädisches Hilfsmittel für seine Lebensgefährtin die gemeinsame Sozialhilfeakte an das Gesundheitsamt Bremerhaven zur Prüfung der Erforderlichkeit dieses Hilfsmittels weitergeleitet worden ist.

  Ich habe das Sozialamt Bremerhaven darauf hingewiesen, daß in diesem Falle eine Offenbarung des Sozialgeheimnisses nach § 69 Abs. 1 Nr. 1 SGB X nur zulässig ist, soweit sie erforderlich ist für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch. Danach war die Weiterleitung der Sozialhilfeakte nicht erforderlich, weil das Gesundheitsamt Bremerhaven für seine Aufgabe lediglich Name und Anschrift der betroffenen Person sowie die Angabe des Hilfsmittels benötigt.

  Das Sozialamt hat erklärt, künftig so zu verfahren.

— Eine Eingabe richtete sich dagegen, daß eine Sozialhilfesachbearbeiterin eines Ortsamtes der Leiterin eines Frauenhauses telefonisch mitgeteilt hat, eine Bewohnerin des Frauenhauses sei wahrscheinlich an Syphilis erkrankt. Dieses habe sie über den Ehemann der Betroffenen erfahren und daraufhin das Frauenhaus gebeten, diese Information an die betroffene Bewohnerin weiterzugeben. Einige Tage später erfuhr die Leiterin des Frauenhauses aus der Meldestelle desselben Ortsamtes, welches für das Frauenhauses zuständig ist, daß dort ebenfalls der Verdacht der Erkrankung bekannt sei.

  Nach Angaben des Leiters des Ortsamtes habe die Sachbearbeiterin — offenbar in Unkenntnis datenschutzrechtlicher Bestimmungen — aus Sorge um die Bewohnerinnen des Frauenhauses und deren Kinder das Frauenhaus informiert. Ihr sei im Nachhinein klar geworden, daß dieses der falsche Weg war und sie sich in ähnlichen Fällen unmittelbar mit der Betroffenen in Verbindung setzen werde.

  Woher die Meldestelle die gleichen Informationen habe, konnte nicht mehr aufgeklärt werden. Der Ortsamtsleiter halte es für möglich, daß das Telefongespräch mit der Leiterin des Frauenhauses mitgehört worden sei. Er habe diesen Vorfall jedenfalls zum Anlaß genommen, auf einer Dienstbesprechung erneut auf die Einhaltung des Sozialgeheimnisses hinzuwirken.

5.7 Gesundheitswesen

5.7.1 Prüfung des Stationären Abrechnungsverfahrens (StAB)

Die technisch-organisatorische Prüfung des StAB-Verfahrens wurde in zwei Stufen vorgenommen. In der ersten Stufe wurden in drei ausgewählten Krankenhäusern (ZKH St.-Jürgen-Straße, ZKH Bremen-Nord, ZKH „Links der Weser") Prüfungen durchgeführt. Die zweite Stufe der Prüfung erfolgte hinsichtlich des DV-technischen Teiles im Rechenzentrum der bremischen Verwaltung (RbV).

Das StAB-Verfahren besteht aus zwei Teilen:

— Dezentral über den Vorschaltrechner IBM-8150 die Erfassung und Auskunftsbereitschaft

— Zentral auf dem Großrechner im RbV die Stapelverarbeitung für die Berechnung der Krankenhausleistungen

Beide Teile sind über Schnittstellenprogramme miteinander verbunden, damit eine online-Stapelübertragung durchgeführt werden kann. Ein Dialog zwischen beiden Teilen ist nicht vorhanden. Die Stapelübertragung beinhaltet den Änderungsdienst für die Abrechnungsdatei mittels Aufnahmedaten der Kliniken, die im Vorschaltrechner zwischengespeichert sind. Für die Stapel-Übertragung vom Zentralrechner zum Vorschaltrechner sind Altsätze, die wieder reaktiviert werden, vorgesehen. Es handelt sich in beiden Fällen um Verwaltungsdaten. Medizinische Daten sind nicht gespeichert.

FFD 12/165

Die Prüfung in den Krankenhäusern umfaßte folgende Schwerpunkte:

— Das Zugriffssystem

— Datenerhebung und -eingabe

— Die Verpflichtung auf das Datengeheimnis

— Räumlichkeiten

— Trennung der medizinischen und Verwaltungsdaten

— Telefondatenerfassung

— Betrieblicher Datenschutzbeauftragter

— Einsatz autonomer Arbeitsplatzrechner.

Es wurden einige Mängel entdeckt, die nach Angabe der Krankenhäuser zwischenzeitlich größtenteils beseitigt worden sind. So wurden in der Sachbearbeitung die abgestuften Zugriffsberechtigungen damit umgangen, daß Sitzungseröffnungen mit einer höheren Zugriffsstufe durchgeführt wurden. Da auf das Sitzungsende verzichtet wurde, konnten Sachbearbeiter mit einer niederen Stufe mit ihren eigenen Transaktionen und mit für sie geschützten Transaktionen weiterarbeiten. Hier wurde anweisungswidrig gehandelt. Da dieses Umgehen des Zugriffsschutzes bei der derzeitigen Verfahrenskonstellation programmäßig nicht zu verhindern ist, bedurfte es hier einer eindringlichen Ermahnung der betroffenen Sachbearbeiter durch die Krankenhausleitung und eines zusätzlichen Umlaufes durch den Senator für Gesundheit.

Eine offensichtlich verbreitete Unsitte der Aufbewahrung des Paßwortes zeigte sich in Einzelfällen auch in den Bereichen der Krankenhäuser. Die persönliche Identifizierung des Sachbearbeiters (Paßwort) konnte hier und da als handschriftliche Eintragung in den Bedienungsunterlagen von Unbefugten entdeckt und damit benutzt werden. Diese „Gedächtnisstütze" wird — nach Angaben der Krankenhäuser — zwischenzeitlich nicht mehr verwendet. Außerdem konnte ich feststellen, daß ein einmal vergebenes Paßwort nicht mehr geändert worden ist. Das erschwerte die Geheimhaltung.

Die Mängel waren durchgängig in allen geprüften Krankenhäuser in Einzelfällen zu verzeichnen.

Im Krankenhaus „Links der Weser" konnte ich zusammen mit einem Bediensteten die Kinderklinik betreten und die Krankenkartei der kleinen Patienten (auch der schon entlassenen) für etwa zehn Minuten einsehen, ohne daß sich verantwortliche Bedienstete in dieser Zeit sehen ließen. Mir wurde erklärt, hier handele es sich um einen Ausnahmefall. Bei einer Nachkontrolle war der entsprechende Raum verschlossen.

Wiederholte Beschwerden aus außer-bremischen Krankenanstalten hinsichtlich der Patientenaufnahme veranlaßten mich, diesen Punkt besonders zu testen. Als Ergebnis kann ich feststellen, daß in den geprüften Bereichen der o. g. Krankenanstalten die Patientenaufnahme in allen geprüften Fällen unter dem Gesichtspunkt des Persönlichkeitsschutzes durchgeführt wurden: Die Aufnahmen erfolgten in geschlossenen Räumen. Draußen wartende Patienten konnten das Aufnahmegespräch nicht verfolgen.

Die Prüfung des programm- und durchführungstechnischen Teiles des StAB-Verfahrens im RbV ergab einige schwerwiegende Mängel. Das RbV arbeitet grundsätzlich im Auftrage und zwar nur den Weisungen des Auftraggebers entsprechend. Der Auftraggeber hat dabei die Pflicht und die Aufgabe, gemäß § 6 Abs. 2 Nr. 8 BrDSG die auftragsgemäße Verarbeitung zu kontrollieren. Die Art der Mängel und die Tatsache, daß sie nicht nur in Einzelfällen erkannt wurden, zeigte, daß diese Kontrolle vom Senator für Gesundheit bzw. von den Krankenhäusern nicht durchgeführt wurde. So war auch in vielen Fällen der Auftraggeber nicht eindeutig zu erkennen; er wechselte zwischen den Krankenhäusern und dem Senator für Gesundheit. Dieses erfordert dringend eine Klarstellung. Zu den Mängeln im einzelnen:

— Unzulässige Übermittlung echter Daten an die Anwendungsentwicklung des RbV

Für Programmieraufträge wurden dem RbV sowohl Formularmuster mit Originaldaten versehen (z. B. Kopien von „echten" Listen) als auch Originaldaten in

den Änderungsanträgen selbst übermittelt. Darüber hinaus wurden Listen mit personenbezogenen Daten aus der monatlichen StAB-Abrechnung dem Anwendungsabschnitt des RbV zur Verfügung gestellt. Inwieweit darüber hinaus weitere personenbezogene Auswertungen der Anwendungsentwicklung übermittelt wurden, konnte nicht abschließend geklärt werden. Diese Offenbarung von Patientendaten gegenüber dem RbV als programmierende Stelle ist rechtlich unzulässig und widerspricht auch den anerkannten Prinzipien einer ordnungsgemäßen Datenverarbeitung. Es wird sowohl die ärztliche Schweigepflicht nach § 203 StGB als auch die Datenübermittlungsbestimmung nach § 1 Abs. 4 BrDSG in Verbindung mit § 24 Abs. 1 BDSG mißachtet.

— Archivierungsprotokolle

Aus den Archivierungs- und Reaktivierungsläufen wurden Protokolle erstellt und u. a. an den Senator für Gesundheit und im RbV (Anwendungsentwicklung) verteilt. Es erfolgten damit Übermittlungen aus dem Originaldatenbestand (Patientendaten) außerhalb der Zweckbestimmung. Inwieweit auch noch zweckentfremdete Speicherungen bei den Empfängern zu verzeichnen sind, konnte nicht festgestellt werden. Dies verstößt gegen die ärztliche Schweigepflicht und die Bestimmungen des § 24 Abs. 1 BDSG.

— Fehlende Änderungsanträge

In der Anwendungsentwicklung des RbV wurden Programmänderungen durchgeführt, ohne daß entsprechende schriftliche Änderungsanträge vorlagen. Mir wurde dargelegt, daß diese Aufträge mündlich bzw. telefonisch erteilt würden. Es konnte jedoch in den Dokumentationsunterlagen kein Hinweis darauf gefunden werden. Es fehlten sowohl Handvermerke als auch die Dokumentation der tatsächlichen Anweisungen des Auftraggebers. Ob und inwieweit das RbV selbst — ohne bzw. abweichend von den Weisungen des Auftraggebers — Programmänderungen durchgeführt hat, konnte nicht festgestellt werden. Ein entsprechender Hinweis darauf, daß der Auftraggeber die weisungsgerechte Durchführung kontrolliert hatte, konnte nicht gefunden werden.

— Verwendung von Originaldaten für Tests

Bei einer stichprobenweisen Prüfung mehrerer Testdateien wurden Extrakte aus Original-StAB-Dateien vorgefunden. In fünf Dateien wurden personenbezogene Originaldaten gespeichert. Es handelt sich dabei u. a. um ärztliche Liquidationsdaten, Nachberechnungsdaten, Stammdaten zur Nachberechnung, Ärzte-Stammdaten. Anweisungen der auftraggebenden Stelle bezüglich dieser durch das RbV selbständig erstellten Auszüge aus den Originaldatenbeständen lagen nicht vor. Mir wurde gesagt, daß es sich hier um mündliche Anweisungen gehandelt hätte; diese Aussage konnte jedoch nicht belegt werden. Eine Anonymisierung dieser Datenbestände wurde nicht vorgenommen. Dazu kam, daß die Extrahierung offensichtlich unter Umgehung der formalen Funktionstrennung im RbV selbsttätig vom Anwendungsabschnitt vorgenommen wurde.

Als Gründe wurden Fehlerbeseitigung, Bestandsbereinigung usw. angegeben. Es hätten anonymisierte Testdaten ausgereicht. Die Verwendung von Originaldaten für Testläufe widerspricht der Ziffer 10.1 der „Anweisung betreffend Planung und Einsatz der automatisierten Datenverarbeitung (ADV) in der bremischen Verwaltung" in der Fassung vom 21. 09. 1981. Hiernach ist Testmaterial, das charakteristische Beispiele des Sachproblems enthält, von der auftraggebenden Stelle zu benennen und der Aufbau eines verfahrensbegleitenden Testbestandes anzustreben.

Der dargestellte Mangel einer ordnungsgemäßen Datenverarbeitung stellt darüber hinaus auch einen Verstoß gegen technische und organisatorische Maßnahmen der Datensicherung (§6 Abs. 2 Nr. 8 und 10 BrDSG) dar. Diese Anforderung verpflichtet auch den Auftragnehmer, die Auftragskontrolle als Folge aus § 8 BrDSG anzusehen. Danach ist die Verarbeitung personenbezogener Daten in allen Phasen der Datenverarbeitung nur im Rahmen der Weisungen des Auftraggebers gestattet. Im übrigen sind diejenigen technischen und organisatorischen Maßnahmen zu treffen, die sicherstellen, daß die Vorschriften des bremischen Datenschutzgesetzes eingehalten werden. Dies gilt insbesondere bezüglich der Speicherung in Testdateien und der Zugriffs- und Übermittlungskontrolle.

Ich habe die dargestellten und bewerteten Mängel der ordnungsgemäßen Datenverarbeitung und die Verstöße gegen das geltende Datenschutzrecht sowohl ge-

genüber dem Senator für Gesundheit als auch gegenüber der Senatskommission für das Personalwesen beanstandet.

5.7.2 Einsatz privater Arbeitsplatzrechner

Ich habe im Jahre 1987 bei allen kommunalen Krankenanstalten angefragt, inwieweit private Personal Computer (Arbeitsplatzrechner) im Einsatz sind. Der Anlaß dazu waren verschiedene Hinweise aus dem Krankenhausbereich, daß von Ärzten private (eigene und von Händlern „leihweise" zur Verfügung gestellte) PC für verschiedene medizinische Aufgaben genutzt werden. Die besondere Datenschutzproblematik bei der Benutzung von PC habe ich wiederholt dargelegt. Die Besonderheit bei Privatrechnern liegt darin, daß diese Rechner und die dort verarbeitete Software und Dateien praktisch unkontrollierbar sind. Diese Rechner sind transportabel und können sowohl am Arbeitsplatz als auch im eigenen Bereich (zu Hause) benutzt werden. Inwieweit bei dieser „offenen" Nutzung das Arztgeheimnis gewahrt bleiben kann, ist nicht festzustellen. Es kann nicht mehr ausgeschlossen werden, daß die ärztliche Schweigepflicht hierbei durchbrochen wird.

Die Antworten der Zentralkrankenhäuser fielen unterschiedlich aus. So wurde teilweise mitgeteilt, daß private PC nicht benutzt werden, während andere Zentralkrankenhäuser die Nutzung privater PC zugaben. In diesen Fällen wurde angegeben, daß die Rechner der Verfügungsgewalt der Krankenhäuser unterstehen. Inwieweit ausstehende Rückantworten den Verdacht zulassen, daß in diesen Krankenanstalten private Rechner genutzt werden, konnte ich bisher nicht feststellen. Es stellt sich für mich als besonders schwierig dar, die Standorte zu erkennen und die Verwendung zu kontrollieren, wenn Krankenanstalten entsprechende Auskünfte nicht geben. Dennoch wird es für den neuen Berichtszeitraum vorrangiges Ziel sein, dies in den Zentralkrankenhäusern zu prüfen.

Außerdem zeigt sich einmal mehr, daß bei dieser Art der Bearbeitung medizinischer und von Verwaltungsdaten dringend eine gesetzliche Regelung in Form des Krankenhaus-Datenschutzgesetzes nötig ist, das auch u. a. die Behandlung und Handhabung von privaten PC beinhaltet. Gerade diese Form der Datenverarbeitung wird von mir als Gefährdungspotential angesehen, dessen Beseitigung dringend erforderlich ist. Gerade bei dieser PC-Nutzung ist für die Praxis klar zu entscheiden, wer datenschutzrechtlich verantwortlich ist und wie dies durch Kontrolle sichergestellt werden kann.

5.7.3 Vernichtung von Formblättern in den Krankenhäusern

Aufgrund einer Beschwerde aus dem Zentralkrankenhaus Bremen-Nord habe ich dort die Vorgehensweise bei der Vernichtung von mit Patientendaten beschrifteten Formularen überprüft.

Es handelt sich bei den genannten Formularen um Befundträger von den Stationen (sogenannte L1- bis L4-Scheine), falsch ausgefüllte bzw. fälschlich abgerollte oder überzählige Formblätter bzw. Entlassungsmitteilungen. Diese mit sensiblen Daten versehenen Scheine werden dem allgemeinen Stationsmüll zugeführt, d. h. sie gelangen in die normalen Verwaltungspapierkörbe, deren Inhalt anschließend in sogenannten Preßcontainern deponiert wird.

Diese Preßcontainer werden, nachdem sie gefüllt sind, von einer Entsorgungsfirma zur Müllverbrennungsanlage in Bremen gebracht und dort in den offenen Bunkern so lange aufbewahrt, bis die Verbrennung stattfindet. Nach Rückfrage in der Verbrennungsanlage wurde mir gesagt, daß der Müll ohne weiteres drei bis vier Tage dort lagern könne und die Möglichkeit nicht auszuschließen sei, daß lose Zettel vom Wind in die Umgebung der MVA getragen würden.

Ich halte die Behandlung der Ausschußmaterialien mit sensiblen Patientendaten für einen Verstoß gegen die ärztliche Schweigepflicht und damit gegen § 203 StGB. Ich habe in diesem Falle jedoch von einer förmlichen Beanstandung abgesehen, da hier — wenn auch etwas leichtfertig — in Unkenntnis der verzögerten Vernichtung gehandelt wurde. Uber den Senator für Gesundheit habe ich die Krankenanstalten aufgefordert, eine separate Vernichtung vorzusehen. Die Vorbereitung dazu wäre die Ablagerung in getrennten, dafür vorgesehenen Papierkörben oder Plastiktüten und eine anschließende Shredderung. Mir ist zugesagt worden, daß eine zentrale Lösung angestrebt wird und ich nach Vollzug Kenntnis erhalte. Zwischenzeitlich wird nach Information des Senators für Gesundheit auch in den anderen kommunalen Krankenanstalten so verfahren. In die Preßcontainer gelangen nunmehr nur noch die zerkleinerten Abfälle.

5.7.4 Datenschutz im Krankenhaus

Die Diskussion um bereichsspezifische Datenschutzregelungen für die Datenverarbeitung in Krankenhäusern ist in Bremen und bundesweit im Gange. Der Senator für Gesundheit hat einen Referentenentwurf erarbeitet, der wohl noch vor der Sommerpause diskutiert werden wird. Ich erinnere in diesem Zusammenhang an die mehrfachen Darstellungen in meinen früheren Jahresberichten. Zur Vorbereitung dieses Entwurfes hat es mehrere Gespräche zwischen dem Senator für Gesundheit und mir gegeben. Eine bewertende Stellungnahme zu diesem Entwurf befindet sich in Vorbereitung und wird erst nach Abschluß dieses Jahresberichtes fertiggestellt werden. Zur Vorbereitung bereichsspezifischer Krankenhausregelungen habe ich im Schwerpunkt folgende Forderungen erhoben:

— Geltung der bereichsspezifischen Datenschutzregelung für alle Krankenhäuser in Bremen

— Regelung der Datenverarbeitungsabläufe innerhalb von Krankenhäusern, wie Erheben, Nutzen, Übermitteln etc.

— Abgrenzung Dokumentation, Verwaltungsdaten, medizinische Daten

— Regelungen bezüglich einzelner Betriebseinheiten und der Datenverarbeitung im Auftrag

— Regelungen hinsichtlich der Datenverarbeitung für Forschung und wissenschaftliche Zwecke

— Erörterung der Notwendigkeit einer Regelung bezüglich Krankheitsregister

— Regelung von technischen und organisatorischen Maßnahmen zur Datensicherung einschließlich der PC-Einsätze, hierzu gehören auch Vorschriften über die Erstellung von Geräteverzeichnissen und Dateibeschreibungen

— Regelung des Rechts auf Auskunft und der Akteneinsicht für den Patienten.

Die umfangreiche automatisierte Datenverarbeitung in den Krankenhäusern erfordert schließlich die Bestellung von Datenschutzbeauftragten für jedes Krankenhaus. Abschließend bedarf es der Regelung von Straf- und Bußgeldvorschriften bei Verstößen gegen Datenschutzbestimmungen. Diese Aufzählung zeigt die wichtigsten Regelungspunkte an.

Der diskutierte Referentenentwurf zu einem Bremischen Krankenhausgesetz enthält diese Punkte überwiegend, ohne daß ich hier jedoch bezüglich des Regelungsinhaltes bereits Festlegungen treffen möchte. Ich gehe davon aus, daß die Beratung des Bremischen Krankenhaus-Datenschutzgesetzes zügig voranschreitet, ich werde meine datenschutzrechtlichen Anforderungen geltend machen.

5.8 Bauwesen

5.8.1 Datenverarbeitung im Baugenehmigungsverfahren

Ein Bürger hat sich mit der Bitte an mich gewandt zu prüfen, ob beim Bauordnungsamt und den am Baugenehmigungsverfahren beteiligten Behörden besondere Daten über ihn gespeichert seien. Zu dieser Vermutung sei er gekommen, weil das Bauordnungsamt ihn im Zusammenhang mit der Erteilung einer Genehmigung zur Erstellung eines Stellplatzes für einen Pkw mitgeteilt habe, daß Nachbarn von der Erteilung der Baugenehmigung in Kenntnis gesetzt worden seien.

Nach meinen Feststellungen hat das Bauordnungsamt auch im vorliegenden Falle nur die personenbezogenen Daten des Antragstellers verarbeitet, die mit dem Antrag auf Erteilung einer Baugenehmigung erhoben worden sind.

Das Bauordnungsamt hat einem Nachbarn mitgeteilt, daß für die Erteilung eines Stellplatzes für Pkw eine Baugenehmigung erteilt worden ist und er als Nachbar innerhalb eines Monats Widerspruch gegen die Baugenehmigung erheben könne. Nach Bekunden des Bauordnungsamtes hat es sich zu dieser Mitteilung veranlaßt gesehen, weil dieser Nachbar sich bereits vor Erteilung der Baugenehmigung gegen das Bauvorhaben gewandt hat. Es hat sich dazu berechtigt gefühlt, weil nur so zu verhindern gewesen ist, daß der rechtliche Bestand der Genehmigung mindestens ein Jahr lang ungewiß geblieben wäre. Eine möglichst schnelle Herstellung der Rechtssicherheit hat nach seiner Ansicht sowohl im öffentlichen als insbesondere auch im Interesse des Antragstellers gelegen.

Im übrigen hat das Bauordnungsamt die personenbezogenen Daten des Betroffenen an solche Behörden übermittelt, deren Aufgabenbereich mit der Erteilung einer Genehmigung berührt werden und die deshalb nach § 92 der Bremischen Landesbauordnung zu hören sind.

Die Bremische Landesbauordnung enthält einige Datenverarbeitungsregelungen und muß deshalb als bereichsspezifische Datenschutzvorschrift angesehen werden. Diese Regelungen erfüllen jedoch nicht die vom Bundesverfassungsgericht an eine das Recht auf informationelle Selbstbestimmung einschränkende Norm gestellten Anforderungen hinsichtlich der Normenklarheit und der Verhältnismäßigkeit.

So regelt z. B. der § 94 dieses Gesetzes, in welchen Fällen Nachbarn im Baugenehmigungsverfahren zu beteiligen sind und für welchen Zweck welche personenbezogenen Daten von Antragstellern in welcher Form an die Nachbarn übermittelt werden sollen, nämlich an Angrenzer vor Erteilung von Befreiungen von baurechtlichen Bestimmungen, wenn deren öffentlich-rechtlich geschützte Belange beeinträchtigt werden könnten. Wenn zu vermuten ist, daß auch öffentlich-rechtlich geschützte Belange weiterer Nachbarn beeinträchtigt werden könnten, sind diesen die personenbezogenen Daten des Antragstellers durch ein öffentliches Auslegungsverfahren bekannt zu machen. Da im vorliegenden Falle der Nachbar nicht Angrenzer war und mit der erteilten Bauerlaubnis auch keine Freistellungen von baurechtlichen Bestimmungen erfolgt sind, war die Übermittlung der personenbezogenen Daten des Antragstellers an den Nachbarn unzulässig. Das Bauordnungsamt hat jedoch verdeutlicht, daß eine solche Interpretation dieser Regelung insoweit verfassungsrechtlich nicht unbedenklich ist, als sie das Recht eines Dritten, Entscheidungen der Verwaltung nachprüfen zu lassen, wenn er sich durch sie in seinen Rechten verletzt fühlt, erheblich einschränkt. Ich habe erhebliche Zweifel, ob das vorgeschriebene Verfahren, nachdem eine Unterrichtung von Nachbarn, die nicht Angrenzer sind, nur über ein öffentliches Auslegungsverfahren erfolgen kann, verfassungskonform ist. Dadurch werden die personenbezogenen Daten einem größeren Personenkreis bekanntgegeben, als es für die Wahrung der Rechte Dritter erforderlich ist. Dieses verletzt m. E. den Verfassungsgrundsatz der Verhältnismäßigkeit.

Die Landesbauordnung schreibt zwar vor, daß vor Erteilung einer Bauerlaubnis die in ihrem Aufgabenbereich berührten Behörden und öffentlichen Stellen von der Baugenehmigungsbehörde zu hören sind, sie enthält jedoch keine Vorschriften darüber, welche personenbezogenen Daten von Antragstellern in welchem Umfange und für welchen Zweck an solche Behörden übermittelt werden dürfen. Die vom Bundesverfassungsgericht geforderte Normenklarheit ist somit bei dieser Vorschrift nicht gegeben.

Der Gesetzgeber bleibt deshalb aufgerufen, die Landesbauordnung, wie in einigen anderen Ländern bereits geschehen, so zu ändern oder zu ergänzen, daß die im Baugenehmigungsverfahren erforderliche Verarbeitung personenbezogener Daten auf eine verfassungsmäßige Grundlage gestellt wird. Die jetzige Situation kann nur noch für eine kurze Übergangszeit hingenommen werden.

5.8.2 Übermittlung eines Gutachtens über den Verkehrswert eines Grundstückes an Pflichtteilsberechtigte

Ein Bürger war als Alleinerbe nach seiner Mutter Eigentümer an einem Grundstück in Bremerhaven geworden. Nachdem zwei Pflichtteilsberechtigte ihm gegenüber einen Pflichtteil geltend gemacht hatten, hat der Betroffene beim Gutachterausschuß des Vermessungs- und Katasteramtes beim Magistrat der Seestadt Bremerhaven einen Antrag auf Erstellung eines Gutachtens über den Verkehrswert des Grundstückes gestellt, dem auch entsprochen worden ist. Der Betroffene hat dann erfahren, daß je eine Ausfertigung des Gutachtens an die beiden Pflichtteilsberechtigten übersandt worden ist, ohne daß diese einen Antrag auf Erstellung eines Gutachtens gestellt haben. Der Betroffene hatte dem Gutachterausschuß vor Fertigstellung des Gutachtens mitgeteilt, daß er das Gutachten zwar noch benötige, jedoch nicht mehr für den Zweck der Erbauseinandersetzung, weil diese durch Einigung mit den Pflichtteilsberechtigten ihre Erledigung gefunden habe. Das Gutachten enthält Angaben über die Vermögensverhältnisse des Grundstückseigentümers.

Der Gutachterausschuß hat als Rechtsgrundlage für die Übermittlung des Gutachtens auch an die beiden Pflichtteilsberechtigten die Vorschriften des § 136 Abs. 5 Bundesbaugesetz (BBauG) genannt. Danach ist er verpflichtet, dem Eigentümer des Grundstücks eine Abschrift des Wertgutachtens zu übersenden. Da die Eigen-

FFD 12/163

tümerin verstorben ist, sei allen Erbberechtigten eine Abschrift zur Kenntnis zu geben. Ein besonderer Antrag hierfür habe nicht vorgelegen und sei auch nicht erforderlich gewesen. Darüber hinaus sei die Äußerung des Alleinerben bezüglich der Erledigung der Erbauseinandersetzung erst nach Fertigstellung und Übersendung des Gutachtens erfolgt. Der Betroffene hat jedoch nachgewiesen, daß seine Mitteilung dem Gutachterausschuß vor Übersendung des Gutachtens übersandt worden ist.

Die Übersendung von Ausfertigungen eines Gutachtens an Pflichtteilsberechtigte stellt die Übermittlung personenbezogener Daten des betroffenen Alleinerben an Stellen außerhalb des öffentlichen Bereichs dar. Eine solche Übermittlung, und somit Einschränkung des Rechts auf informationelle Selbstbestimmung, ist jedoch nur zulässig, wenn eine verfassungsmäßige Rechtsvorschrift sie erlaubt. Als bereichsspezifische Rechtsvorschrift sind auf den vorliegenden Fall die Bestimmungen des § 136 BBauG anzuwenden. Nach dieser Vorschrift hat der Gutachterausschuß ein Gutachten für Pflichtteilsberechtigte zu erstatten, wenn diese es beantragen und der Wert des Grundstücks für einen Pflichtteil von Bedeutung ist. Beide genannten Voraussetzungen müssen erfüllt sein. Da nach den Angaben des Vermessungs- und Katasteramtes in Bremerhaven solche Anträge nicht gestellt worden sind, kann diese Vorschrift die im vorliegenden Falle vorgenommene Übermittlung nicht rechtfertigen.

Nach dieser Vorschrift ist eine Abschrift eines erstatteten Gutachtens an den Eigentümer des Grundstücks oder eines Rechts an einem Grundstück zu übersenden. Da die beiden Pflichtteilsberechtigten zu keiner Zeit Eigentum an dem Grundstück erworben haben, berechtigte diese Bestimmung ebenfalls nicht zur Datenübermittlung.

Gutachten können ganz oder teilweise anderen Personen unter der Voraussetzung zur Kenntnis gebracht werden, daß diese ein berechtigtes Interesse nachweisen und keine berechtigten Interessen anderer beeinträchtigt werden. Der Eigentümer des Grundstücks ist in diesen Fällen vorher zu hören. Diese Vorschrift kann jedoch nicht auf Pflichtteilsberechtigte angewendet werden. Das ergibt sich daraus, daß der Gesetzgeber für diesen Personenkreis eine abschließende Anspruchsregelung getroffen hat, die einen Antrag der Betroffenen und den Nachweis voraussetzt, daß der Wert des Grundstücks für den Pflichtteil von Bedeutung ist.

Für die Beurteilung des vorliegenden Falles kommt es darauf jedoch schon deshalb nicht an, weil das Vermessungs- und Katasteramt sich ein berechtigtes Interesse der beiden Pflichtteilsberechtigten offensichtlich nicht hat nachweisen lassen und offensichtlich auch nicht geprüft hat, ob dem berechtigten Interessen des Alleinerben entgegen gestanden haben, was bei der Übermittlung personenbezogener Daten grundsätzlich gegeben ist, weil die Wahrung des Rechts auf informationelle Selbstbestimmung immer ein berechtigtes Interesse des Betroffenen darstellt, das nur dann eingeschränkt werden kann, wenn die berechtigten Interessen anderer von so schwerem Gewicht sind, daß sie in der Lage sind, daß Recht des Betroffenen auf informationelle Selbstbestimmung zurückzudrängen.

Der Gutachterausschuß hat den Betroffenen nicht, wie vorgeschrieben, zu der von der Behörde beabsichtigten Übermittlung personenbezogener Daten gehört.

Nach alledem war die Übermittlung des Gutachtens an die Pflichtteilsberechtigten unzulässig. Da für Übermittlungen von Gutachten nunmehr die Vorschriften des am 01. 07. 1987 in Kraft getretenen Baugesetzbuches anzuwenden sind und darin eine Übermittlung an Dritte außer an den Eigentümer nicht vorgesehen ist, habe ich dem Gutachterausschuß gegenüber die Erwartung geäußert, daß ähnliche Übermittlungen personenbezogener Daten künftig unterbleiben. Ich erwarte zu dem Beschwerdefall noch eine abschließende Stellungnahme des Magistrats.

5.9 Finanzwesen

5.9.1 Erlaß einer Steuerdaten-Abruf-Verordnung nach § 30 Abs. 6 Satz 2 der Abgabenordnung (StDAV)

In meinem letzten Jahresbericht habe ich unter Pkt. 5.9.1.1 über die Änderung des § 30 der Abgabenordnung (AO) und die Vorlage eines Entwurfes einer Steuer-Daten-Abrufverordnung nach § 30 Abs. 6 Satz 2 AO durch den Bundesminister für Finanzen berichtet. Nach dieser Vorschrift kann der Bundesminister der Finanzen zur Wahrung des Steuergeheimnisses durch Rechtsverordnung mit Zustimmung des Bundesrates bestimmen, welche technischen und organisatorischen Maßnah-

men gegen den unbefugten Abruf von Daten zu treffen sind. Insbesondere kann er nähere Regelungen treffen über die Art der Daten, deren Abruf zulässig ist, sowie über den Kreis der Amtsträger, die zum Abruf solcher Daten berechtigt sind. Der Senator für Finanzen hat mir einen mehrfach überarbeiteten Verordnungsentwurf des Bundesministers für Finanzen zur Stellungnahme zugeleitet.

Der Entwurf sieht vor, daß ein automatisiertes Datenabrufverfahren dann eingerichtet werden darf, wenn die bereitgehaltenen Daten dazu bestimmt und ihrer Art nach geeignet sind, der Durchführung von bestimmten Verfahren in Steuersachen zu dienen. Eine Einschränkung, wonach die Daten für die genannten Verfahren auch erforderlich sein müssen, fehlt. Darüber hinaus enthält er keine nähere Bestimmung der Daten, die geeignet und erforderlich sind für die Durchführung der genannten Verfahren. Diese Regelung wird somit dem Grundsatz der Normenklarheit nicht gerecht.

Den Obersten Finanzbehörden der Länder und den Oberfinanzdirektionen soll im Wege der Dienst- und Fachaufsicht sowie dem Bundesministerium der Finanzen im Rahmen der internationalen Rechts- und Amtshilfe und den Rechnungshöfen im Rahmen der Rechnungsprüfung eine Abrufberechtigung zugebilligt werden. Dieses bedeutet, daß bei den Oberfinanzdirektionen, den Obersten Finanzbehörden der Länder und beim Bundesminister der Finanzen sowie bei den Rechnungshöfen des Bundes und der Länder zentrale Abrufmöglichkeiten geschaffen werden können, die den unmittelbaren Zugriff auf sämtliche Daten der Finanzämter des jeweiligen Zuständigkeitsbereiches ermöglichen. Da bei den Finanzämtern über Steuerpflichtige alle bedeutsamen Daten über familiäre, gesundheitliche und wirtschaftliche Verhältnisse, über Beziehungen zu politischen Parteien, Religionsgemeinschaften, gemeinnützigen Organisationen, Versicherungen, Banken usw. gespeichert sind, könnten sich die genannten Stellen innerhalb ihres Zuständigkeitsbereiches jederzeit Einblick darin verschaffen. Dabei ist zu bedenken, daß die große Mehrheit aller Bürger steuerpflichtig ist.

Eine solche Regelung erscheint mir verfassungsrechtlich bedenklich, weil die Einrichtung solcher zentralen Datenabrufmöglichkeiten gegen den Grundsatz der Verhältnismäßigkeit, insbesondere des Übermaßverbotes verstößt. Solche zentralen Datenabrufmöglichkeiten sind nicht erforderlich, da für die Verfahren bei den Oberfinanzdirektionen und den Obersten Finanzbehörden sowie den Rechnungshöfen bei der Bearbeitung von Einzelfällen ohnehin die Akten heranzuziehen sind. Von diesen Behörden sind bei der Bearbeitung von Einzelfragen in aller Regel keine Entscheidungen unter Zeitdruck zu treffen. Sollten in Einzelfällen Eilentscheidungen notwendig werden, stehen zu deren Erledigung ggf. andere Mittel, wie Telefon, Telefax, Fernschreiben und Eilbrief zur Verfügung. Der von einem solchen Verfahren offensichtlich erwartete Rationalisierungseffekt dürfte äußerst gering sein. Dem steht gegenüber, daß durch zentrale Zugriffsmöglichkeiten eine neue Gefahrenquelle für die Datensicherheit entsteht und Mißbrauch nicht ausgeschlossen werden kann.

Nach Angaben des Senators für Finanzen war die Frage der Abrufberechtigung der Obersten Finanzbehörden und Oberfinanzdirektionen auf Bundesebene strittig, so daß die Aufnahme der Abrufberechtigung durch Mehrheitsbeschluß erfolgte. Ich gehe davon aus, daß der Senator für Finanzen meine Auffassung hierzu weiterhin auf Bundesebene vertreten wird.

In diesem Zusammenhang haben sich zwischen dem Senator für Finanzen und mir erneut unterschiedliche Auffassungen darüber ergeben, wann ich bei datenschutzrechtlich bedeutsamen Gesetzesvorhaben des Bundes, die von den Ländern mit beraten werden, zu beteiligen bin. Der Senator für Finanzen meint, meine Beteiligung würde erst dann erforderlich sein, wenn Inhalt und Begründung datenschutzrechtlich bedeutsamer Entwürde von Rechts- und Verwaltungsvorschriften für das Abstimmungsverfahren zwischen Bund und Ländern verbindlich sind. Insoweit sei ich erst dann zu beteiligen, wenn abstimmungsreife Referentenentwürfe vorliegen. Einer wirksamen Datenschutzkontrolle und -beratung kann ich jedoch nur dann gerecht werden, wenn mir solche Entwürfe so frühzeitig wie nur möglich und in jeder Phase der Beratung zugänglich gemacht werden. Nur so kann ich datenschutzrechts-relevante Rechts- und Verwaltungsvorschriften intensiv und zeitgerecht durcharbeiten, Stellungnahmen und Verbesserungsvorschläge vorlegen. Eben deshalb hat der Senatskommissar für den Datenschutz mit Rundschreiben an die Senatsmitglieder vom 3. September 1980 gebeten, mich bei der Überprüfung von datenschutzrechtlich bedeutsamen Referentenentwürfen zu beteiligen, unabhängig davon, ob sie bereits als abstimmungsreif bzw. verbindlich angesehen werden

können. Der Senator für Inneres, der seinerzeit zuständig für den Datenschutz im öffentlichen Bereich war, hat die senatorischen Dienststellen mit Schreiben vom 2. Februar 1982 gebeten, entsprechend zu verfahren.

Ich erwarte daher, daß mir der Senator für Finanzen Entwürfe von datenschutzrechtlich bedeutsamen Rechts- und Verwaltungsvorschriften künftig bereits dann vorlegt, wenn sie ihm durch den Bundesminister der Finanzen zugeleitet worden sind.

5.9.2 Aufbewahrung von Kraftfahrzeugsteuerakten

Eine Tageszeitung hat mich darüber informiert, daß sie festgestellt habe, daß im Finanzamt Bremen-Mitte Kraftfahrzeugsteuerakten, die personenbezogene Daten von Steuerpflichtigen enthalten, in nicht verschlossenen Rollschränken auf Fluren des Dienstgebäudes untergebracht seien, die für Außenstehende zugänglich seien. Sie hat mich um Äußerung gebeten, ob das datenschutzrechtlich zulässig ist.

Eine von mir unverzüglich durchgeführte Prüfung hat ergeben, daß die Kraftfahrzeugsteuerakten tatsächlich in unverschlossenen Rollschränken auf Fluren untergebracht waren, zu denen die Öffentlichkeit freien Zutritt hat. Das Finanzamt hielt die Steuerdaten trotzdem für ausreichend gesichert und sah in dem offenen Zugang keine Beeinträchtigung des Steuergeheimnisses.

Daß diese Form der Datensicherung völlig unzureichend war, ergibt sich schon allein daraus, daß ich während der von mir durchgeführten Prüfung feststellen konnte, daß kein Bediensteter anwesend war, der die Akten hätte beaufsichtigen können.

Dieser Vorgang verstößt sowohl gegen die Vorschriften über das Steuergeheimnis als auch gegen die Bestimmungen des Bremischen Datenschutzgesetzes, nach denen die technischen und organisatorischen Maßnahmen zu treffen sind, die für die Sicherung und den Schutz personenbezogener Daten erforderlich sind.

In einer nachgehenden Prüfung konnte ich mich davon überzeugen, daß das Finanzamt meiner Beanstandung inzwischen Rechnung getragen und die Akten nunmehr in einem Kellerraum untergebracht hat, der durch eine mit einem Sicherheitszylinderschloß versehenen Eisentür ausreichend gegen unbefugten Zutritt gesichert ist.

Dabei bleibt erwähnenswert, daß das Finanzamt den Vorfall zum Anlaß genommen hat, die Datensicherung seines gesamten Aktenbestandes zu überprüfen und notwendige bauliche und organisatorische Maßnahmen durchgeführt hat.

Ich habe den Verstoß gegenüber dem Senator für Finanzen beanstandet, obwohl die Mängel zwischenzeitlich abgestellt worden waren. Ich sah mich dazu insbesondere deshalb veranlaßt, weil der Senat in seiner Antwort auf eine entsprechende Anfrage in der aktuellen Stunde der Bremischen Bürgerschaft zu erkennen gegeben hat, daß er erwartet, das Ergebnis meiner Prüfung mitgeteilt zu erhalten.

5.10 Häfen, Schiffahrt und Verkehr

5.10.1 Führung eines Flughauptbuches durch die Flugplatzhalter

Durch eine Eingabe ist bekannt geworden, daß die Flugplatzhalter durch die Luftfahrtbehörden der Länder im Rahmen der Genehmigung zum Anlegen und Betrieb eines Flugplatzes grundsätzlich verpflichtet werden, ein Flughauptbuch zu führen. Nach Angaben eines Petenten werden von Flugzeugführern, die unkontrollierte Flüge durchführen, u. a. auch personenbezogene Daten des Flugzeugführers verarbeitet.

Dazu hat mir der Senator für Häfen, Schiffahrt und Verkehr mitgeteilt, daß die Flugplatzhalter im Lande Bremen verpflichtet sind, Flughauptbücher zu führen. Sie enthalten neben dem Namen des verantwortlichen Luftfahrzeugführers das Kennzeichen des Luftfahrzeugs, Angaben über den Flugzeugtyp, die Startzeit und den Zielort des beabsichtigten Fluges und dienen nach Angaben der senatorischen Dienststelle informatorischen Zwecken insbesondere mit der Absicht, Angaben über die Anzahl und die Art des Luftverkehrs zu erhalten. Das Führen des Hauptflugbuches ist an keine Form gebunden und lediglich der Luftaufsicht bzw. den Flugleitern zugänglich. Informationen werden nicht weitergegeben, vielmehr ist davon auszugehen, daß die jeweilige Flugplatzgesellschaft das Buch intern und für einen fest umrissenen kleinen Personenkreis einsichtbar führt. Lediglich die Luftfahrtbehörden könnten die Angaben des Hauptflugbuches jederzeit einsehen. Nach

FFD 12/165

seiner Ansicht werden datenschutzrechtliche Interessen nicht berührt, da außer dem Namen des verantwortlichen Luftfahrzeugführers keinerlei personenbezogene Daten erscheinen.

Ich habe dieser Auffassung des Senators für Häfen, Schiffahrt und Verkehr widersprochen. Im datenschutzrechtlichen Sinne sind personenbezogene Daten alle Einzelangaben über persönliche und sachliche Verhältnisse, die einer natürlichen Person zugeordnet werden können. Nach der Darstellung der senatorischen Behörde läßt sich aus dem Flughauptbuch neben dem Namen mindestens entnehmen, mit welchem Flugzeug der Flugzeugführer an welchem Tag um welche Uhrzeit wohin geflogen ist oder einen Flug beabsichtigt hat. Diese Angaben geben Auskunft über persönliche Aktivitäten des betroffenen Luftfahrzeugführers. Es handelt sich somit um personenbezogene Daten.

Die sich aus der Führung des Flughauptbuches ergebende Verarbeitung der personenbezogenen Daten ist ohne Einwilligung der Betroffenen nur aufgrund einer verfassungsgemäß zustande gekommenen Rechtsvorschrift im überwiegenden Allgemeininteresse zulässig. Es bedarf zu ihrer Zulässigkeit in aller Regel einer bereichsspezifischen Norm. Als bereichsspezifische Rechtsvorschriften sind im vorliegenden Falle das Luftverkehrsgesetz (LuftVG) und die dazu ergangene Luftverkehrsordnung (LuftVO) anzusehen.

Aus den von der senatorischen Behörde zitierten §§ 22 und 24 LuftVO läßt sich eine Erlaubnis für die mit der Verpflichtung zur Führung eines Flughauptbuches in der dargestellten Form verbundene Verarbeitung personenbezogener Daten nicht ersehen oder ableiten. Nach § 22 Abs. 1 Nr. 8 LuftVO ist der Luftfahrzeugführer lediglich verpflichtet, sich bei der Flugleitung zu melden. § 24 Abs. 2 LuftVO verpflichtet den Luftfahrzeugführer nur, auf Verlangen den für die Luftaufsicht zuständigen Personen näher bestimmte Dokumente zur Einsicht und Prüfung vorzulegen. Darüber hinaus kann die LuftVO das Recht auf informationelle Selbstbestimmung nicht einschränken, weil die Ermächtigung in § 32 des Luftverkehrsgesetzes zum Erlaß einer Verordnung im Hinblick auf die zu Art. 80 GG entwickelte Wesentlichkeitstheorie dazu nicht ausreicht. Auch dem Gesetz über die Luftverkehrsstatistik vermag ich keine Vorschrift zu entnehmen, welche die Verarbeitung der personenbezogenen Daten der Luftfahrzeugführer in dem hier in Rede stehenden Umfange erlaubt. Das gilt insbesondere für die damit verbundenen Datenübermittlungen.

Ich habe den Senator für Häfen, Schiffahrt und Verkehr gebeten, sich unter Berücksichtigung der vorstehenden Ausführungen zu entschließen, künftig auf die Verpflichtung der Flugplatzhalter zur Führung des Flughauptbuches zu verzichten oder eine Form der Führung zu finden, welche die Verarbeitung personenbezogener Daten ohne Einwilligung der Betroffenen ausnimmt.

Da die Kompetenz für die Erledigung luftrechtlicher Angelegenheiten weitgehend den Bundesländern dadurch übertragen wurde, daß sie im Rahmen der Bundesauftragsverwaltung tätig werden, hat der Senator für Häfen, Schiffahrt und Verkehr die Angelegenheit auf einer Sitzung der Luftverkehrsreferenten erörtert. Dieser Bund/Länder-Fachausschuß Luftfahrt (BLFA-L) ist zu dem Ergebnis gekommen, daß ein Verzicht auf die Führung des Flughauptbuches aus Sicherheitsgründen nicht in Betracht kommen kann. Um eine gründliche Prüfung zu ermöglichen, hat er seinen Unterausschuß Flugbetrieb beauftragt, sich mit dieser Angelegenheit zu befassen. Danach will der BLFA-L die Angelegenheit erneut erörtern und danach seinen Unterausschuß Recht und Verwaltung damit befassen und selbst nochmals darüber beraten.

Daraus ergibt sich, daß beabsichtigt ist, die bisherige Praxis der Verarbeitung personenbezogener Daten ohne ausreichende Rechtsgrundlage über einen längeren Zeitraum fortzusetzen. Ich habe erhebliche datenschutzrechtliche Bedenken dagegen.

Eine solche Praxis könnte nur unter dem Gesichtspunkt der Anwendung des Übergangsbonus hingenommen werden. Die vom Bundesverfassungsgericht in ständiger Rechtsprechung dazu herausgebildeten Voraussetzungen scheinen mir hier nicht erfüllt zu sein. Ich vermag nicht zu erkennen, daß ohne die Fortsetzung der bisherigen Praxis eine Funktionsunfähigkeit staatlicher Einrichtungen eintreten würde oder die Fortsetzung zur Abwehr gravierender Nachteile für das Gemeinwohl unerläßlich ist. Das ergibt sich schon allein daraus, daß in der Freien und Hansestadt Hamburg kein Flughauptbuch geführt wird und bisher deswegen von

FFD 12/1.163

keiner Seite geltend gemacht worden ist, daß dadurch die Funktionsunfähigkeit staatlicher Einrichtungen gegeben sei oder gravierende Nachteile für das Gemeinwohl entstanden seien.

Darüber hinaus habe ich erhebliche Zweifel, ob im vorliegenden Falle überhaupt die Möglichkeit der Anwendung des Übergangsbonus gegeben ist, da der Verordnungsgeber in den §§ 22 bis 27 a der LuftVO eine abschließende Regelung über die Datenverarbeitung im Zusammenhang mit dem Flugbetrieb auf Flugplätzen und deren Umgebung getroffen hat. So ist z. B. im § 25 der LuftVO festgelegt, für welche Art von Flügen ein Flugplan abzugeben ist. Soweit von verschiedenen Seiten die Unverzichtbarkeit der in Rede stehenden Datenverarbeitung damit begründet wird, daß die Eintragungen im Flughauptbuch in erster Linie der Rekonstruktion von Flugweg und Flugzeit für den Such- und Rettungsdienst dienen, hat der Verordnungsgeber mit der Vorschrift des § 25 Abs. 2 LuftVO es bei unkontrollierten Flügen ausdrücklich der Entscheidung des Luftfahrzeugführers überlassen, ob er zur Erleichterung der Durchführung des Such- und Rettungsdienstes einen Flugplan übermitteln will.

Ich habe den Senator für Häfen, Schiffahrt und Verkehr gebeten, mir seine Auffassung zu dieser Angelegenheit mitzuteilen und ggf. darauf hinzuwirken, daß der Bundesminister für Verkehr seine Weisung an die Länder, die Führung eines Flughauptbuches von den Flugplatzhaltern zu verlangen, revidiert. Eine Antwort steht noch aus.

5.10.2 Verarbeitung personenbezogener Daten von Einwendern beim Planfeststellungsverfahren Verkehrsflughafen Bremen

Das Hafenbauamt Bremen hat mich um datenschutzrechtliche Stellungnahme zu einem Automatisierungsvorhaben zur Erarbeitung von Stellungnahmen zu Einwendungen gegen das Planfeststellungsverfahren zur Erweiterung des Verkehrsflughafens Bremen gebeten.

Das Hafenbauamt Bremen wird in diesem Verfahren aufgrund eines zwischen dem Senator für Häfen, Schiffahrt und Verkehr und der Flughafen Bremen GmbH geschlossenen Vertrages im Auftrag der Flughafen GmbH tätig, die einen Antrag auf Ergänzung bzw. Änderung der Genehmigung des Betriebes eines Flugplatzes in Bremen gestellt hat. Der Senator für Häfen, Schiffahrt und Verkehr als Genehmigungsbehörde im Sinne des Luftverkehrsgesetzes hat offensichtlich die Durchführung eines Planfeststellungsverfahrens für erforderlich erachtet. Wegen der die Landesgrenzen überschreitenden Lage des Flughafens Bremen haben das Land Niedersachsen und die Freie Hansestadt Bremen einen Staatsvertrag geschlossen, nach dem das Planfeststellungsverfahren durch das Land Niedersachsen im Benehmen mit dem Senator für Häfen, Schiffahrt und Verkehr der Freien Hansestadt Bremen durchgeführt werden soll. Das Land Niedersachsen hat die Bezirksregierung Hannover zur Planfeststellungsbehörde im Sinne des § 10 des Luftverkehrsgesetzes bestimmt. Die Bezirksregierung Hannover hat nach Auslegung der Pläne alle eingegangenen Einwendungen einschließlich der darin enthaltenen personenbezogenen Daten sowohl an die Flughafen Bremen GmbH als auch an das Hafenbauamt Bremen mit der Bitte um Stellungnahme übersandt. Es handelt sich dabei um einige tausend Einzeleinwendungen.

Ich habe erhebliche Bedenken wegen der Zulässigkeit der Übermittlung der personenbezogenen Daten durch die Bezirksregierung Hannover an das Hafenbauamt Bremen und gegen die Verarbeitung dieser Daten durch das Hafenbauamt geltend gemacht.

Sowohl die Übermittlung als auch die Verarbeitung dieser Daten stellen einen Eingriff in das verfassungsmäßige Recht der Betroffenen auf informationelle Selbstbestimmung dar. Ein solcher Eingriff ist jedoch nur aufgrund einer verfassungsmäßig zustandegekommenen bereichsspezifischen Rechtsgrundlage zulässig, welche die rechtsstaatlichen Gebote der Normenklarheit und Verhältnismäßigkeit erfüllen muß. Als bereichsspezifische Vorschrift ist der § 10 des Luftverkehrsgesetzes anzusehen. Er enthält Verfahrensvorschriften für zur Genehmigung von Flughäfen notwendige Planfeststellungsverfahren. Wenn diese Vorschriften Lücken aufweisen, sind diese nach den allgemeinen Grundsätzen des Verwaltungsverfahrens auszufüllen. Diese Grundsätze haben ihren Niederschlag in den allgemeinen Verwaltungsverfahrensgesetzen gefunden. Nach § 10 Luftverkehrsgesetz können gegen den öffentlich auszulegenden Plan bei der von der Landesregierung bestimmten Behörde oder einer von ihr bezeichneten Stelle Einwendungen (nur) schriftlich erhoben werden. Die eingegangenen Einwendungen sind von der Plan-

feststellungsbehörde mit allen Beteiligten mit dem Ziel zu erörtern, Einigung zwischen den Beteiligten zu erzielen. Die Vorschrift verpflichtet die Planfeststellungsbehörde zwar zur Erörterung der Einwendungen mit allen Beteiligten und normiert damit auch ein Recht aller Beteiligten, an der Erörterung teilzunehmen, sie berechtigt die Genehmigungsbehörde aber nicht, wie im vorliegenden Falle geschehen, einem Beteiligten (Antragsteller) die personenbezogenen Daten der übrigen Beteiligten (Einwender) zu übermitteln.

Eine Erlaubnis für eine solche Datenübermittlung kann auch nicht daraus entnommen werden, daß die personenbezogenen Daten der Betroffenen bei der Erörterung ohnehin für alle Beteiligten offenkundig werden. Der Betroffene ist einerseits nicht verpflichtet, sich an der Erörterung zu beteiligen, andererseits verbleibt ihm bei Teilnahme eine Entscheidung darüber, in welchem Umfange er seine Daten den Beteiligten während der Erörterung bekanntgeben will.

Hierbei bleibt auch zu berücksichtigen, daß die Planfeststellungsbehörde auch ohne Teilnahme des Einwenders an der Erörterung pflichtgemäß über die Einwendungen zu entscheiden hat, so daß dem Anliegen des Einwenders evtl. auch ohne Offenlegung seiner personenbezogenen Daten gegenüber Dritten Rechnung getragen werden kann.

Die Zulässigkeit der Datenübermittlung kann auch nicht mit den dem Verwaltungsverfahren innewohnenden Grundsatz des Rechtes auf Akteneinsicht von Beteiligten begründet werden. Das Recht auf Akteneinsicht ist auf Teile der Akten begrenzt, deren Kenntnis zur Geltendmachung oder Verteidigung rechtlicher Interessen des Beteiligten erforderlich ist und den berechtigten Interessen anderer Beteiligter oder dritter Personen nicht entgegenstehen. Die Beteiligten haben gar einen Anspruch darauf, daß die Behörde ihre personenbezogenen Daten nicht unbefugt offenbart. Für den vorliegenden Fall vermag ich nicht zu erkennen, daß die Kenntnis der personenbezogenen Daten der Einwender zur Geltendmachung oder Verteidigung der rechtlichen Interessen des Antragstellers Flughafen Bremen GmbH erforderlich ist. Auf keinen Fall sehe ich ein so starkes rechtliches Interesse, daß dieses in der Lage sein könnte, den Anspruch der Einwender auf Wahrung ihres Rechtes auf informationelle Selbstbestimmung zurückzudrängen. Hierbei ist zu beachten, daß Einwendungen gegen Planfeststellungsverfahren in vielen Fällen äußerst sensible Angaben zur Person enthalten, die Einblick in die persönlichen, wirtschaftlichen und sozialen Verhältnisse des Einwenders geben. Ich habe die Beteiligten gebeten, die nach meiner Auffassung unzulässig übermittelten Daten entweder zu löschen oder aber von den Betroffenen eine Einwilligung zur Verarbeitung ihrer personenbezogenen Daten einzuholen.

In einer Erörterung des Problems mit allen beteiligten Behörden konnten diese sich nicht entschließen, meinem Vorschlag zu folgen. Sie machten insbesondere geltend, daß eine Planfeststellungsbehörde keine Möglichkeit habe, Einwendungen sachgerecht zu bearbeiten, wenn sie nicht berechtigt sei, den Antragsteller um eine Stellungnahme zu den Einwendungen zu bitten, da ihr jegliche Kenntnis fehle, die zur Bearbeitung der Einwendungen notwendig sei, was letztlich zu einer unsachgemäßen Entscheidung über die Einwendungen führen müsse. Die Planfeststellungsbehörde müsse auch die Möglichkeit haben, beim Antragsteller anzufragen, ob dieser eine Möglichkeit der Einigung mit dem Einwender sehe. Die Einholung einer Stellungnahme des Antragstellers zu den Einwendungen sei also aus Zweckmäßigkeitserwägungen erforderlich und sinnvoll. Im übrigen habe der Betroffene mit dem Erheben von Einwendungen konkludent der Verarbeitung seiner personenbezogenen Daten auch insoweit zugestimmt, als diese an den Antragsteller übermittelt und von diesem verarbeitet werden. Außerdem sei dieses Verfahren seit vielen Jahren von allen Planfeststellungsbehörden, die nach den verschiedenen Planfeststellungsvorschriften arbeiten, so geübt worden. Soweit die Bedenken des Datenschutzbeauftragten berechtigt sein sollten, sei es Aufgabe des Gesetzgebers, neue datenschutzgerechte Verfahren zu entwickeln und zu normieren. Bis dahin jedoch seien die Planfeststellungsbehörden auf die Beibehaltung der bisher geübten Verfahren dringend angewiesen.

Wie eingangs bereits dargelegt, vermögen weder Zweckmäßigkeitserwägungen noch Verwaltungsübung die Verarbeitung personenbezogener Daten zu erlauben. Der Auffassung, daß der Bürger mit seiner Einwendung bereits konkludent der hier beanstandeten Datenverarbeitung zustimmt, vermag ich mich nicht anzuschließen, da das geltende Datenschutzrecht nur die ausdrückliche schriftliche Einwilligung für solche Fälle kennt, in denen eine gesetzliche Erlaubnisvorschrift nicht vorliegt. Das bisher geübte Verfahren kann auch nicht bis zum Erlaß neuer die

Datenverarbeitung erlaubenden Vorschriften hingenommen werden, da das Luftverkehrsgesetz hinsichtlich der Behandlung von Einwendungen abschließende präzise Verfahrensregelungen enthält und auch nicht zu erkennen ist, daß ohne dieses Verfahren gravierende Nachteile für das Allgemeinwohl entstehen können. Soweit der Planfeststellungsbehörde die Übermittlung der personenbezogenen Daten der Einwender an den Antragsteller für die Durchführung des Planfeststellungsverfahrens förderlich oder bedeutsam erscheinen mag, verbleibt ihr nach meiner Auffassung nur die Möglichkeit, für die Verarbeitung die Zustimmung der Betroffenen einzuholen.

Das Hafenbauamt hat mir mitgeteilt, daß es auf Weisung der Bezirksregierung Hannover einen Teil der von dieser übermittelten personenbezogenen Daten gelöscht bzw. die Datenträger vernichtet habe. Für den verbleibenden Teil habe die Bezirksregierung Hannover die Verarbeitung im Interesse einer sachgerechten Gegenäußerung zu den Einwendungen für erforderlich gehalten und eine entsprechende Weisung erteilt.

Der Senator für Häfen, Schiffahrt und Verkehr hat bei dem inzwischen eingeleiteten Planfeststellungsverfahren für den Verkehrslandeplatz Luneort in Bremerhaven mit der amtlichen Bekanntmachung über die Auslegung des Planes die evtl. Einwendungsführer gebeten, ausdrücklich mitzuteilen, ob sie mit der Weitergabe ihrer personenbezogenen Daten an Dritte, insbesondere an die Flugplatzbetriebsgesellschaft als Antragsteller, im Interesse einer möglichst weitgehenden Aufklärung und fachlichen Beurteilung ihrer Einwendungen einverstanden sind. Dieses Verfahren ist aus datenschutzrechtlicher Sicht zu begrüßen. Ich schließe daraus, daß meine datenschutzrechtlichen Bedenken künftig beachtet werden.

Nach meinen bisherigen Feststellungen wird das hier von mir kritisierte Verfahren auch von anderen Behörden geübt, die nach anderen Rechtsvorschriften, z. B. nach dem Bremischen Verwaltungsverfahrensgesetz, dem Bundesfernstraßengesetz, dem Wassergesetz und dem Eisenbahnverkehrsgesetz Planfeststellungsverfahren durchführen. Ich werde mich im Rahmen der mir zur Verfügung stehenden Möglichkeiten bemühen, dieses zu überprüfen und ggf. auf datenschutzgerechte Verfahren hinzuwirken.

5.11 Magistrat Bremerhaven

Weitergabe von Daten durch Stadtverordnete an die Presse

In Zeitungen in Bremerhaven erschienen Artikel u. a. „Warum riecht der Grünkohl penetrant nach Chemie?", in denen neben Ausführungen zum Stand des Verwaltungsverfahrens auch Namen verantwortlicher Beamter und Politiker genannt wurden. Die Ortspolizeibehörde Bremerhaven überreichte mir in Ablichtung einen bei ihr entstandenen Vorgang mit der Bitte um Prüfung, ob die von einem Stadtverordneten nach Akteneinsicht vorgenommene Unterrichtung der Presse möglicherweise einen Verstoß gegen datenschutzrechtliche Bestimmungen beinhalten könnte. Aufgrund der Aktenlage war nicht erkennbar, ob und ggf. in welchem Umfang der Stadtverordnete nach vorgenommener Akteneinsicht gem. § 18 Abs. 3 Satz 1 der Verfassung für die Stadt Bremerhaven die Presse über Einzelheiten der Aktenlage unterrichtet hat. Eine Befragung des verantwortlichen Redakteurs habe ich nicht angestrebt, da dieser sich zu Recht auf das grundrechtlich geschützte Presseprivileg und den Informantenschutz berufen könnte. Von einer Befragung des Stadtverordneten habe ich abgesehen, weil ich unter Zugrundelegung der veröffentlichten Presseartikel keinen Verstoß gegen datenschutzrechtliche Bestimmungen feststellen konnte.

Zur Begründung habe ich darauf hingewiesen, daß eine besondere Regelung, die dem Stadtverordneten ermöglicht, nach Akteneinsicht zugängliche Informationen an die Öffentlichkeit weiterzugeben, sich aus der Stadtverfassung nicht ergibt. Eine Anwendung der Datenverarbeitungsregelungen des Bremischen Datenschutzgesetzes schied ebenfalls aus, so daß lediglich noch eine Prüfung des Vorgangs nach § 20 Abs. 1 Satz 1 BrDSG in Betracht kam, wonach ich auch die Einhaltung anderer Vorschriften über den Datenschutz zu überwachen habe.

Unter datenschutzrechtlichen Gesichtspunkten kam ohnehin nur die Weitergabe von Informationen an die Presse in Betracht, durch die in rechtswidriger Weise Persönlichkeitsrechte von Amtsträgern oder Beamten verletzt werden können.

Somit verblieb lediglich die Prüfung, ob eine Mitteilung von Verwaltungshandlungen in Datenschutzrechte eingreift. Soweit die Namen leitender hochrangiger

FFD 12/163

Amtsträger in dem Artikel genannt wurden, standen diese ohnehin als Persönlichkeiten des öffentlichen Lebens ständig im öffentlichen Interesse und sind in dieser Funktion auch dem Leser der Regionalzeitschriften bekannt.

Eine Rechtsverletzung dahingehend, daß hier falsche Tatsachen oder unwahre Behauptungen aufgestellt worden sind, konnte ich den mir zur Verfügung gestellten Unterlagen nicht entnehmen. Das von den namentlich genannten Personen von einem Gegendarstellungsrecht Gebrauch gemacht worden war, ist mir nicht angezeigt worden.

Eine Abwägung des öffentlichen Interesses an der Veröffentlichung gegenüber dem Schutz der Privatsphäre, wie es die herrschende Rechtsprechung verlangt, kam in dem zu entscheidenden Fall nicht in Betracht, da die dienstliche Tätigkeit der persönlich Genannten ausschließlicher Gegenstand der Pressedarstellung war, nicht hingegen ein privates Verhalten. Dieses dienstliche Verhalten und damit die Tätigkeit der Verwaltung zu kontrollieren, ist Aufgabe der Stadtverordnetenversammlung und ihrer gewählten Vertreter. Ausdrucksform ist der § 18 Abs. 3 der Verfassung der Stadt Bremerhaven, der dem Stadtverordneten ein Akteneinsichtsrecht gibt.

Der Stadtverordnete ist als gewählter Vertreter des Volkes grundsätzlich berechtigt, über alle Dinge, die ihm in seiner Funktion als Stadtverordneter bekannt werden, die Öffentlichkeit zu informieren. Die Presse ist dabei ein Verbreitungsmedium, dessen sich der Verordnete bedienen kann.

Dieser Grundsatz gilt aber sicherlich nicht uneingeschränkt, sondern auch der Stadtverordnete ist verpflichtet, ein Geheimhaltungsinteresse der Verwaltung zu berücksichtigen.

Eine ausdrückliche Regelung, nach der der Stadtverordnete die ihm durch Akteneinsicht zugänglich gewordenen Informationen an die Öffentlichkeit weitergibt, ergibt sich aus der Stadtverfassung im Gegensatz zur Landesverfassung für die Bürgerschaftsabgeordneten nach Art. 83 Abs. 2 Bremische Landesverfassung nicht. Auf der anderen Seite läßt sich aus der in § 20 der Stadtverfassung postulierten Unabhängigkeit der Mitglieder der Stadtverordnetenversammlung nicht ableiten, daß ein Stadtverordneter völlig frei in seiner Entscheidung ist, in welchem Umfange er die durch Akteneinsicht erlangten Informationen an die Presse weiterleiten will.

Ohne näher auf die Verschwiegenheitspflicht des Stadtverordneten eingehen zu müssen, kann zumindest festgestellt werden, daß diese Verschwiegenheitspflicht nicht weitergehen kann als die derjenigen Personen, die zu ehrenamtlicher Tätigkeit bestellt werden. Wegen § 10 der Verfassung für die Stadt Bremerhaven kann mithin von einem Stadtverordneten in diesem Fall nicht mehr verlangt werden als von einem städtischen Beamten. Da es hier um die Informationsweitergabe an die Presse geht, hätten die Beamten und daher auch der Stadtverordnete das Pressegesetz zu beachten.

Nach § 4 Pressegesetz haben die Behörden der Gemeinden eine Auskunftspflicht gegenüber der Presse. Was für die Behörden gilt, muß auch wegen der unabhängigen Stellung des Stadtverordneten dieser für sich in Anspruch nehmen können.

Eine besondere Geheimhaltungsstufe konnte ich dem Vorgang nicht entnehmen, eine Kennzeichnung als „VS-NfD" oder gar „Vertraulich" wäre auch nach den Sicherheitsrichtlinien nicht angezeigt.

Schließlich konnte ich auch nicht feststellen, daß der Stadtverordnete sich durch das oben beschriebene Verhalten nach § 203 Abs. 2 StGB strafbar gemacht haben könnte, da er weder Amtsträger noch ein besonders für den öffentlichen Dienst Verpflichteter ist. Der Stadtverordnete als Abgeordneter steht in keinem öffentlich-rechtlichen Amtsverhältnis und nimmt auch keine Aufgaben der öffentlichen Verwaltung wahr. Aus diesem Grund kann er auch nicht als einer für den öffentlichen Dienst besonders Verpflichteter im Sinne von § 11 Abs. 1 Nr. 4 StGB angesehen werden, da nach § 42 der Verfassung für die Stadt Bremerhaven die Verwaltung vom Magistrat und nicht von der Stadtverordnetenversammlung durchgeführt wird.

Daher war unter keinem rechtlichen Gesichtspunkt ein datenschutzrechtlicher Verstoß erkennbar.

5.12 Sonstige öffentliche Stellen, Körperschaften u. a.

5.12.1 Zentrale Registrierung von Arbeitnehmern, die krebserregenden Stoffen oder Arbeitsverfahren ausgesetzt sind, beim Gemeindeunfallversicherungsverband

Der Bremische Gemeindeunfallversicherungsverband hat erwogen, sich an dem von der Berufsgenossenschaft Chemie durchgeführten „Zentralen Organisationsdienst für nachgehende Untersuchungen (ODIN)" zu beteiligen. Er hat mich um datenschutzrechtliche Beurteilung der Zulässigkeit der mit diesem Verfahren verbundenen Verarbeitung personenbezogener Daten von Arbeitnehmern gebeten.

In dem von der Berufsgenossenschaft Chemie eingerichteten Verfahren sollen Arbeitnehmer erfaßt werden, die mit Stoffen in Berührung gekommen sind, deren krebserregende Wirkung mit relativ hoher Sicherheit nachgewiesen ist und für die Grenzwerte festgelegt sind, oder die krebserregenden Arbeitsverfahren ausgesetzt worden sind. Gespeichert werden sollen neben Namen, Anschrift, Staatsangehörigkeit, Geschlecht, Rentenversicherungsnummer, Personalnummer des Betriebes, Geburtsdatum und Datum der Einstellung in den Betrieb, insbesondere Angaben über Kontakte mit Gefahrstoffen bei der Arbeit.

Die Arbeitgeber sollen verpflichtet werden, Arbeitnehmer bei ODIN anzumelden, wenn sie krebserregenden Stoffen oder Arbeitsverfahren erstmalig ausgesetzt werden. Sie sollen dann alle Veränderungen, wie z. B. Beendigung des Kontaktes, sowohl aus betriebsbedingten Gründen als auch durch Beendigung des Arbeitsverhältnisses melden. Der Arbeitnehmer soll nach dem Ausscheiden aus dem Betrieb über die über ihn gespeicherten Daten informiert und gleichzeitig darüber aufgeklärt werden, daß er nach seinem Ausscheiden aus dem Betrieb einen Anspruch auf kostenlose Vorsorgeuntersuchung hat. Ihm wird gleichzeitig in Aussicht gestellt, daß man sich zu gegebener Zeit unaufgefordert mit ihm in Verbindung setzen wird, um näheres über die Untersuchung zu vereinbaren. Er soll gleichzeitig gebeten werden, für diesen Zweck Änderungen seiner Anschrift an ODIN zu geben. Langfristig ist geplant, die freiwillige Meldung von Änderungen der Anschrift des Arbeitnehmers durch ein automatisiertes Abfrageverfahren bei Meldebehörden zu ersetzen. Der Arbeitgeber soll von den gesamten Meldungen eine Kopie wie Personalpapiere mindestens bis zum Ablauf des Jahres verwahren, in dem der Betroffene 75 Jahre alt geworden ist oder wäre.

Als Ziele der Einrichtung des ODIN-Verfahrens werden im wesentlichen genannt:

— Sicherstellung der gesundheitlichen Betreuung des Betroffenen nach dem Ausscheiden aus dem dafür bis dahin zuständigen Betrieb,

— Sicherung von Beweisen für evtl. auftretende Renten- oder andere Entschädigungsansprüche,

— Zentrale Organisation der Abrechnung und Beitreibung der Kosten für Vorsorgeuntersuchungen.

Für die Durchführung dieses Verfahrens bedarf es der Verarbeitung einer Vielzahl äußerst sensibler personenbezogener Daten der Betroffenen durch die Arbeitgeber und Berufsgenossenschaften. Dies stellt einen Eingriff in deren informationelles Selbstbestimmungsrecht dar. Nach geltendem Datenschutzrecht ist ein solcher Eingriff jedoch nur im überwiegenden Allgemeininteresse zulässig und er bedarf einer verfassungsmäßigen gesetzlichen Grundlage, die den Geboten der Normenklarheit und der Verhältnismäßigkeit gerecht wird. Die Verwendung der Daten ist auf den gesetzlich festgelegten Zweck begrenzt.

Soweit im Zusammenhang mit diesem Verfahren personenbezogene Daten durch die Arbeitgeber verarbeitet werden sollen, sind bei der Prüfung der Zulässigkeit die Vorschriften des § 22 des Bremischen Datenschutzgesetzes betreffend den Datenschutz bei Dienst- und Arbeitsverhältnissen mit öffentlichen Stellen zu beachten, da Mitglieder des Bremischen Gemeindeunfallversicherungsverbandes bis auf wenige Ausnahmen öffentliche Stellen sind. Nach dieser Vorschrift dürfen öffentliche Stellen Daten über ihre Beschäftigten nur verarbeiten, soweit dieses zur Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es erlaubt oder zwingend voraussetzt. Da die hier beabsichtigte Verarbeitung für die Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses nicht erforderlich ist, ist ihre Zulässigkeit davon abhängig, ob sie durch eine der genannten Rechtsgrundlagen erlaubt wird oder zwingend ist. Als bereichs-

spezifische Normen sind in diesem Fall das Chemikaliengesetz und die dazu ergangene Gefahrstoffverordnung anzusehen. Sie regeln abschließend, in welchem Umfange personenbezogene Daten zum Zwecke des Schutzes des Lebens der Arbeitnehmer, die mit gefährlichen Stoffen in Berührung kommen, verarbeitet werden dürfen.

Die Arbeitgeber sind danach verpflichtet, für Arbeitnehmer, die aufgrund der Bestimmungen der Gefahrstoffverordnung ärztlich untersucht worden sind, eine Kartei zu führen, die in etwa die gleichen Daten des Arbeitnehmers enthalten muß, wie sie im ODIN-Verfahren zur Verarbeitung vorgesehen sind. Die Normen enthalten abschließende Regelungen darüber, an welche Stellen der Arbeitgeber Daten übermitteln darf bzw. zu deren Übermittlung er verpflichtet ist. Eine Übermittlung der Daten an Berufsgenossenschaften ist dabei nicht vorgesehen. Der Arbeitgeber hat die Vorsorgekartei und ärztliche Bescheinigungen dem Arbeitnehmer beim Ausscheiden aus dem Betrieb auszuhändigen. Eine Offenbarung der hier enthaltenen Angaben an Dritte ist unzulässig. Die am ODIN-Verfahren beteiligten Berufsgenossenschaften berufen sich zur Rechtfertigung der Verarbeitung der personenbezogenen Daten insbesondere auf das internationale Übereinkommen über die Verhinderung und Bekämpfung der durch krebserregende Stoffe und Einwirkungen verursachten Berufsgefahren (ILO-Übereinkommen), welches durch Gesetz vom 13. 05. 1976 Bestandteil des Bundesrechts geworden ist.

Dieses verpflichtet die ratifizierenden Mitglieder jedoch nur, die Maßnahmen vorzuschreiben, die zum Schutz der Arbeitnehmer gegen die Gefahren einer Exposition gegenüber krebserregenden Stoffen oder Einwirkungen zu treffen sind, für die Einführung eines geeigneten Aufzeichnungssystems zu sorgen und sicherzustellen, daß sich Arbeitnehmer während und nach ihrer Beschäftigung ärztlichen Untersuchungen oder biologischen Tests unterziehen können. Maßnahmen selbst schreibt das Übereinkommen nicht vor. Es enthält nur Prinzipien, deren Umsetzung im Hoheitsbereich des jeweiligen Staates bleibt. Es bestimmt, daß jeder ratifizierende Staat im Wege der Gesetzgebung oder mittels anderer, den innerstaatlichen Gepflogenheiten und Verhältnissen entsprechende Methoden und in Beratung mit den maßgebenden beteiligten Arbeitgeber- und Arbeitnehmerverbänden, die zur Durchführung der Bestimmungen des Übereinkommens erforderlichen Maßnahmen zu treffen hat. Es enthält nur Aufgabenbeschreibungen, jedoch keine Befugnisse und kann deshalb keine ausreichende Rechtsgrundlage für Eingriffe in Grundrechte sein. Selbst wenn man in der Erwähnung der Einführung eines geeigneten Aufzeichnungssystems eine solche Rechtsgrundlage sehen wollte, würde sie die im ODIN-Verfahren beabsichtigte Datenverarbeitung nicht erlauben, denn das Übereinkommen legt fest, daß die betroffenen Arbeitnehmer alle zur Verfügung stehenden Informationen über die mit ihrer Arbeit verbundenen Gefahren und die zu treffenden Maßnahmen erhalten und an Untersuchungen teilnehmen können sollen. Die freiwillige Entscheidung der Arbeitnehmer soll also mit Informationen gefördert werden. Dem liegt ein Konzept der Eigenverantwortlichkeit der Betroffenen zugrunde, während die Konzeption von ODIN dagegen vom nicht allzu mündigen Bürger ausgeht, der an die Wahrnehmung seiner Interessen besser immer wieder erinnert werden soll. Vor diesem Hintergrund gesehen, kann das ODIN-Verfahren vielmehr als nicht vereinbar mit dem ILO-Übereinkommen gesehen werden, denn es ist zu besorgen, daß schutzwürdige Belange der Betroffenen beeinträchtigt werden.

Dadurch, daß der Arbeitnehmer durch regelmäßiges Anschreiben mit dem Ziel, ihn zur Teilnahme an Vorsorgeuntersuchungen anzuhalten, gegen seinen Willen ständig daran erinnert wird, daß er früher einmal eine das Krebsrisiko erhöhende Tätigkeit ausgeübt hat, kann durchaus eine Streßsituation bei ihm entstehen. Dazu kommt, daß die regelmäßige Aufforderung zur Teilnahme an Untersuchungen die Freiheit der Entscheidung des Betroffenen infolge des dadurch entstehenden psychischen Drucks beeinträchtigen kann. Ein solcher Druck kann z. B. dadurch entstehen, daß er befürchtet, Nachteile zu haben, falls er aufgrund der Kontakte mit den Gefahrstoffen erkrankt und Leistungen der Berufsgenossenschaft in Anspruch nehmen muß. Bedenkt man dabei, daß ärztliche Untersuchungen anerkanntermaßen ein nicht unerheblicher Streßfaktor für die Betroffenen sind, muß bezweifelt werden, daß das ODIN-Verfahren als Mittel zur Erreichung der erklärten Ziele, nämlich Sicherstellung der gesundheitlichen Betreuung und Sicherung von Beweisen für evtl. auftretende Entschädigungsansprüche, dem Grundsatz der Verhältnismäßigkeit entspricht. Das Chemikaliengesetz und die dazu ergangene Gefahrstoffverordnung haben die Forderungen des ILO-Übereinkommens mit deren Erlaß erfüllt und dabei eine Form der Verarbeitung der personenbezogenen Daten der Betroffenen normiert, die als verfassungskonform angesehen werden kann.

Soweit die Unfallversicherungsträger sich auf die Unfallverhütungsvorschriften als Rechtsgrundlage für die Zulässigkeit der Verarbeitung der Daten berufen, ist beachtlich, daß die Hoheit der mit Satzungsrecht begabten Körperschaften sich auf ihre Mitglieder, nämlich die Arbeitgeber und die Versicherten, also die bei den Mitgliedern beschäftigten Arbeitnehmer, beschränkt. Sie können nicht eingreifen in Grundrechte von Arbeitnehmern, die auf die Gestaltung der Satzungen keinen Einfluß nehmen können, weil sie nicht in den satzungsrechtsetzenden Organen vertreten sind. Versicherte sind aber nur tatsächlich Beschäftigte, die der Verfügungsgewalt eines Mitgliedes unterstehen, nicht aber ausgeschiedene Arbeitnehmer, es sei denn, sie erhalten Leistungen der Berufgenossenschaft. Demnach können Unfallverhütungsvorschriften zumindest nicht die Verarbeitung personenbezogener Daten nicht mehr versicherter Betroffener legitimieren. Im übrigen ist zu bezweifeln, ob die Ermächtigung der Reichsversicherungsordnung zum Erlaß von Unfallverhütungsvorschriften als ausreichende gesetzliche Grundlage für Eingriffe in das Recht auf informationelle Selbstbestimmung angesehen werden kann.

Ich habe dem Bremischen Gemeindeunfallversicherungsverband mitgeteilt, daß die beabsichtigte Beteiligung am ODIN-Verfahren aus den vorstehenden Gründen datenschutzrechtlich unzulässig ist. Der Bremische Gemeindeunfallversicherungsverband hat mir erklärt, daß er sich bei einer möglichen Beteiligung am ODIN-Verfahren auf solche Betroffenen beschränken will, die in die damit verbundene Verarbeitung ihrer personenbezogenen Daten ausdrücklich eingewilligt haben.

Anzumerken bleibt, daß von dem ODIN-Verfahren für die betroffenen Arbeitnehmer ähnliche Gefahren erwartet werden können, wie sie in der politischen Diskussion um ein allgemeines bundesweites Krebsregister zum Ausdruck gekommen sind (vgl. den 5. Jahresbericht unter Pkt. 5.2.9.1). Insoweit kann vermutet werden, daß eine eventuell beabsichtigte gesetzliche Regelung, die das ODIN-Verfahren in der bisher vorgesehenen Form erlauben soll, nicht dem Verfassungsgrundsatz der Verhältnismäßigkeit, insbesondere dem Verbot des Übermaßes gerecht würde.

5.12.2 Datenverarbeitung bei der Durchführung der Wahlen zu den Arbeitnehmerkammern

Aus Anlaß der im Jahre 1987 durchgeführten Wahlen zu den Arbeitnehmerkammern hat mich eine große Zahl von Eingaben und Beschwerden sowohl von Arbeitgebern als auch von Arbeitnehmern erreicht, die vornehmlich die Frage der Zulässigkeit der Übermittlung der personenbezogenen Daten von Arbeitnehmern durch die Arbeitgeber an die zuständigen Wahlvorstände und der Verwendung der Wählerverzeichnisse als Mitgliederverzeichnisse durch die Arbeitnehmerkammern zum Gegenstand hatten.

Ich habe die Eingaben und Anfragen dahingehend beschieden, daß aufgrund der im Jahre 1987 vom Senator für Wirtschaft und Außenhandel erlassenen Wahlordnung für die Wahlen zu den Arbeitnehmerkammern sowohl die vorgeschriebene Übermittlung der Arbeitnehmerdaten durch die Arbeitgeber an die Wahlvorstände als auch die Nutzung der Wählerverzeichnisse als Mitgliederverzeichnisse durch die jeweilige Arbeitnehmerkammer zulässig ist.

Es bleibt jedoch darauf hinzuweisen, daß die entsprechenden Vorschriften der Wahlordnung nur im Rahmen des Übergangsbonus als zulässig angesehen werden können, weil die Ermächtigung zum Erlaß der Wahlordnung im Gesetz über die Arbeitnehmerkammern nicht die an eine das Recht auf informationelle Selbstbestimmung einschränkende Norm geforderte Voraussetzung der Normenklarheit erfüllt..

Der Gesetzgeber bleibt deshalb aufgerufen, alsbald eine entsprechende Regelung vorzunehmen.

6. Nicht-öffentlicher Bereich

6.1 Versand- und Einzelhandel

6.1.1 Datenschutzprobleme beim Versandhandel

Bereits in meinem letzten Jahresbericht unter Pkt. 6.3.1 hatte ich darauf hingewiesen, daß die seit mehreren Jahren von den obersten Aufsichtsbehörden getragene gemeinsame Initiative mit dem Bundesverband des deutschen Versandhandels über Datenschutzfragen ins Gespräch zu kommen, von dieser Seite auf Ablehnung stieß. Wegen der sich häufenden Probleme wurde im letzten Jahr mit Vertretern des Bundesverbandes des deutschen Versandhandels über die datenschutzrechtlichen Probleme ein Gespräch geführt, wobei allerdings von seiten des Versand-

handels keinerlei Entgegenkommen gegenüber den Vorschlägen der Datenschutzaufsichtsbehörden zu erkennen war.

Bei diesem Gespräch haben die Vertreter der Datenschutzaufsichtsbehörden nochmals ausführlich ihre Forderung nach mehr Transparenz für den Betroffenen bei der Verarbeitung seiner Daten durch den Versandhandel hingewiesen. Dabei wurde betont, daß nicht beabsichtigt sei, für den Umworbenen über das Bundesdatenschutzgesetz hinausgehende Rechte zu begründen. Die Gewährleistung der Rechte des Betroffenen setzt jedoch bereits nach der geltenden Rechtslage ein Höchstmaß an Transparenz voraus; auch die Entwicklung der Rechtsprechung und die geplante Bundesdatenschutzgesetz-Novelle zielten in diese Richtung.

Zahlreiche Eingaben zeigen nämlich, daß bei den Betroffenen zum Teil großes Unbehagen herrscht, weil sie nicht nachvollziehen können, auf welchem Wege ein werbendes Unternehmen in den Besitz ihrer Adressen gelangt ist. Die Geltendmachung ihrer Rechte, insbesondere die Löschung von Anschriften, stößt in der Praxis auf erhebliche Schwierigkeiten. Die Vertreter der Datenschutzaufsichtsbehörden schlugen deshalb vor, die mit den Vertretern des Zentralausschusses der Werbewirtschaft und des Deutschen Direktmarking Verbandes erzielten Lösungsvorschläge auch beim Versandhandel als Grundlage für Werbemaßnahmen zu übernehmen.

Die Vertreter des Bundesverbandes des deutschen Versandhandels wiesen mit Nachdruck darauf hin, daß die dort erzielten Lösungsmöglichkeiten vom Versandhandel nicht akzeptiert werden könnten. Zum einen bestehe keine umfassende Deckungsgleichheit der Interessenlage der Verbände, zum anderen sehe der Bundesverband keine Notwendigkeit für das von den Datenschutzreferenten vorgeschlagene Verfahren. Im übrigen habe er auch keine Möglichkeit, seinen Mitgliedern ein bestimmtes Verfahren vorzuschreiben, sondern sei auf deren freiwillige Mitwirkung angewiesen.

Eine Umfrage unter seinen Mitgliedern habe ergeben, daß Anfragen nach der Adressenherkunft nur in verschwindend geringem Umfange gestellt würden. Die Umworbenen seien im übrigen an weiterer Aufklärung nicht interessiert. Im übrigen wiesen die Vertreter des Bundesverbandes darauf hin, daß die Herkunft einer Anschrift in vielen Fällen schon deshalb nicht mehr feststellbar sei, weil meistens mehrere Adressenbestände zusammengeführt würden und eine Zuordnung einzelner Adressen anschließend nicht mehr möglich sei. Außerdem bereite es in diesen Fällen technische Schwierigkeiten, dem Betroffenen die Selektionskriterien mitzuteilen. Um die von den Vertretern der Datenschutzaufsichtsbehörden geforderte Bekanntgabe der Selektionskriterien erfüllen zu können, müßten in die Werbeschreiben unterschiedliche, auf die jeweils genutzten Adreßbestände bezogene Hinweise aufgenommen werden. Eine solche Verfahrensweise sei aber völlig unverhältnismäßig. Jede zusätzliche Information zur Datenverarbeitung, sei es durch Hinweis im Werbeschreiben oder durch gesonderten Beipackzettel, würden erhebliche Zusatzkosten verursachen und seien für den Versandhandel nicht zumutbar. Jedenfalls bestehe seitens der Umworbenen kein Bedürfnis für eine solche Aufklärung.

Aufgrund der Ausführungen des Versandhandels kann nicht ausgeschlossen werden, daß durch weitere Aufklärung der Betroffenen über die Datenverarbeitung dies zu einem erhöhten Auskunftsverlangen der Kunden bei den speichernden Stellen führen könnte. Der Vorschlag der Vertreter der Datenschutzaufsichtsbehörden, auf dem Bestellschein durch entsprechende Ankreuzfelder den Betroffenen die Möglichkeit zu eröffnen, der Weitergabe seiner Anschrift zu Werbezwekken an Dritte zu widersprechen, wurde von den Vertretern des Versandhandels mit dem Hinweis zurückgewiesen, daß dies bei der geringen Zahl von Widersprüchen gegen die Adreßweitergabe nicht gerechtfertigt sei und jede zusätzliche Information den Kunden verunsichere.

Auch das Anliegen der Vertreter der Datenschutzaufsichtsbehörden, dem Kunden das Datenaustauschverfahren zwischen dem Versandhandel und der Schufa transparenter zu machen, stieß auf Ablehnung. Die Vertreter des Bundesverbandes machten deutlich, daß von ihren Mitgliedsunternehmen unter Hinweis auf diese geringe Zahl von Anfragen dieser Vorschlag ebenfalls grundsätzlich abgelehnt werde. Allerdings erklärten sie sich bereit, mit ihren Mitgliedsunternehmen die Frage zu erörtern, ob der für den normalen Kunden häufig mißverständliche Zusatz „— Bonität vorausgesetzt —"durch eine andere Formulierung ersetzt werden könne, die für Neukunden oder für Einrichtung eines Kreditkontos dem Kunden deutlicher mache, daß eine Schufa-Anfrage erfolge. Auch soll mit den Mitglieds-

unternehmen diskutiert werden, ob ein Betroffener von einer Negativ-Meldung an die Schufa unterrichtet werden kann. Es sei denkbar, hierzu einen entsprechenden Hinweis in das Mahnschreiben an den Betroffenen aufzunehmen. Dabei gingen die Vertreter des Versandhandels davon aus, daß in der Regel nur Mahnungen wegen unbestrittener Forderungen gemeldet werden; dies soll jedoch noch geprüft werden. Die Vertreter des Verbandes der Versandhäuser sagten zu, die Aufsichtsbehörden über das Ergebnis der verbandsinternen Meinungsbildung zu unterrichten.

Zur Frage der Identitätsprüfung bei fehlendem Geburtsdatum teilten die Vertreter des Versandhandels mit, daß seitens der Schufa inzwischen neben dem Geburtsdatum auch die Angabe des Geburtsortes gefordert werde. Fehle diese, erteile die Schufa keine Auskünfte mehr. Da der Geburtsort bei Bestellungen aber nicht erfragt werde, ergäben sich für den Versandhandel insoweit erhebliche Schwierigkeiten.

Die Anregung der Datenschutzreferenten, ein gemeinsames Gespräch zwischen Versandhandel, Schufa und Aufsichtsbehörde zu führen, soll zunächst mit den Mitgliedsunternehmen des Versandhandels erörtert werden.

Die Auffassung der Datenschutzaufsichtsbehörden, die Versandhandelsunternehmen unterlägen als Adreßanbieter dem 4. Abschnitt des Bundesdatenschutzgesetzes, wurde von den Vertretern des Versandhandels u. a. mit dem Hinweis darauf abgelehnt, die angekündigte Novelle des § 24 BDSG lasse eine Klarstellung in ihrem Sinne erwarten. Eine Annäherung in dieser Frage wurde nicht erzielt.

6.1.2 Täterkartei der Zentrale zur Eindämmung von Diebstählen im Buchhandel

Mir ist bekannt geworden, daß im Jahre 1970 der Verein „Zentrale zur Eindämmung von Ladendiebstählen im Buchhandel e. V." mit Sitz in Frankfurt am Main mit dem Ziel gegründet worden sei, Wiederholungstäter von Ladendiebstählen im Buchhandel schneller zu erkennen und durch den Hinweis im Geständnisprotokoll, es würde eine Aufnahme in eine zentrale Täterkartei erfolgen, einen zusätzlichen Abschreckungseffekt zu erzielen. Die Tätigkeit des Vereins sollte eine besondere Form der Dienstleistung für die Buchhändler darstellen. Aus der Kartei sollten Auskünfte nur an die Polizei erteilt werden.

Eine Prüfung durch die zuständige Aufsichtsbehörde hat ergeben, daß der Verein bereits seit Jahren keine Aktivität mehr entfaltet. Eine Löschung der Daten wurde verlangt.

6.1.3 Bonitätsprüfung

Von einem Bürger war ich gebeten worden zu prüfen, warum er als Baustoffkäufer seine Ware noch vor Anlieferung bezahlen sollte. In diesem Zusammenhang äußerte er die Vermutung, daß der Baustoffhändler im Rahmen einer Bonitätsprüfung über eine Auskunftei fälschlicherweise Auskünfte über seinen, mit einer Firma in Konkurs gegangenen Bruder erhalten haben könne.

Ich habe bei dem Baustoffhändler eine Prüfung durchgeführt. Der Inhaber dieser Firma erklärte mir, mit welchen Kredit- und Wirtschaftsauskunfteien er zusammenarbeitet. Die von mir eingesehenen Auftrags- und Rechnungsunterlagen ergaben keine Anhaltspunkte dafür, daß Auskünfte von einer Bank oder bei einer Auskunftei eingeholt worden waren. Vielmehr sei es so gewesen, daß der Bruder für den Beschwerdeführer die Baustoffe telefonisch bestellt hatte und Barzahlung vereinbart hatte. Daß der Käufer die Waren vor Anlieferung bezahlen sollte, wurde damit begründet, daß aufgrund einer zu geringen Fahrzeugkapazität ein firmenfremder Spediteur eingeschaltet wurde, der aber nicht kassieren durfte.

6.2 Auskunfteien, Detekteien

6.2.1 Zentrale Datei über Mieter

Die Entwicklung der letzten Jahre hat gezeigt, daß für die verschiedensten Bereiche des privaten Rechtsverkehrs Auskunfteien entstehen. Neuerdings hat sich in Münster die Immobilien-Schutzgesellschaft der Vermieter mbH (ISV) gebildet. Sie versteht sich als Gegenpol zu den aus ihrer Sicht mieterfreundlichen Gesetzen und den Mieterschutzverbänden und hat sich die Aufgabe gestellt, Vermieter vor finanziellen Verlusten bei der Vermietung und Verpachtung zu schützen.

Nach eigenen Angaben hat die Firma 57 000 Anschriften von Vermietern mit Mehrfamilienhäusern aus der gesamten Bundesrepublik von einem Adreßverlag angekauft, sie sind nach Postleitzahlbezirken sortiert.

Vermietern wird in einem Anschreiben gezielt Schutz vor Mietverlust durch Speicherung und Weitergabe von Negativdaten über Mieter angeboten. Der Vermieter wird aufgefordert, Mieterdaten für das Informationssystem zu liefern. Dieses bundesweit gesammelte Datenmaterial wird in einem zentralen Informationssystem gespeichert, aufbereitet und für Auskunftszwecke bereitgehalten. In dem Antwortschreiben der ISV heißt es weiter, daß die zur Verfügung gestellten Auskünfte die nötige Selektion der Mieter erleichtere und objektiviere, so daß Mietausfälle und der damit zusammenhängende Ärger zumeist vermieden werden könne. Außerdem behauptet die Vermieter-Schutzgesellschaft in dem Anschreiben, daß die Speicherung von Negativdaten über Mieter von allen Datenschutzbeauftragten der Länder genehmigt worden ist.

Eine Genehmigung für ein solches Informationssystem wurde weder durch die Datenschutzbeauftragten des Bundes und der Länder noch durch die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich gegeben.

Wegen der überregionalen Bedeutung dieser neuen Auskunftei haben sich die obersten Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich mit dieser Angelegenheit befaßt. Sie halten das vorliegende Konzept dieser Firma für ein Auskunftssystem über Mieter für datenschutzrechtlich nicht vertretbar.

Als Rechtsgrundlage für die vorgesehene geschäftsmäßige Verarbeitung personenbezogener Daten im Sinne des § 31 Satz 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) kämen §§ 32 bis 35 BDSG in Betracht. Das Speichern der Daten von Mietern zum Zwecke der Übermittlung an anfragende Vermieter ist nach § 32 Abs. 1 BDSG nur zulässig, soweit kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange der Betroffenen beeinträchtigt werden.

Bei der gebotenen Abwägung dieses Informationsinteresses gegenüber den schutzwürdigen Belangen der Betroffenen sind die besonderen Gefahren, die sich für diese aus einem solchen Informationssystem ergeben können, zu berücksichtigen. Würde die Warndatei der Vermieter in der vorgesehenen Form verwirklicht, so müßte dies für eine darin mit Negativdaten erfaßte Person dazu führen, daß dieser die Beschaffung einer neuen Wohnung nahezu unmöglich gemacht oder zumindest erheblich erschwert wird. Angesichts dieser Gefahr für ein Rechtsgut von so elementarer Bedeutung kann aus der Sicht des Datenschutzes ein Warnsystem über Mieter allenfalls nur unter sehr eingeschränkten Voraussetzungen akzeptiert werden.

Erhebliche Bedenken bestehen nicht nur gegen die im sogenannten „Datenbogen über den Mieter" vorgesehenen, vom Vermieter auszufüllenden Datenfelder, sondern gegen das Verfahren insgesamt, soweit dies aus den vorliegenden Unterlagen erkennbar wird. Angaben des Vermieters über Mietschulden, Nebenkostenschulden oder Kautionsschulden des Mieters sind als solche weder eindeutig noch hinreichend gesichert und bergen damit in erheblichem Maße die Gefahr einer Beeinträchtigung schutzwürdiger Belange des Mieters in sich. Selbst in Fällen, in denen eine solche Forderung tatsächlich besteht, kann deren Nichterfüllung seitens des Mieters die verschiedensten Gründe haben, deren Berechtigung vielfach nur gerichtlich geklärt werden kann. In gleicher Weise ist ein Mahnbescheid — als einseitiger Akt des Vermieters — in hohem Maße geeignet, schutzwürdige Belange zu beeinträchtigen und zwar auch dann, wenn die gleichzeitige Meldung oder Nachmeldung eines Widerspruchs gegen den Mahnbescheid durch den Vermieter vorgesehen ist. Die „Wohnungskündigung" wegen zugrundeliegender Forderungen aus dem Mietverhältnis ist in ihrer Aussagefähigkeit ebenso wenig eindeutig und gesichert wie die behauptete Mietforderung als solche. Die hierzu von der Firma gegebenen Erläuterungen legen es zudem nahe, daß auch Kündigungen aus sonstigem „wichtigen Grund" zur Erfassung in der Datei gemeldet werden können. Störungen des Mietverhältnisses beruhen aber erfahrungsgemäß vielfach auf Verhaltensweisen beider Vertragspartner, sind häufig in starkem Maße durch deren Persönlichkeit geprägt und lassen schon deshalb regelmäßig einen Schluß auf künftiges Fehlverhalten des Mieters nicht zu. Entsprechendes gilt für Räumungsklagen, die aus verschiedenen Gründen erhoben werden können und über deren Berechtigung regelmäßig nur die Gerichte entscheiden können.

Ohne besondere Mitwirkung des betroffenen Mieters mitteilungsfähig und zu Auskunftszwecken speicherungsfähig erscheinen daher allenfalls folgende Angaben:

Vollstreckungsbescheid wegen Mietschulden einschließlich Nebenkostenschulden (soweit es sich nicht um Bagatellforderungen handelt), rechtskräftiges Ur-

teil auf Zahlung solcher Schulden oder wegen vertragswidrigen Verhaltens des Mieters oder rechtskräftiges Räumungsurteil aus diesen Gründen sowie die vom Gerichtsvollzieher bescheinigte fruchtlose Pfändung und die vom Vermieter erwirkte Abgabe der eidesstattlichen Versicherung bzw. des Haftbefehls zur Abgabe der eidesstattlichen Versicherung jeweils auf der Grundlage titulierter Forderungen aus dem Mietverhältnis.

Darüber hinausgehende Mitteilungen des Vermieters an die Warndatei der Vermieter-Schutzgesellschaft könnten zwar auf der Grundlage einer ausdrücklichen schriftlichen Einwilligung des betroffenen Mieters in Betracht kommen. Eine solche Einwilligung darf aber nicht zur Bedingung für den Abschluß eines Mietvertrages gemacht werden. Sie wäre somit grundsätzlich erst nach Abschluß des Mietvertrages einzuholen, was ggf. nachzuweisen wäre. Damit dürfte die Einwilligung aber kaum praktikabel sein.

Die nach dem vorliegenden Konzept offenbar beabsichtigte und nach § 34 Abs. 1 BDSG erforderliche Benachrichtigung des Betroffenen durch die Auskunftei über die erfolgte Datenspeicherung reicht demgegenüber keinesfalls aus, um eine Beeinträchtigung schutzwürdiger Belange der Betroffenen auszuschließen. Der Mieter ist nicht verpflichtet, am Aufbau einer solchen Warndatei mitzuwirken; er braucht deshalb weder auf ein Anschreiben der Auskunftei zu reagieren, noch kann aus seiner Nichtäußerung gegenüber der Auskunftei auch die Richtigkeit der dort zur Speicherung vorgesehenen Angaben des Vermieters geschlossen werden. Andererseits kann es keineswegs akzeptiert werden, wenn — wie offenbar vorgesehen — dem Widerspruch des Betroffenen gegen die Speicherung seiner Daten bei der Mieterauskunftei in keinem Falle Bedeutung zugemessen werden soll.

Erhebliche Anforderungen wären im übrigen hinsichtlich der Verantwortlichkeit der Vermieter-Schutzgesellschaft als Betreiber des Informationssystems zu stellen, dies nicht zuletzt deshalb, weil die als Vertragspartner in Betracht kommenden Vermieter im Regelfall keiner Datenschutzkontrolle unterliegen. Dies gilt nicht nur hinsichtlich der Einhaltung gesetzlicher Löschungs- und Sperrungsfristen und der organisatorischen und technischen Maßnahmen zur Datensicherung, sondern — offenbar entgegen den bisherigen Vorstellungen der Auskunftei — auch hinsichtlich der inhaltlichen Richtigkeit der zu Auskunftszwecken gespeicherten Daten. Im Zuge der zunehmenden Automatisierung im Bereich der Auskunfteien ist nicht auszuschließen, daß in naher Zukunft größeren Vermietern ein Direktzugriff auf den Mieterdatenbestand der Vermieter-Schutzgesellschaft ermöglicht wird. Ein solcher Direktzugriff durch einen zukünftigen Vermieter im Rahmen der Anbahnung eines Mietvertragsverhältnisses greift so tief in das informationelle Selbstbestimmungsrecht des angehenden Mieters ein, daß der Weg zum „gläsernen Mieter" nicht mehr weit ist und somit schutzwürdige Belange des Mieters regelmäßig überwiegen dürften.

Dieser Fall macht erneut deutlich, daß das Bundesdatenschutzgesetz und damit der Gesetzgeber keinen ausreichenden Schutz im privaten Bereich bietet. Auch der vorliegende Entwurf zur Novellierung des Bundesdatenschutzgesetzes bringt für den Bürger keine Verbesserung.

6.2.2 Detekteien

Die Wahlkampfaffäre in Schleswig-Holstein warf auch Schatten in Bremen. Aufgrund einer Beschwerde überprüfte ich die Bremerhavener Detektei, deren Mitarbeiter in Schleswig-Holstein den Spitzenkandidaten der SPD heimlich observiert hatten. Da die Daten in dieser Detektei nicht in einer Datei, sondern aktenmäßig verarbeitet werden, war das Bundesdatenschutzgesetz nicht anwendbar, so daß ich meinen Kontrollbesuch abbrechen mußte.

Dieser Fall verdeutlicht einmal mehr die unbefriedigende Rechtslage im nichtöffentlichen Bereich. Während im staatlichen Bereich z. B. die Tätigkeit des Verfassungsschutzes an gesetzliche Regelungen gebunden wird, deren Einhaltung durch parlamentarische Kontrollgremien und Datenschutzbeauftragte kontrolliert werden, können Detekteien gegenwärtig ohne gesetzliche Regelungen und räumlich unbegrenzt, Bürger observieren. Zum Tätigkeitsbereich von Detektiven gehört es, fremde Personen zu observieren, d. h., Informationen über diese Personen zu erheben und diese gewonnenen Informationen an den Auftraggeber weiterzugeben. Die weitere Verwendung liegt dann im Belieben des Auftraggebers. So ist es z. B. möglich, daß im Strafprozeß Beweismittel verwertet werden dürfen, die durch Detektive in rechtswidriger Weise für die Strafverteidigung beschafft wurden. Die bei solchen Observationen zu Tage geförderten Informationen können —

ohne Rücksicht auf ihre Richtigkeit und aus dem Sachzusammenhang gerissen — sehr weitreichende Konsequenzen für den Betroffenen nach sich ziehen, die bis zum Rufmord reichen. Man denke nur daran, daß der Auftraggeber eines Detektives nur die ihm genehmen Ermittlungsergebnisse veröffentlicht oder auf andere Weise verbreitet. Die Eingriffsqualität der Observation steht derjenigen im öffentlichen Bereich nicht nach.

Die bisherige Rechtslage läßt eine Begrenzung der Tätigkeit von Detekteien nicht zu. Die gewerberechtliche Anzeigepflicht nach § 14 GewO erlaubt keine Beschränkung der Ermittlungstätigkeit von Detektiven. Da die Detekteien in der Regel keine Dateien im Sinne des Bundesdatenschutzgesetzes führen, fallen sie nicht unter den Anwendungsbereich des Bundesdatenschutzgesetzes und unterliegen damit auch nicht der externen Datenschutzkontrolle. Eine staatliche Berufsordnung existiert ebenfalls nicht. Die Grenze für die Ermittlungstätigkeit von Detektiven bildet lediglich das Strafgesetzbuch. Es verbietet nicht, Bürger Tag und Nacht zu observieren. Eine nachträgliche Unterrichtung über eine solche Maßnahme ist nicht vorgesehen.

Das vom Bundesverfassungsgericht aus dem Grundgesetz abgeleitete Recht auf informationelle Selbstbestimmung muß auch für die Informationsverarbeitung durch Detekteien und ähnlich tätige Auskunfteien gelten. Auch aus diesem Grunde sollte die Beschränkung des Bundesdatenschutzgesetzes auf die Informationsverarbeitung in Dateien aufgehoben werden und dieses Gesetz auf jegliche Informationsverarbeitung Anwendung finden.

Der Bundesgesetzgeber ist aufgefordert, die Tätigkeit der Detekteien gesetzlich zu begrenzen. Dabei ist die Zulässigkeit der Informationsbeschaffung und -verarbeitung exakt zu normieren. Für die Betroffenen sind Auskunfts- und Löschungsansprüche, für die Detekteien Benachrichtigungs- und Löschungspflichten zu schaffen. Die Detekteien sind einer ständigen Kontrolle durch Datenschutzaufsichtsbehörden zu unterwerfen, die Kontrollbefugnisse der Aufsichtsbehörden sind gegenüber der jetzigen Rechtslage auszuweiten.

6.3 Datenschutz in der Versicherungswirtschaft

6.3.1 Verhandlungen mit der Versicherungswirtschaft

6.3.1.1 Schweigepflichtentbindungsklausel

Seit mehreren Jahren verhandeln die Datenschutzaufsichtsbehörden mit der Versicherungswirtschaft über die Anpassung der Schweigepflichtentbindungsklausel an die datenschutzrechtlichen Erfordernisse. Den letzten Stand der Verhandlungen hatte ich im 9. Jahresbericht unter Pkt. 6.5.1 dargestellt. Es hat langer Verhandlungen bedurft, um festzustellen, welche von der gegenwärtig benutzten Klausel scheinbar abgedeckten Recherchen der Versicherungen bei Ärzten nur aufgrund einer konkreten Einzeleinwilligung zulässig sind und daher nicht in die Klausel mit aufgenommen werden können.

Nachdem insoweit Einvernehmen bestand, bedurfte der von der Versicherungswirtschaft auf der letzten Sitzung vorgelegte Formulierungsentwurf nur noch in zweierlei Richtungen einer Präzisierung. Zum einen wurde von den Datenschutzaufsichtsbehörden vorgeschlagen, daß die Klausel nicht mehr so allgemein gefaßt wird, daß sie sowohl für Lebensversicherungen als auch für Kranken- und Unfallversicherungen gilt, sondern daß für jeden Versicherungszweig eine eigenständige Schweigepflichtentbindungsklausel formuliert wird. Zum anderen sollte die Geltungsdauer der Einwilligungsklausel präzisiert werden. Hierbei ist zu differenzieren nach der Dauer und dem Kreis der von der Schweigepflicht Entbundenen bei Abschluß des Vertrages und bei Abwicklung des Vertrages. Hinsichtlich der Geltung der Schweigepflichtentbindung bei Abschluß des Vertrages soll die Kündigungsfrist durch die Versicherung als zeitliche Begrenzung genommen werden. Die Entbindung von der Schweigepflicht kann sich hier nur auf vor Vertragsabschluß behandelnde Ärzte beziehen.

Die Schweigepflichtentbindungsklausel bei Lebensversicherungen hat nach dem letzten Verhandlungsstand den folgenden Wortlaut:

„Ich ermächtige den Versicherer zur Nachprüfung und Verwertung der von mir über meine Gesundheitsverhältnisse genannten Angaben alle Ärzte, Krankenhäuser und sonstigen Krankenanstalten, bei denen ich in Behandlung war oder sein werde, sowie andere Personenversicherer über meine Gesundheitsverhältnisse bei Vertragsabschluß zu befragen; dies gilt für die Zeit vor der Auftrags-

annahme und die nächsten drei Jahre nach der Antragsannahme. Der Versicherer darf auch die Ärzte, die die Todesursache feststellen, und die Ärzte, die mich im letzten Jahr vor meinem Tode untersuchen und behandeln werden, sowie Behörden mit Ausnahme von Sozialversicherungsträgern, über die Todesursache oder die Krankheit, die zum Tode geführt haben, befragen.
Insoweit entbinde ich alle, die hiernach befragt werden, von der Schweigepflicht auch über meinen Tod hinaus."

Bei der Schweigepflichtentbindung in Krankenversicherungsverträgen bezogen auf den Leistungsfalle soll klargestellt werden, daß nur die vom Patienten eingereichten Rechnungen zum Anlaß genommen werden können, bei dem durch die Rechnung ausgewiesenen Arzt Nachfrage zu halten. Rechtlich ist die Einreichung einer Arztrechnung bei entsprechender Formulierung der Einwilligungsklausel dann so zu werten, daß damit der Versicherungsnehmer gegenüber der Versicherung konkret erklärt, daß er den aus der Rechnung erkennbaren behandelnden Arzt im Rahmen der Rechnungsprüfung durch das Versicherungsunternehmen von seiner Schweigepflicht entbindet.

Diese Vorschläge müssen im Gesamtverband der deutschen Versicherungswirtschaft noch abgestimmt werden. Es geht um eine praktikable und für die Versicherungswirtschaft auch unter ökonomischen Gesichtspunkten akzeptable Lösung dieses Datenschutzproblems. Die Gespräche sind noch nicht abgeschlossen.

6.3.1.2 Ermächtigungsklausel zur Datenverarbeitung

Die Neuformulierung der in den allgemeinen Geschäftsbedingungen der Versicherungswirtschaft enthaltenen Klausel, die das Versicherungsunternehmen zu verschiedenen Datenverarbeitungen ermächtigt, ist ebenfalls seit langem ein Auseinandersetzungspunkt zwischen der Versicherungswirtschaft und den Obersten Aufsichtsbehörden für den Datenschutz. Den letzten Stand hierzu habe im im 9. Jahresbericht unter Pkt. 6.5.2 dargestellt.

Wegen der zum Teil recht umfangreichen Datenverarbeitung im eigenen Versicherungsunternehmen wie auch der Übermittlung an Zentraldateien oder dem Abgleich mit Datenbeständen anderer Versicherungsunternehmen können die gesamten Datenverarbeitungsvorgänge eines Versicherungsunternehmens nicht vollständig in einer Klausel dargestellt werden, sondern bedürfen der Erläuterung durch ein Merkblatt. Über diese Trennung zwischen Datenverarbeitungsklausel und ergänzendem Merkblatt hatte man sich bei den Gesprächen bereits geeinigt. Die Versicherungswirtschaft hatte daraufhin den Entwurf einer Klausel und eines Merkblattes vorgelegt (Parallele bei dem mit den Banken erzielten Ergebnis zur Schufa-Klausel und Merkblatt/vgl. in meinem 9. Jahresbericht unter Pkt. 6.2.3). Der Wortlaut der Klausel sollte dabei alle in den jeweiligen Branchen möglichen Datenverarbeitungen abdecken. Die vorgelegten Texte zur Klausel und zum Merkblatt waren nach Meinung der Verhandlungspartner aber dadurch so unübersichtlich geworden, daß den Besprechungsteilnehmern vielfältige Auslegungsmöglichkeiten wahrscheinlich erschienen, die in dieser Weite selbst von keiner Sparte der Versicherungswirtschaft beabsichtigt sind.

Die Versicherungswirtschaft ist daher gebeten worden, Datenverarbeitungsklauseln für die einzelnen Versicherungszweige und darauf abgestimmt ein Merkblatt zu entwickeln. Durch die Erstellung des Merkblattes soll die Datenverarbeitung für den Versicherungsnehmer transparenter gestaltet werden, damit er sich ein Bild davon machen kann, zu welchen Zwecken seine Daten verarbeitet werden. Die Versicherungswirtschaft hat zugesagt, neue Formulierungen vorzulegen.

Die Vertreter der Obersten Aufsichtsbehörden haben bei der letzten Besprechung im übrigen darauf hingewiesen, daß sie es nicht für ausreichend erachten würden, wenn der abschlußbereite Versicherungskunde erst nach Unterschrift des Vertrages die Zusendung des Merkblattes erbitten kann. Vielmehr ist von ihm mit seiner Unterschrift zu dokumentieren, daß er bei Vertragsabschluß die Möglichkeit gehabt hat, vom Inhalt des Merkblattes Kenntnis zu nehmen. Nur eine in Kenntnis der Datenverarbeitung abgegebene Willenserklärung kann eine rechtsverbindliche Willenserklärung darstellen. Es muß dem potentiellen Versicherungsnehmer daher vor Abschluß des Vertrages möglich sein, sich auch über die Form der Datenverarbeitung zu informieren. Der Kunde kann selbstverständlich auf die Kenntnisnahme des Merkblattes ggf. verzichten. In diesen Fällen müßte der Kunde die Datenverarbeitungsklausel aber gegen sich gelten lassen.

Auch zu diesem Punkt bedarf es also noch weiterer Verhandlungen. Ich erwarte, daß nach mehrjährigen Verhandlungen allmählich ein Ergebnis sichtbar wird.

6.3.2 Übermittlung von Mitgliederdaten im Rahmen von Gruppenversicherungsverträgen

Bereits im 8. Jahresbericht hatte ich unter Pkt. 6.5.1 auf datenschutzrechtliche Probleme bei der Weitergabe von Mitgliederdaten an Versicherungen im Rahmen sog. Gruppenversicherungsverträge hingewiesen. Dem lagen mehrere Beschwerden von Betroffenen zugrunde, die nicht hinnehmen wollten, daß ihre personenbezogenen Daten, die sie einem Verband als Mitglied gegeben hatten, an Privatversicherungen weitergegeben werden. Erst auf mein intensives Drängen hat sich der Landesverband Bremen dieser Organisation dafür entschieden, bereits in die Beitrittserklärung eine Klausel aufzunehmen, deren Text lautet: „Ich bin damit einverstanden, daß meine Anschrift im Rahmen des XY-Gruppenversicherungsvertrages an die YZ-Versicherung weitergegeben werden darf." Der Beitretende kann sich zwischen den Alternativen ja und nein entscheiden. Damit wurde meinen früher geäußerten Empfehlungen zur Gewährung des Datenschutzes zum Teil entsprochen.

6.3.3 Weitergabe von Versicherungsdaten an den Geschädigten

Ein Bürger beschwerte sich darüber, daß seine Haftpflichtversicherung gegenüber seinen Nachbarn geäußert hat, daß sie einen Schaden nicht regulieren will, weil schon 6 Schadensfälle eingetreten seien, bei denen es Schwierigkeiten bei der Regulierung gegeben habe.

Der Bürger äußerte mir gegenüber die Befürchtung, daß durch diese Indiskretion Nachteile in seiner beruflichen Entwicklung entstehen könnten. Der Bürger hatte allerdings zwecks leichterer Regulierung des Schadens, den sein minderjähriger Sohn angerichtet hatte, dem Nachbarn seine Versicherung und die Versicherungsnummer mitgeteilt.

Meine Prüfung hat ergeben, daß der Nachbar sich unmittelbar an den Versicherer gewandt hatte. Die Haftpflichtversicherung teilte mir mit, daß sie den eingetretenen Schaden in voller Höhe reguliert habe, zu einer Auskunft über die Anzahl der Vorschäden des Versicherungsnehmers sei es nicht gekommen.

Ein Versicherungsnehmer muß allerdings in solchen Fällen, in denen die Regulierung des Schadens zwischen Geschädigten und Versicherungsunternehmen unmittelbar erfolgen soll, damit rechnen, daß dem Geschädigten mitgeteilt wird, daß eine Regulierung des Schadens durch sie nicht in Betracht kommt. Eine Mitteilung des Grundes, warum nicht reguliert wird, sei es wegen des Schadensverlaufs, sei es wegen vertraglicher Ausschlußgründe an den Geschädigten, ist allerdings nicht zulässig. Solche Erklärung darf die Versicherung allein gegenüber dem Versicherungsnehmer abgeben. Bei Ablehnung der Regulierung durch das Versicherungsunternehmen muß sich der Geschädigte dann wieder an die Schädiger wenden und von ihm eine Regulierung des Schadens verlangen.

6.4 Datenschutz bei Ärzten

Der Patient eines Röntgenarztes beschwerte sich bei mir darüber, daß sich die Rechnungsnummer einer Liquidationsrechnung aus dem Untersuchungsdatum und dem Geburtsdatum zusammensetzte. Aus dem Aufbau der Rechnungsnummer war dies auch für Dritte leicht zu erkennen. Beides sind personenbezogene Daten, die im Zusammenhang mit der Behandlung bzw. Untersuchung des Patienten der ärztlichen Schweigepflicht unterliegen. Der Arzt zwingt den Patienten insoweit, bei bargeldloser Zahlung sowohl sein Geburtsdatum als auch das Behandlungsdatum auf dem Überweisungsträger preiszugeben. Der Patient hätte nur eine Chance, die Daten geheimzuhalten, wenn er die Rechnungsnummer wegläßt oder bar bezahlt.

Ich habe den Arzt aufgefordert, den Aufbau der Rechnungsnummer so zu verändern, daß eindeutige personenbezogene Merkmale darin nicht mehr enthalten sind. Der Arzt hat meinen Anregungen entsprochen.

6.5 Arbeitnehmerdatenschutz

6.5.1 Einsichtsrecht in Personalakten durch Bevollmächtigten

Eine Firma hat dem Bevollmächtigten eines ausländischen Arbeitnehmers, der selbst die Akteneinsicht wegen Sprachschwierigkeiten gar nicht sinnvoll ausüben

FFD/12/163

kann und sich auch nicht auf den Betriebsrat verweisen lassen wollte, die Einsichtnahme in die Personalakte verwehrt. Die Firma vertrat den Standpunkt, die Personalakte sei Bestandteil der Handakte der Prozeßbevollmächtigten des Unternehmens und unterliege auch aus diesem Grunde nicht dem Akteneinsichtsrecht.

Der Bevollmächtigte hat mich um datenschutzrechtliche Stellungnahme gebeten.

Der Wahrnehmung des einem Arbeitnehmer nach § 83 des Betriebsverfassungsgesetzes (BetrVG) zustehenden Rechtes auf Einsichtnahme in über ihn geführte Personalakten durch einen Bevollmächtigten stehen datenschutzrechtliche Bestimmungen nicht entgegen. Die damit verbundene Bekanntgabe personenbezogener Daten an den Bevollmächtigten stellt keine Übermittlung im datenschutzrechtlichen Sinne dar, da der Bevollmächtigte nicht im eigenen Namen, sondern für den Berechtigten handelt.

Das Akteneinsichtsrecht nach dem Betriebsverfassungsgesetz soll dem Arbeitnehmer die Möglichkeit eröffnen zu erfahren, welche Daten über ihn gesammelt werden und ihn in die Lage versetzen zu kontrollieren, für welchen Zweck diese Daten verwendet werden. Er soll auch kontrollieren können, ob die über ihn gesammelten Daten richtig sind. Diese Vorschrift soll den Arbeitnehmer gegen den Mißbrauch der über ihn gesammelten Daten schützen. Sie verpflichtet zugleich den Arbeitgeber zu Verhaltensmaßnahmen, die eine Überschaubarkeit der Verwendung von Arbeitnehmerdaten gewährleistet.

Bei dieser Intention des Gesetzgebers ist jede Auslegung der Vorschrift in Richtung einer Verkürzung des Akteneinsichtsrechts unzulässig. Wenn man in dem vorliegenden Fall, in dem der Betroffene der deutschen Sprache kaum mächtig ist — jedenfalls nicht soweit, daß er deutsch lesen kann — Arbeitnehmer darauf verweisen würde, daß es sich bei dem Akteneinsichtsrecht nur um ein persönliches Recht handele, das er nicht mittels eines Bevollmächtigten ausüben könne, würden Sinn und Zweck der Vorschrift ins Leere gehen. Es muß ihm deshalb das Recht eingeräumt werden, sein Recht durch eine Person seines Vertrauens wahrnehmen zu lassen. Der Betroffene kann dabei auch nicht darauf verwiesen werden, daß er das Recht habe, ein Betriebsratsmitglied bei der Akteneinsicht hinzuzuziehen. Dieses im Betriebsverfassungsgesetz normierte Recht zielt nicht darauf ab, das Akteneinsichtsrecht des Betroffenen zu verkürzen. Es soll ihm vielmehr durch die Hinzuziehung einer mit Personalangelegenheiten vertrauten Person ein zusätzlicher Schutz gewährt werden.

Auch Rechtsmeinung und Rechtsprechung erkennen überwiegend an, daß der Arbeitnehmer zumindest in besonderen Fällen die Akteneinsicht von einem Bevollmächtigten ausüben lassen kann.

Der Auffassung des Arbeitgebers, daß das Akteneinsichtsrecht im Falle eines laufenden Arbeitsrechtsprozesses nicht gegeben sei, da die Personalakte dann Bestandteil der Prozeßakten des Prozeßgegners sei, kann nicht beigetreten werden, da offensichtlich ist, daß sich eine solche Einschränkung dieses Rechts weder aus dem Wortlaut noch aus der Zielsetzung der Vorschrift des § 83 BetrVG entnehmen läßt. Der Arbeitnehmer kann im vorliegenden Fall unter den gegebenen Umständen das ihm zustehende Akteneinsichtsrecht durch einen Bevollmächtigten wahrnehmen lassen.

6.5.2 Aufbewahrung und Behandlung von Bewerbungsunterlagen durch den Arbeitgeber

Auf einem Campingplatz in der Umgebung Bremens wurde eine Vielzahl von Bewerbungsunterlagen aus den Jahren 1985 und 1986 gefunden, die mir übergeben worden sind. Es handelt sich um Bewerbungsschreiben, Zeugnisse, Lebensläufe, Fotos und Anschreiben der Arbeitsverwaltung.

Ich habe dem Arbeitgeber, der einen Friseursalon betrieben hatte, meine datenschutzrechtliche Auffassung wie folgt dargelegt:

Mit der Einleitung und Durchführung des Bewerbungsverfahrens entsteht zwischen den Verhandelnden ein Anbahnungsverhältnis mit dem Ziel, einen Dienstvertrag nach § 611 BGB abzuschließen. Insoweit ist hier ein vorvertragliches Vertrauensverhältnis entstanden, aus dem Verhaltenspflichten zur gegenseitigen Sorgfalt und Rücksichtnahme erwachsen, deren Verletzung Schadensersatzansprüche begründen.

Nach Rechtsprechung und Literatur ist herrschende Auffassung, daß aus dem Grundsatz von Treu und Glauben nach § 242 BGB der allgemeine Rechtsgrundsatz

folgt, daß derjenige, der sich zum Zweck der Aufnahme von Vertragsverhandlungen in den Einflußbereich eines anderen begebe, in angemessenem Umfang die Berücksichtigung seiner Interessen verlangen kann.

Die beiden Vertragspartnern obliegenden Pflichten beinhalten u. a. die Obhutspflicht. Zur Obhutspflicht gehören insbesondere die sorgfältige Aufbewahrung und Behandlung der Bewerbungsunterlagen des Arbeitnehmers. Beide Verhandlungspartner haben darüber hinaus über die ihnen im Zusammenhang mit den Vertragsverhandlungen bekanntgewordenen Geheimnisse Stillschweigen zu bewahren. Außerdem haben beide Partner im Rahmen der Anbahnung eines Vertragsverhältnisses allgemeine Schutzpflichten zu beachten, wonach Person, Eigentum und sonstige Rechtsgüter des Vertragspartners nicht verletzt werden dürfen.

Insoweit gehört die Beachtung des informationellen Selbstbestimmungsrechts ebenfalls zu den Schutzpflichten bei der Anbahnung eines Vertragsverhältnisses.

Im Rahmen dieser Pflichten oblag es dem Arbeitgeber, die Bewerbungsunterlagen ordnungsgemäß aufzubewahren und nach Abschluß des Bewerbungsverfahrens den abschlägig beschiedenen Bewerberinnen zurückzugeben bzw. zu vernichten.

Der Arbeitgeber hat sich meiner Auffassung angeschlossen. Die Unterlagen sind inzwischen vernichtet worden.

6.5.3 Personalfragebogen im Rahmen von Bewerbungsverfahren

In mehreren Eingaben von Betroffenen und Betriebsräten ging es um die Frage, in welchem Umfange personenbezogene Daten der Betroffenen im Rahmen von Bewerbungs- und Einstellungsverfahren durch den Arbeitgeber mit Hilfe eines Personalfragebogens erhoben werden dürfen. Die Betroffenen wurden u. a. nach dem Vornamen und dem Beruf des Vaters gefragt und welche Elternteile noch leben.

Die inhaltliche Gestaltung des Personalfragebogens unterliegt nach § 94 Abs. 1 Betriebsverfassungsgesetz (BetrVG) der Mitbestimmung des Betriebsrats, der neben dem Arbeitgeber die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer gemäß § 75 Abs. 2 BetrVG zu schützen und zu fördern hat. Diese Schutzpflichten setzen bereits im Bewerbungsverfahren ein.

Nach herrschender Rechtsmeinung und der Rechtsprechung des Bundesarbeitsgerichts ergibt sich folgende datenschutzrechtliche Bewertung:

Hinsichtlich der Zulässigkeit der Datenerhebung im Einstellungsverfahren bedarf es der Abwägung der gegensätzlichen Interessen.

Der Arbeitgeber ist legitimerweise daran interessiert, möglichst umfassende Informationen über den Bewerber zu erhalten, um nach Auswertung der Bewerberdaten eine fundierte Personalentscheidung fällen zu können.

Dagegen hat der Arbeitnehmer/Bewerber einen Anspruch auf den Schutz seiner Persönlichkeitsrechte. Hier ist insbesondere das Recht auf informationelle Selbstbestimmung zu nennen.

Das Recht des Arbeitgebers zur Erhebung von Arbeitnehmerdaten ist insoweit eingeschränkt. Der Arbeitnehmer/Bewerber ist nur dann zur Beantwortung von Fragen verpflichtet, wenn der Arbeitgeber im Einzelfall an der Antwort ein berechtigtes, billigenswertes und schützenswertes Interesse hat. Um unzulässigen, das Informationsbedürfnis des Arbeitgebers überschreitenden Fragen begegnen zu können, hat das Bundesarbeitsgericht darüber hinaus dem Bewerber oder Arbeitnehmer die Möglichkeit eingeräumt, die das Recht zur Datenerhebung überschreitenden Fragen wahrheitswidrig zu beantworten. Die wahrheitswidrige Beantwortung einer unzulässigen, rechtswidrigen Frage wird nicht als arglistige Täuschung gewertet, die eine spätere Anfechtung des Arbeitsvertrages nach § 123 BGB rechtfertigen könnte.

Der rechtlich zulässige Umfang des Personalfragebogens ergibt sich unter Berücksichtigung dieser Grundsätze und bedarf einer umfangreichen Interessenabwägung. Bei der Interessenabwägung im Rahmen der Gestaltung eines Personalfragebogens muß auch unterschieden werden, ob es sich noch um die Anbahnung eines Arbeitsverhältnisses (Bewerbungsverfahren) handelt oder ob bereits die Einstellung vorgenommen werden soll.

Die zu erhebenden Daten müssen sich danach konkret auf den für den Bewerber vorgesehenen Arbeitsplatz beziehen. Daraus ergibt sich, daß der Bewerber/Arbeit-

nehmer z. B. die Angabe der vorgenannten Daten, die seine familiäre Situation betreffen und nicht im Zusammenhang mit dem angestrebten Arbeitsplatz stehen, ablehnen kann.

Schließlich muß der Personalfragebogen unverzüglich vernichtet werden, sobald Bewerbungen abschlägig beschieden worden sind.

6.5.4 Durchführung beruflicher Bildungsmaßnahmen zur Verbesserung der Vermittlungsaussichten

Die Mitarbeiter eines Trägers beruflicher Bildungsmaßnahmen zur Verbesserung der Vermittlungsaussichten gem. § 41a AFG hatten sich mit einer Eingabe an mich gewandt und gefragt, ob es datenschutzrechtlich zulässig sei, daß sie verpflichtet seien, über Teilnehmer ihres Lehrganges im Nachhinein einen Fragebogen auszufüllen, der sehr intime Daten der Kursteilnehmer enthält. Die Erhebung und die weitere Verarbeitung der Daten sollte die Grundlage für eine konzeptionelle Weiterentwicklung (Evaluation) des Trägers bilden.

Der Träger der Maßnahme nach § 41a AFG ist ein privatrechtlicher Verein, ich war daher als Aufsichtsbehörde gem. § 30 BDSG zuständig. Die §§ 22 ff. BDSG enthalten nur sehr allgemeine Datenverarbeitungsregelungen, die gleichermaßen für Personaldatenverarbeitung der Privatwirtschaft wie für die Datenverarbeitung der Versicherungswirtschaft und der Banken gelten. Sie bieten daher für die Situation eines Arbeitslosen keinen ausreichenden Schutz. Das Arbeitsamt Bremen, daß mit dem Träger zur Durchführung der Maßnahme nach § 41a AFG einen Vertrag geschlossen hat, habe ich deshalb angeschrieben und darauf hingewiesen, daß Kurse zur Verbesserung der Vermittlungsaussichten nach § 41a AFG das Arbeitsamt Bremen auch selbst durchführen könnte. In diesem Falle würden die Daten der Kursteilnehmer durch die besonderen Vorschriften des SGB geschützt. Eine Datenerhebung, wie sie der privatrechtliche Träger vorsieht, wäre nur unter den strengen Voraussetzungen des § 75 SGB X zulässig gewesen. Die Teilnehmer einer Maßnahme (Arbeitslose) dürfen aber dadurch, daß die Maßnahme von einem privaten Träger durchgeführt wird, nicht schlechter gestellt werden. Ich habe daher gegenüber dem Arbeitsamt Bremen erklärt, es wäre zu begrüßen, wenn es in den Verträgen mit privaten Einrichtungen sicherstellen würde, daß die Vorschriften des SGB X wenigstens entsprechend angewandt werden.

Es war scheinbar nicht mehr möglich, im konkreten Fall den Vertrag mit dem Träger nachzubessern bzw. auf die Einhaltung eines entsprechenden Verfahrens hinzuwirken. Mir wurde aber seitens des Arbeitsamtes erklärt, daß aufgrund der Mittelvergabe Verhandlungen für das Jahr 1988 geführt und ein neuer Vertrag zwischen dem Träger und dem Arbeitsamt erforderlich werden. Darin wolle man den datenschutzrechtlichen Anforderungen Rechnung tragen. Auf meine Anregung hin wird sich der Träger im neuen Vertrag datenschutzrechtlichen Vorschriften des SGB I und X unterwerfen.

Ich habe darauf hingewiesen, daß der Träger der Maßnahme nach § 41a AFG selbstverständlich im Einzelfall z. B. bei langfristigem unentschuldigten Fehlen etc. das Arbeitsamt unterrichten kann. Nicht hingegen erforderlich sei eine lückenlose vollständige Dokumentation der Lebenssituation des Arbeitslosen vor Aufnahme der Maßnahme und während der Maßnahme durch Speicherung all dieser Daten auf einem zentralen Computer. Auch wenn diese Daten dann zur Erstellung eines abstrakten Tätigkeitsberichts genutzt werden, ist es erforderlich zur Wahrung des informationellen Selbstbestimmungsrechts, daß der einzelne Teilnehmer gefragt wird, ob er seine Daten zu dieser Form empirischer Sozialforschung hergeben will. Ihm sind daher neben dem Datensatz Sinn und Zweck der Datenverarbeitung und die beabsichtigten Auswertungskriterien vor Einwilligung bekanntzugeben.

Die Vertreterin des Arbeitsamtes erklärte, daß das Arbeitsamt ohnehin eine solch dezidierte datenmäßige Begleitung der Maßnahme weder gefordert noch für notwendig erachtet hätte. Das Arbeitsamt Bremen habe ich auch gebeten zu prüfen, in welchem Umfange dem privaten Träger Daten zur Aufnahme der Maßnahme zur Verfügung zu stellen sind. In dem Vertrag war vorgesehen, daß neben einer Vormerkkarte ein Kurzantrag mit dem Datum der Antragsabgabe, dem Organisationszeichen und der ausgebenden Stelle sowie Name, Vorname des Teilnehmers beizufügen sind. Es könnte durchaus ausreichend sein, daß lediglich ein Kurzantrag, ergänzt um einige Daten, ausreichend ist. Die Vormerkkarte enthält häufig sehr viele Daten über den Arbeitslosen. Ein Leerformular dieser Karte, das mir bei einer Besprechung vorgelegt wurde, war mit der Aufschrift „Nur für den internen Dienstgebrauch" gekennzeichnet.

Das Arbeitsamt erklärte, grundsätzlich die Datenschutzfragen bei solchen Maßnahmen auch in bezug auf andere Träger mit dem Landesarbeitsamt zu klären und eine Untersuchung auch in anderen Bereichen zu veranlassen und sich dazu ggf. um die Beratung des Bundesbeauftragten für den Datenschutz zu bemühen.

Ich werde den Abschluß des neuen Vertrages zum Anlaß nehmen, bei diesem Träger die Einhaltung der getroffenen Datenschutzvereinbarungen zu kontrollieren.

6.5.5 Fragebogen über Berufsalltag bei einer Bremer Kaffeefirma

Eine Gewerkschaft hat vor dem Werkstor einen Fragebogen „Umfrage 1987 — Wie sieht Ihr beruflicher Alltag aus?" an die Mitarbeiter einer großen Bremer Kaffeefirma verteilt.

Der Betriebsrat dieser Firma bat mich um datenschutzrechtliche Beurteilung des Formulars, mit dem Daten über betriebliche Vorgänge bzw. Arbeitsabläufe erhoben werden sollten. Der Betriebsrat vertrat die Auffassung, daß die Anonymität der Mitarbeiter bei der Erhebung und Verarbeitung dieser Daten nicht gewahrt sei. In dem umfangreichen Fragebogen wurde nach Geschlecht, Alter, Schulabschlüsse und nach Eintrittsdatum in die Firma gefragt. Es sollten weiterhin Angaben über die Arbeitszeit, Gehalt/Lohn, in welchem Organisationsteil tätig, über Urlaub, Pausen, Tätigkeit des Betriebsrates, betriebliches Klima u. a. gemacht werden. Mit dieser Fragebogenaktion erhoffte sich die Gewerkschaft Hilfestellung für die anstehenden Tarifverhandlungen.

Bei einem Gespräch mit der Gewerkschaft wurde mir erklärt, daß die Fragebogen in einer nicht automatisierten Form ausgewertet und zwei Monate nach Ablauf der Aktion vernichtet werden sollen. Man sicherte mir zu, daß über die Vernichtung ein Protokoll erstellt wird. Die Gewerkschaft bestätigte mir inzwischen auf meine Anfrage hin die Vernichtung.

Bei der datenschutzrechtlichen Prüfung des Fragebogens kam ich zu dem Ergebnis, daß der Fragebogen, wenn er vollständig ausgefüllt wird, nicht anonym ist, weil er mit gewissem Zusatzwissen (Kenntnis der Betriebszusammenhänge) personenbeziehbar ist. Ich habe die Gewerkschaft darauf hingewiesen, daß, wenn mehrere Fragebogen eingehen, sie als Sammlung den Dateibegriff nach dem Bundesdatenschutzgesetz erfüllen und als interne Datei gem. § 1 Abs. 2 BDSG zu qualifizieren ist.

Ich habe dem Betriebsrat meine datenschutzrechtliche Bewertung mitgeteilt.

6.5.6 Umgang mit Personaldaten bei einem Berufsbildungswerk

Der Betriebsrat der Bildungseinrichtung hatte sich an mich gewandt und gefragt, ob die Übermittlung einer Liste mit Personaldaten an das Landesamt für Verfassungsschutz zum Zwecke der Überprüfung zulässig sei. Die datenschutzrechtliche Überprüfung beim Landesamt für Verfassungsschutz habe ich unter Pkt. 5.3.1.1 dieses Berichtes ausführlich dargestellt. An dieser Stelle soll geklärt werden, ob es zulässig ist, daß privat-rechtlich organisierte Stellen vollständige Listen über die bei ihnen beschäftigten Personen oder Listen ganzer Belegschaftsgruppen an das Landesamt für Verfassungsschutz weitergeben dürfen.

Der Betriebsrat hatte mir eine Liste zugesandt, in der sämtliche zu dem Zeitpunkt beschäftigte Personen bei der Einrichtung mit Personalnummer, Namen, Vornamen, Geburtsdatum, Abteilung und Eintrittstermin aufgeführt waren.

Da anfangs nicht klar war, ob überhaupt eine entsprechende Liste an das Landesamt für Verfassungsschutz weitergegeben sein konnte, habe ich zunächst bei dem Bildungsträger die Vermutung des Betriebsrates überprüft. Meine Prüfung habe ich dabei auf § 30 BDSG gestützt. Danach habe ich im Einzelfall die Ausführungen des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz (z. B. § 83 Betriebsverfassungsgesetz) zu prüfen.

Die zu prüfende Stelle wollte mir anfangs das Prüfungsrecht versagen, weil es sich um eine Liste handele, also nicht um eine dateimäßige Personaldatenverarbeitung. Ich habe darauf hingewiesen, daß gerade auch dieser Einwand Prüfungsgegenstand sein müsse.

Richtig ist, daß, soweit ich die Datenverarbeitung nach Vorschriften des Bundesdatenschutzgesetzes prüfe, mir das Gesetz nur dann eine Prüfkompetenz einräumt, wenn die Datenverarbeitung in Dateien erfolgt. Allerdings ist dafür nicht erforderlich, daß die Daten gerade erst für den konkreten Fall aus einer Datei entnommen

FFD 12/163

worden sind. Eine Zwischenspeicherung in anderer Form als einer Datei, wie z. B. durch manuelle Übertragung in eine Liste, hebt den Zusammenhang grundsätzlich nicht auf (so auch die ganz herrschende Kommentarmeinung). Dieses Ergebnis ist auch sachgerecht, da ansonsten die einfache Möglichkeit der speichernden Stellen bestände, den Schutz des Bundesdatenschutzgesetzes dadurch zu umgehen, indem man neben der dateimäßigen Datenverarbeitung Akten oder Listen anlegen würde, die dann nicht mehr durch die Vorschriften des Bundesdatenschutzgesetzes geschützt wären. Da die Verarbeitung der Personaldaten bei der zu prüfenden Stelle bereits zum Zeitpunkt des behaupteten Datenschutzverstoßes in automatisierter Form betrieben wurde, konnte ich die Zweifel an meiner Prüfkompetenz bei der zu prüfenden Stelle ausräumen. Im übrigen besteht auch unter den Aufsichtsbehörden nach dem Bundesdatenschutzgesetz in den Ländern Einigkeit darüber, daß, wenn Daten in Dateien als auch in Akten, Listen oder in anderer Weise gespeichert werden, diese insgesamt dem Schutz des Bundesdatenschutzgesetzes unterliegen.

Im Zuge der Besprechung wurde mir erklärt, daß die Geschäftsleitung seinerzeit, also ca. 1979/80, eine Kopie aus dem Personalstammbuch gefertigt habe, diese Kopie für geschäftsinterne Zwecke verwendet habe und im Anschluß daran die Liste in einen verschlossenen Umschlag gesteckt habe, der dann mit den Worten „Vertrauliche Unterlagen der Geschäftsleitung" beschriftet worden sei und in einem Tresor mit doppelter Sicherung deponiert worden sei. Der Tresor sei dann später ausgeräumt und in die Rechnungsabteilung verlegt worden. Wie der betreffende Briefumschlag mit den Personalunterlagen abhanden gekommen sei und wo er verblieben sei, konnte auch der betriebliche Datenschutzbeauftragte der Stelle trotz gründlicher Recherchen nicht mehr aufklären. Auch ein von der Geschäftsleitung in Auftrag gegebenes graphologisches Gutachten konnte die Vorwürfe des Betriebsrats nicht entkräften.

Da ich den Vorwürfen sowohl als Landesbeauftragter für den Datenschutz wie auch als Aufsichtsbehörde nach dem Bundesdatenschutzgesetz nachgehen mußte und dabei nichts unversucht lassen darf, was der Aufklärung dienen kann, habe ich die speichernde Stelle noch einmal gebeten, einen hierfür in Frage kommenden Personenkreis zu befragen.

Die daraufhin an mich gerichtete Frage der speichernden Stelle, ob es ein Aussageverweigerungsrecht in Analogie zur Strafprozeßordnung gäbe, habe ich wie folgt beantwortet: Gemäß § 30 Abs. 2 Satz 2 BDSG kann der Auskunftspflichtige die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder eine der in § 383 Abs. 1 Nrn. 1—3 der Zivilprozeßordnung bezeichneten Angehörigen der Gefahr strafrechtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

Daraufhin hat die Geschäftsleitung der geprüften Stelle 17 Personen befragt. Von diesen 17 Personen haben 16 alle Fragen mit Nichtwissen beantwortet. Eine Person hat die Fragen trotz mehrmaliger Aufforderung durch die Geschäftsleitung nicht beantwortet.

Aufgrund des Prüfungsergebnisses bei der privaten Stelle und meiner Nachforschungen bei dem Landesamt für Verfassungsschutz Bremen mußte ich zu dem Ergebnis kommen, daß eine vollständige Liste des Stammpersonals oder aber wenigstens große Teile daraus an das Landesamt für Verfassungsschutz Bremen zur Überprüfung übermittelt worden sind. In welchem Umfang und auf welchem Wege die Datenweitergabe erfolgte, ließ sich nicht mehr feststellen, ein Zusammenwirken zwischen einer öffentlichen Stelle und der Geschäftsleitung des Bildungsträgers konnte ich jedoch nicht mehr ausschließen.

Rechtlich habe ich den Vorgang wie folgt beurteilt:

Eine Übermittlung personenbezogener Daten an das Landesamt für Verfassungsschutz Bremen stellt einen Verstoß gegen § 24 Abs. 1 BDSG dar, da eine Überprüfung der gesamten Belegschaft oder großer Teile gegen schutzwürdige Belange der Betroffenen verstößt. Eine Übermittlung von Personaldaten an das Landesamt für Verfassungsschutz zu diesem Zwecke ist gesetzlich nicht vorgesehen. Die Datenübermittlung war somit rechtswidrig, auch wenn die Weitergabe mündlich oder in Kopie einer Liste geschehen sein sollte. Die Datenübermittlung an das Landesamt für Verfassungsschutz Bremen verstößt daneben auch gegen die sich aus § 242 BGB ergebenden Pflichten des Arbeitgebers aus dem Arbeitsvertrag zur Geheimhaltung von Personalunterlagen.

FFD 12/163

Dieses Ergebnis habe ich der Geschäftsleitung des Bildungswerks, dem Betriebsrat und den Beschäftigten, die sich an mich gewandt hatten, mitgeteilt.

6.5.7 Gewinnung von Beschäftigtenadressen zur Vorbereitung einer Betriebsratswahl

Die Geschäftsleitung eines Betreuungs- und Erholungswerks hat sich bei mir darüber beschwert, daß nach ihrer Meinung die Angestelltenkammer eine Liste mit Namen bei der ihr beschäftigten Personen im Vorfeld einer Betriebsratswahl an eine Gewerkschaft weitergeleitet habe. Später seien dann die Beschäftigten des Betreuungs- und Erholungswerks von dieser Gewerkschaft angeschrieben worden. Daraufhin hätten sich Beschäftigte bei der Personalstelle des Vereins beschwert und den Vorwurf erhoben, die Geschäftsleitung habe das Adressenmaterial an die Gewerkschaft übermittelt.

Ich habe diesen Vorgang geprüft und dabei die Vermutung, die Angestelltenkammer habe eine Datenübermittlung an die Gewerschaft vorgenommen, nicht bestätigt gefunden. Nach meinen Feststellungen haben einzelne Gewerschaftsmitglieder Adressen von Beschäftigten des Werks an ihre Gewerkschaft weitergeleitet.

Unabhängig davon, daß es sich bei der Weitergabe von Arbeitnehmerdaten durch Beschäftigte an eine Gewerkschaft in diesem Fall nicht um einen Vorgang handelt, der sich nach den Vorschriften des Bundesdatenschutzgesetzes beurteilt, waren die Arbeitnehmer berechtigt, entsprechende Mitteilungen an eine Gewerkschaft zu machen. Nach § 17 Abs. 2 BetrVerfG i. V. m. § 2 BetrVerfG sind drei wahlberechtigte Arbeitnehmer oder eine im Betrieb vertretene Gewerkschaft einladungsberechtigt; wobei nur eine im Betrieb vertretene Gewerkschaft in Betracht kommt. Im Betrieb vertreten ist jede Gewerkschaft, die einen Arbeitnehmer des Betriebes zu ihren Mitgliedern zählt. Dabei ist gleichgültig, ob der Betreffende wahlberechtigt ist oder nicht. Voraussetzung ist lediglich, daß er zur Belegschaft gehört, die vom Betriebsrat repräsentiert wird, also nicht leitender Angestellter ist. Daher ist das von der Gewerkschaft vorgenommene Einladungsschreiben resp. der Aushang rechtmäßig gewesen, da insbesondere auch Beschäftigte des Betreuungs- und Erholungswerks nach Mitteilung der Gewerkschaft Mitglieder eben dieser Gewerkschaft sind.

Ich habe die Geschäftsleitung von meinem Ergebnis in Kenntnis gesetzt.

6.5.8 Bundesweite Mitarbeiterumfrage 1987 bei einem Kreditinstitut

Den Beschäftigten eines Kreditinstitutes im Lande Bremen war gemeinsam von der Geschäftsleitung und des Gesamtbetriebsrates ein Mitarbeiterfragebogen zugesandt worden, in dem die Mitarbeiter aufgefordert wurden, ihre persönliche Meinung zu diversen Fragen abzugeben. Der etwa 20seitige Fragebogen enthielt eine Fülle von Fragen, die mit verschieden intensiv abgestuften Antwortmöglichkeiten verbunden waren. Die Fragebogenaktion soll dazu dienen, Zahlen und Fakten zu liefern, um die Personalabteilung und den Betriebsrat handlungsfähiger und bei wichtigen Entscheidungen weitsichtiger und umsichtiger zu machen. Die Rücksendung der Fragebogen war mit einer Verlosung gekoppelt. Der nicht namentlich gekennzeichnete Fragebogen sollte in ein Kuvert gesteckt werden, die personenbezogenen Daten der Teilnehmer auf eine Teilnehmerkarte geschrieben werden und die Teilnehmerkarte mit dem Kuvert in einen Antwortumschlag gesteckt werden. Den Teilnehmern wurde versichert, daß zur Wahrung der absoluten Geheimhaltung der Betriebsrat die Einsendungen auseinander sortieren werde. Die Auswertung der Fragebögen selbst soll von einer externen EDV-Firma übernommen werden.

In einem Teil der Fragen, den sogenannten statistischen Angaben, wurde nach dem Geschlecht, dem Alter, der Dauer der Anstellung bei dem Kreditinstitut, dem Firmenbereich, der Tarifgruppe und anderen beschäftigungsrelevanten Daten gefragt. Der örtliche Betriebsrat hatte sich an mich gewandt und um eine datenschutzrechtliche Stellungnahme gebeten.

Ich habe dazu erklärt, daß das oben beschriebene Verfahren zwar anonym wirkt und bei Einhaltung der beschriebenen Verfahren möglicherweise auch eine Reidentifizierung einzelner Mitarbeiter ausgeschlossen sein könnte, in vielen Fällen aber eine eindeutige Zuordnung zu einem Mitarbeiter aufgrund der o. a. Angaben im Statistikteil nicht ausgeschlossen sein könne. Inwieweit das Verfahren an sich anonym ist, hängt weitestgehend auch von anderen Faktoren wie Anzahl der Teilnehmer und dem EDV-mäßigen Auswertungsverfahren der Fragebögen ab. Die

Auswertungsprogramme und die dahinterstehenden Fragestellungen sind entscheidend für die Möglichkeit und den Grad der Deanonymisierung.

Da die statistischen Angaben in engem Zusammenhang zu den übrigen Antworten des Fragebogens stehen, habe ich empfohlen, in Zukunft diesen Teil von den übrigen Fragen abzutrennen und in verschiedenen Umschlägen direkt an die Erfassungsstelle zu schicken.

Da die Auswertungsziele nur sehr vage angesprochen wurden, wie z. B. Arbeitsunzufriedenheit, Handlungsfähigkeit, weitsichtige und umsichtige Entscheidungsmöglichkeiten, kann das Datenmaterial quasi in alle Richtungen ausgewertet werden. Da die Teilnahme allerdings freiwillig erscheint, wäre dies unter datenschutzrechtlichen Gesichtspunkten nicht zu beanstanden. Besser wäre es allerdings gewesen, den Teilnehmern das Auswertungskonzept bekannt zu geben, damit nicht nur der lockenden Gewinnchance gefolgt wird, sondern auch die Datenverarbeitung in einen Einwilligungskonsens sich niederschlägt.

Da die Auswertung der Fragebogen nicht im Lande Bremen erfolgen sollte, habe ich dem Betriebsrat anheimgestellt, sich insoweit an die zuständige Aufsichtsbehörde zu wenden.

6.6 Mieterdatenschutz

Mietinteressentenfragebogen

Ich wurde aufgefordert zu prüfen, ob es datenschutzrechtlich zulässig ist, daß bei Mietbewerbungen um Sozialwohnungen den Interessenten umfangreiche Fragebogen vorgelegt werden, in denen sie aufgefordert werden, ihre persönlichen Verhältnisse offenzulegen. Es wurden sogar Fälle bekannt, in denen gefordert wurde, eine unterschriebene Erklärung des bisherigen Vermieters vorzulegen, in der dieser bestätigt, daß es sich um einen „ordentlichen und pünktlichen Mieter" handelt. Gefordert werden ferner Angaben zur Staatsangehörigkeit, Geburtsdaten des Mieters und der mit einziehenden Personen, zum Arbeitgeber und pauschale Lohn- und Gehaltsabtretungserklärungen und Fremdbürgschaften.

Bei meiner Überprüfung der Eingabe habe ich festgestellt, daß die Interessentenfragebogen in der Regel Bestandteil der Mieterakte bei den vermietenden Unternehmen wird und nicht dateimäßig geführt wird. Soweit die Mietinteressentenfragebogen jedoch in Dateien geführt werden, sind sie nicht zur Übermittlung bestimmt und somit sind lediglich die Regelungen für interne Dateien (§ 1 Abs. 2 Satz 3 BDSG) anwendbar. Danach sind nur Vorkehrungen zur Datensicherung nach § 6 BDSG zu treffen. Inhaltliche Kriterien, in welchem Umfang rechtlich zulässig Daten von Mietern gespeichert werden dürfen, ergeben sich daraus nicht.

Wegen der generellen Problematik hatte ich mich an die anderen Obersten Aufsichtsbehörden für den Datenschutz in den Ländern gewandt. Bei der Besprechung im Düsseldorfer Kreis wurde deutlich, daß auch in den anderen Ländern entsprechende Probleme bei Mietinteressentenfragebogen anstehen.

Die Ländervertreter im Düsseldorfer Kreis stimmten darin überein, daß es sich grundsätzlich um Datenverarbeitung im Rahmen der Zweckbestimmung eines vertragsähnlichen Vertrauensverhältnisses (§ 23 2. Alternative BDSG) handelt und daß sich der Rahmen der Zulässigkeit dieser Datenverarbeitung aus dem Vertragsrecht (BGB, AGB) und insbesondere dem Mietvertragsrecht ergibt.

Datenschutz zugunsten der Mieter ist bei der beschriebenen Form der Datenverarbeitung nach den Vorschriften des geltenden Bundesdatenschutzgesetzes nicht möglich.

6.7 Sonstige Fälle aus dem nicht-öffentlichen Bereich

Besucherkontrolle bei Firmen

Eine Reihe von Beschwerden hatte ich zusammengefaßt und zum Anlaß genommen, eine Datenschutzprüfung bei einem Luft- und Raumfahrtunternehmen im Lande Bremen durchzuführen. Von diesen Fällen, die sich im übrigen einvernehmlich klären ließen, möchte ich nur über den folgenden berichten. Ein Berufskraftfahrer erklärte mir, daß bei der Firma vom Werkschutz Name, Anschrift und Personalausweis verlangt wurden. Auf seine Frage, was mit seinen Daten gemacht würde, sei ihm lediglich erklärt worden, diese würden gespeichert. Da ihm die Antwort des Werkschutzes nicht ausreichte, hat er sich an mich gewandt und um datenschutzrechtliche Prüfung gebeten.

Ich habe bei meiner Prüfung festgestellt, daß die Firma vom Besucher den Personalausweis vor Betreten des Werksgeländes verlangte. Dem Besucher wird ein Besucherausweis und eine sichtbar zu tragende Ausweiskarte ausgehändigt. Der Besucherausweis muß von dem Besuchten mit Ankunfts- und Abgangsuhrzeiten versehen und abgezeichnet werden. Bei Verlassen des Werkgeländes wird dem Besucher gegen Rückgabe des Ausweisformulars und der Ausweiskarte der Personalausweis wieder ausgehändigt. Die Besucherausweise werden chronologisch abgelegt und gesammelt.

Meine Prüfung der Aufbewahrung der Besucherausweise ergab, daß die technisch und organisatorischen Datenschutzmaßnahmen ausreichend waren. Bei der Einsichtnahme stellte ich allerdings fest, daß früher die Personalausweise mit Lichtbild komplett abgelichtet worden waren. Mir wurde erklärt, daß bis 1984 eine Kopie des Personalausweises zum Besucherausweis genommen worden sei. Danach habe man dieses Verfahren — wie ich zu Recht bestätigen kann — aus datenschutzrechtlichen Überlegungen geändert und nur noch folgende Daten erhoben: Name, Anschrift, Firma, gewünschter Gesprächspartner und Personalausweisnummer.

Alle Daten werden nach den Angaben der Firma nicht automatisiert verarbeitet, sondern lediglich abgelegt und z. B. für evtl. Spionagefälle aufbewahrt. Die Prüfung ergab allerdings, daß die Sammlung der Besucherausweise mehrere Jahrgänge umfaßte. Ob eine so lange Aufbewahrungsdauer erforderlich ist, habe ich bezweifelt. Ich habe daher angeregt, die Frage der Aufbewahrungsdauer der Besucherausweise gelegentlich mit den öffentlichen Auftraggebern, die der Firma diese Auflage erteilt haben, zu besprechen. Da das Verfahren sicherstellt, daß in jeden Zeitpunkt beim Pförtner festgestellt werden kann, welcher Besucher sich auf dem Werksgelände befindet, habe ich angeregt, daß anstelle des Personalausweises dem Besucher ermöglicht werden solle, auch ein anderes Pfand zu hinterlegen.

Das Unternehmen hat mir daraufhin erklärt, es möchte diese Vorgehensweise mit den Personalausweisen generell weiter praktizieren, sollte in Zukunft jedoch ein Besucher — an dessen Besuch das Unternehmen stark interessiert sei — sich weigern, seinen Personalausweis am Tor zu hinterlegen, sei man bereit, ein anderes Pfand zu akzeptieren, welches sicherstellt, daß der Besucher sich beim Verlassen des Werks am Empfang ordnungsgemäß abmeldet. Die Frage der Aufbewahrungsfrist der Besucherausweise sei von dem zentralen Sicherheitsbereich nochmals mit dem öffentlichen Auftraggeber abgestimmt worden. Das Bundeswirtschaftsministerium (BMWI) bestehe weiterhin auf eine 10jährige Aufbewahrungszeit.

Da sich die Funktion des Besucherausweises durch die Rückgabe beim Pförtner erledigt, denn damit ist sichergestellt, daß der Besucher das Werksgelände wieder verlassen hat, halte ich allenfalls eine Aufbewahrungsfrist von drei Jahren für hinnehmbar. Da ich aber von dem Unternehmen nicht verlangen kann, gegen die Auflagen des BMWI zu verstoßen, habe ich mich an den Bundesbeauftragten für den Datenschutz gewandt und ihn gebeten, sich in meinem Sinne mit dem BMWI in Verbindung zu setzen.

6.8 Ordnungswidrigkeiten

In meinem 9. Jahresbericht unter Pkt. 6.11 hatte ich über ein Reiseunternehmen berichtet, daß nebenbei einen Adreßhandel betrieb. Das Unternehmen hatte Werbe- und Verkaufsveranstaltungen organisiert und die Anschriften von mehreren tausend Veranstaltungsteilnehmern verschiedenen Hilfsorganisationen zum Kauf angeboten.

Aufgrund verschiedener Beschwerden habe ich das Unternehmen einer datenschutzrechtlichen Prüfung unterzogen. Das Unternehmen habe ich auf die Registermeldepflicht nach § 39 BDSG hingewiesen; es kam der Registermeldepflicht jedoch nicht nach.

Bei einer Überprüfung in den Geschäftsräumen des Unternehmens hat der Geschäftsführer meinen Mitarbeitern unvollständige Auskünfte über den Adreßhandel und die Herkunft und Lagerung der angebotenen Adressen gegeben und ihnen unter Androhung von Gewalt das Betreten zu seinen Geschäftsräumen verwehrt.

Dies stellte einen Verstoß gegen § 30 Abs. 2 und 3 i. V. m. § 40 Abs. 1 BDSG dar.

Ich habe daher ein Ordnungswidrigkeitsverfahren gegen den Geschäftsführer eingeleitet und wegen des krassen Datenschutzverstoßes ein Bußgeld über DM 5000,—

verhängt. Der dagegen eingelegte Einspruch wurde inzwischen zurückgenommen. Drei andere Ordnungswidrigkeitenverfahren habe ich nach Anhörung und Belehrung wegen Geringfügigkeit eingestellt.

Dabei habe ich festgestellt, daß zum einen Rechtsunsicherheiten über die Auslegung der Meldepflichtvorschriften bei Änderung der Rechtsform des Unternehmens bestehen. Zum anderen bestehen Unklarheiten bei Namensänderung, inwieweit diese gemäß § 39 BDSG mitzuteilen sind.

Mit dieser Mitteilung soll gewährleistet werden, daß die verarbeitenden Stellen identifiziert werden und verarbeitete Daten zugeordnet werden können.

Soweit diese Vorschriften von den Verantwortlichen der Unternehmen nicht in genügendem Maße entsprochen wurden, habe ich in der Regel leichte Fahrlässigkeit mit einem derartig geringen Verschulden angenommen, daß ich von der Verfolgung einer Ordnungswidrigkeit abgesehen habe.

Diese Unternehmen habe ich regelmäßig darauf aufmerksam gemacht, daß es sinnvoll ist, sich an mich als Aufsichtsbehörde zu wenden, wenn der geringste Anlaß zur Vermutung besteht, daß evtl. eine Änderung der Registermeldung vorzunehmen ist.

7. Forderungen aus früheren Jahresberichten

Ich habe zuletzt im 5. Jahresbericht unter Stand und Perspektive des Datenschutzes (Pkt. 8 vom 31. März 1983) eine Zusammenstellung, wie die Empfehlungen des Landesbeauftragten in seinen Jahresberichten durch Senat und Datenschutzausschuß behandelt wurden, veröffentlicht. Stand und Perspektive des Datenschutzes stellen sich erst recht nach einem Zeitraum von 10 Jahren Datenschutztätigkeit im Lande Bremen. Ich habe dies deshalb zum Anlaß genommen, erneut in Form einer Bilanz Forderungen aus meinen früheren Jahresberichten, die bisher noch nicht zufriedenstellend bearbeitet wurden, aufzugreifen. Bei den nachfolgend aufgelisteten 32 Einzelpunkten handelt es sich um Forderungen, die sich an den Bund, das Land als Gesetzgebungsorgane wie an die Verwaltung richten. Mehrere der dort genannten Punkte befinden sich bereits seit Jahren in der Diskussion, ohne daß inzwischen eine den Datenschutz zufriedenstellende Entscheidung getroffen wurde. Bei wiederum anderen Punkten ist darauf hinzuweisen, daß eine gründliche Diskussion und umfangreiche Erörterung mit Experten und Sachverständigen für die beste Lösung erforderlich ist. So erklärt sich manche Zeitverzögerung aus der Sache, viele Zeitverzögerungen sind jedoch inzwischen unverständlich. Insgesamt erinnere ich daran, daß das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung aus dem Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG hergeleitet hat und den Eingriff an strenge Voraussetzungen bindet.

1. Bereits mehrfach (zuletzt 9. Jahresbericht unter Pkt. 5.2.1.1) haben die Datenschutzbeauftragten des Bundes und der Länder auf die Schaffung von gesetzlichen Regelungen für die Verarbeitung von personenbezogenen Daten beim Militärischen Abschirmdienst und beim Bundesamt für Verfassungsschutz hingewiesen.

2. Hinsichtlich der von mir geforderten (9. Jahresbericht unter Pkt. 5.2.6.1) Schaffung einer gesetzlichen Regelung der Datenverarbeitung beim Ausländerzentralregister und Anpassung der das Ausländerrecht regelnden Rechtsvorschriften ist der Bundesgesetzgeber noch nicht tätig geworden.

3. Bereits in meinem 6. Jahresbericht unter Pkt. 5.3.2.3 habe ich die Anpassung der Zweckbestimmung des Melderegisters und der Übermittlungsregelungen an das Volkszählungsurteil im Bremischen Meldegesetz gefordert; sie ist jedoch vom Landesgesetzgeber nicht aufgenommen worden.

4. Die von mir im 8. Jahresbericht unter Pkt. 5.2.2.1 geforderte Anpassung des automatisierten Melderegisters an das neue Melderecht (DEMOS-Entwicklung in Bremen) ist immer noch nicht vorgenommen worden, obwohl die Übergangsfristen dafür bereits Ende 1987 abgelaufen sind.

5. Ich habe gegenüber dem Senator für Inneres dargelegt, daß die Auswertung des Melderegisters zur Feststellung des Müllgefäßvolumens auf keiner verfassungsgemäßen Rechtsgrundlage beruht (8. Jahresbericht unter Pkt. 5.2.2.1). Der Senator für Inneres ist nach wie vor nicht bereit, sich meiner Rechtsauffassung anzuschließen.

FFD 12/1163

6. Bereits in meinem 7. Jahresbericht unter Pkt. 5.2.1.3 habe ich die Anpassung des Personenstandsgesetzes an das Volkszählungsurteil des Bundesverfassungsgerichts gefordert. Inzwischen liegt ein erster Entwurf des Bundesministers des Innern vor.

7. Die Novellierung des Gesetzes über die Statistik der Bevölkerungsbewegung und des Bevölkerungsstandes im Sinne des Volkszählungsurteils (7. Jahresbericht unter Pkt. 5.2.1.1) steht noch aus.

8. Ebenso hat der Landesgesetzgeber die von mir geforderte (8. Jahresbericht unter Pkt. 5.2.4.2) Novellierung des Landesstatistikgesetzes immer noch nicht vorgenommen.

9. Auch das Hochschulstatistikgesetz des Bundes (8. Jahresbericht unter Pkt. 5.2.4.5) steht noch aus.

10. In meinem 9. Jahresbericht habe ich unter Pkt. 5.2.2.2 dargelegt, daß zur Ausführung des Paßgesetzes noch kein Gesetzentwurf des Senators für Inneres vorliegt. Auch in der Zwischenzeit hat sich kein neuer Sachverhalt ergeben.

11. Die Anpassung des KOKIS-/FAZID-Verfahrens an die neue Fahrzeugregisterverordnung steht noch aus (8. Jahresbericht unter Pkt. 5.2.3.1).

12. In meinem 7. Jahresbericht habe ich unter Pkt. 2.1 (6. Spiegelstrich) die Notwendigkeit eines Zeugnisverweigerungsrechts für Datenschutzbeauftragte herausgestellt und unterstrichen, daß hierzu der Landesbeauftragte für den Datenschutz oberste Landesbehörde im Sinne von § 96 StPO sein müßte, um dem Zeugnisverweigerungsrecht Rechnung zu tragen. Der Landesgesetzgeber hat bei der Novellierung des Bremischen Datenschutzgesetzes meine Anregung nicht übernommen.

13. Wie bereits mehrfach gefordert (8. Jahresbericht unter Pkt. 2.1.3) hat der Bundesminister des Innern erneut einen Entwurf zur Novellierung des Bundesdatenschutzgesetzes vorgelegt, der jedoch bei weitem nicht die Anforderungen des Volkszählungsurteils erfüllt. Es werden also weitere intensive Beratungen erforderlich sein.

14. Nachdem bereits mehrfach die Schaffung gesetzlicher Regelungen der Informationspflichten von Gerichten und Staatsanwälten gefordert wurde (zuletzt 9. Jahresbericht unter Pkt. 5.3.1.4), hat der Bundesminister der Justiz den Entwurf eines Justizmitteilungsgesetzes vorgelegt.

15. Auch im Strafverfahren haben die Datenschutzbeauftragten des Bundes und der Länder mehrfach Informationsverarbeitungsregelungen gefordert (9. Jahresbericht unter Pkt. 5.3.1.6); es liegen inzwischen Entwürfe vor.

16. Der Bundesminister der Justiz hat der Forderung nach Datenschutzregelungen im Strafvollzug (8. Jahresbericht unter Pkt. 5.3.1.4) lediglich insoweit Rechnung getragen, als er einen ersten Referentenentwurf vorgelegt hat.

17. Auch für das Schuldnerverzeichnis nach § 915 Zivilprozeßordnung (ZPO) sind immer noch keine gesetzlichen Datenschutzregelungen getroffen worden (9. Jahresbericht unter Pkt. 5.3.1.5).

18. Das gleiche gilt hinsichtlich der Änderung der Vorschriften über die öffentliche Bekanntmachung der Entmündigung gem. § 687 ZPO (siehe auch 9. Jahresbericht unter Pkt. 5.3.1.8).

19. Die von mir geforderten bereichsspezifischen Datenschutzregelungen im Privatschulgesetz des Landes Bremen (6. Jahresbericht unter Pkt. 5.5.2.1) sind vom Senator für Bildung, Wissenschaft und Kunst noch nicht vorgenommen worden.

20. Das gleiche gilt hinsichtlich des Bremischen Weiterbildungsgesetzes (9. Jahresbericht unter Pkt. 5.4.2).

21. Die Anpassung der datenschutzrelevanten Vorschriften des Berufsbildungsgesetzes, insbesondere hinsichtlich der Verarbeitung personenbezogener Daten durch die Prüfungsausschüsse, ist durch den Bundesgesetzgeber bisher nicht erfolgt (9. Jahresbericht unter Pkt. 5.10.1).

22. Obwohl der Senat meine Auffassung hinsichtlich der Notwendigkeit eines Bremischen Archivgesetzes teilt, ist vom Senator für Bildung, Wissenschaft und Kunst immer noch kein entsprechender Entwurf vorgelegt worden, der die

Anforderungen des Bundesverfassungsgerichts in seinem Volkszählungsurteil einbezieht (8. Jahresbericht unter Pkt. 5.4.1.2).

23. Die dringend notwendige Regelung bereichsspezifischen Arbeitnehmerdatenschutzes ist vom Bundesgesetzgeber — auch im neuesten Entwurf eines Bundesdatenschutzgesetzes — nicht aufgegriffen worden (8. Jahresbericht unter Pkt. 5.5.1.2).

24. Das Dialogsystem „Programmierte Sozialhilfe" (PROSOZ) befindet sich noch in der Testphase. An der Entwicklung eines Datenschutzkonzeptes bin ich beteiligt (9. Jahresbericht unter Pkt. 5.5.1.2); siehe auch unter Pkt. 5.6.1 dieses Berichts.

25. Hinsichtlich der von mir geforderten Schaffung von bereichsspezifischen Datenschutzregelungen im Krankenhaus (9. Jahresbericht unter Pkt. 5.6.1.1) hat der Senator für Gesundheit nunmehr einen ersten Referentenentwurf vorgelegt; siehe auch unter Pkt. 5.7.4 dieses Berichts.

26. Im Bereich der medizinischen Dokumentation und statistischen Auswertungen (MEDUSA-K) sind meine Anregungen noch nicht verwirklicht worden (9. Jahresbericht unter Pkt. 5.6.1.2).

27. Im Zusammenhang mit der Behandlung von Bedenken und Anregungen bei der Bauleitplanung durch die Stadtbürgerschaft habe ich angeregt, die personenbezogenen Daten von Einwendern in den Mitteilungen des Senats so zu verschlüsseln, daß sie nicht als Bürgerschaftsdrucksache der Öffentlichkeit zugänglich gemacht werden (8. Jahresbericht unter Pkt. 5.9.1.1); meinen Anregungen hat der Senator für Umwelt und Stadtentwicklung noch nicht Rechnung getragen.

28. Die Erteilung von Auskünften aus dem Gewerbemelderegister an nicht-öffentliche Stellen (z. B. an Auskunfteien) erfolgt ohne Rechtsgrundlage. Ich habe wiederholt die Anpassung der datenschutzrelevanten Vorschriften des Gewerberechts durch den Bundesgesetzgeber gefordert (9. Jahresbericht unter Pkt. 5.8.1.2).

29. Um datenschutzrechtliche Probleme bereits bei der Entwicklung von Datenverarbeitungs- und Nachrichtenübertragungstechniken zu berücksichtigen, habe ich eine enge Kooperation zwischen der für die Vergabe staatlicher Förderungsmittel zu deren Entwicklung zuständigen Stelle und mir angeregt (8. Jahresbericht unter Pkt. 5.10.1.1). Der Senator für Wirtschaft, Technologie und Außenhandel hat meine Anregung noch nicht aufgegriffen.

30. Für die Festsetzung einer Reihe kommunaler Abgaben (z. B. Müllabfuhrgebühr und Deichbeiträge) werden Besteuerungsgrundlagen von Finanzbehörden an die Stadtgemeinden übermittelt (9. Jahresbericht unter Pkt. 5.9.1.1, 3. Spiegelstrich). Die dafür notwendige Anpassung des § 31 Abgabenordnung (AO) durch den Bundesgesetzgeber ist bisher nicht erfolgt.

31. Der Austausch von Kontrollmitteilungen für die Hundesteuer durch die Gemeinden erfolgt ohne Rechtsgrundlage (9. Jahresbericht unter Pkt. 5.9.1.1, 4. Spiegelstrich). Auch hier bedarf es einer Rechtsgrundlage oder die Mitteilungen sind einzustellen.

32. Die Finanzbehörden verlangen bei der Vorlage ärztlicher Atteste, daß diese eine ärztliche Diagnose enthalten. Ich habe dem Senator für Finanzen gegenüber erklärt, daß ärztliche Diagnosen für Besteuerungszwecke nicht erforderlich sind und deshalb das Verlangen unzulässig ist (8. Jahresbericht unter Pkt. 5.11.1.1, 2. Spiegelstrich). Meine Anregung wurde nicht verwirklicht.

Bremerhaven, den 25. März 1988

Dr. Alfred Büllesbach

Landesbeauftragter für den Datenschutz

FFD.121.163

Anlage 1

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 4./5. Mai 1987 über

Rückmeldung von der Justiz an die Polizei

I.

Die Datenschutzbeauftragten des Bundes und der Länder und die Datenschutzkommission Rheinland-Pfalz haben sich während ihrer Konferenz am 4./5. Mai 1987 mit dem Problem der Information der Polizei durch Staatsanwaltschaften und Gerichte über den Ausgang von Strafverfahren befaßt:

Die von der Polizei geführten Datensammlungen beruhen zu einem großen Teil auf Erkenntnissen, die im Rahmen der polizeilichen Tätigkeit in Strafverfahren anfallen. Diese Erkenntnisse sind vorläufiger Natur. Die tatsächlichen Feststellungen werden im weiteren Verlauf des Verfahrens oft ergänzt oder korrigiert; Staatsanwaltschaft und Gericht können zu einer anderen Bewertung von Strafbarkeit und Verschulden kommen. Polizeiliche Datensammlungen können mehr als sonstige behördliche Datensammlungen das verfassungsrechtlich geschützte Persönlichkeitsrecht der betroffenen Bürger beeinträchtigen; dies gilt vor allem dann, wenn aus kriminalpolizeilichen Sammlungen Erkenntnisse an andere Stellen weitergegeben werden.

Bei Datensammlungen der Polizei muß daher in besonderem Maße darauf geachtet werden, daß nur richtige, im Einzelfall tatsächlich erforderliche Daten für den jeweils zulässigen Zeitraum gespeichert werden. Um dies sicherzustellen, sieht eine Bestimmung der „Mitteilungen in Strafsachen" vor, daß die Staatsanwaltschaft die Polizei über den Ausgang der Strafverfahren unterrichtet. Tatsächlich jedoch erfährt die Polizei in vielen Fällen den Ausgang der Strafverfahren nicht oder nicht vollständig, was zur Folge hat, daß ihre Datensammlungen teilweise unrichtig sind und das Daten nicht gelöscht werden, obwohl die Gründe, die zur Speicherung geführt haben, nicht mehr zutreffen. Dieser Zustand ist für den betroffenen Bürger besonders nach einem für ihn günstigen Verfahrensausgang nicht hinnehmbar. Die Unterrichtung über den Ausgang des Verfahrens ist unabdingbare Voraussetzung dafür, daß die Polizei ihre datenschutzrechtliche Pflicht zur Löschung oder Berichtigung erfüllen kann.

II.

In jedem Einzelfall hat deshalb eine Unterrichtung der Polizei zu erfolgen, die sicherstellt, daß sie die zur Aktualisierung ihrer Datensammlungen unerläßlichen Informationen erhält. Hierbei sind insbesondere folgende Grundsätze zu beachten:

— Bei Verurteilungen sind Straftatbestand und Strafmaß mitzuteilen.

— Wird der Betroffene freigesprochen, genügt in der Regel die Mitteilung des Urteilstenors. Wurde der Tatverdacht nicht ausgeräumt, benötigt die Polizei ergänzende Informationen, um feststellen zu können, ob zur Erfüllung polizeilicher Aufgaben weiterhin Daten über den Betroffenen zu speichern sind.

— Wird ein Strafverfahren eingestellt, sind die Rechtsgrundlagen für diese Entscheidung, ein etwa bestehendes Verfahrenshindernis oder die Einstellung mangels hinreichenden Tatverdachts mitzuteilen. Wurde der Tatverdacht nicht ausgeräumt, benötigt die Polizei ebenfalls ergänzende Informationen, um feststellen zu können, ob zur Erfüllung polizeilicher Aufgaben weiterhin Daten über den Betroffenen zu speichern sind.

Ist eine Unterrichtung in angemessener Zeit nicht erfolgt, muß sich die Polizei nach dem Ausgang des Verfahrens erkundigen.

III.

Das Recht auf informationelle Selbstbestimmung verlangt eine korrekte Datenspeicherung bei der Polizei ohne Ausnahme. Die Konferenz begrüßt deshalb Bemühungen einiger Justiz- und Innenverwaltungen, durch regelmäßige Übermittlungen von der Staatsanwaltschaft an die Polizei die Voraussetzungen für eine Aktualisierung der polizeilichen Datensammlungen zu schaffen, und drängt auf eine Beschleunigung.

Die Konferenz hält eine ausdrückliche gesetzliche Regelung entweder in dem geplanten Justizmitteilungsgesetz oder in der Strafprozeßordnung für erforderlich.

Ungeachtet dessen ist auch in der Übergangszeit bis zu einer solchen gesetzlichen Regelung eine Unterrichtung der Polizei unerläßlich, wenn sie bei der Nutzung ihrer Datensammlungen nicht Gefahr laufen soll, das informationelle Selbstbestimmungsrecht der Betroffenen zu verletzen.

Anlage 2

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Neukonzeption des Ausländerzentralregisters

I.

Unter Federführung des Bundesministers des Innern wird zur Zeit das bestehende Ausländerzentralregister (AZR) beim Bundesverwaltungsamt mit dem Ziel einer Effizienzsteigerung überarbeitet.

Grundsätzlich ist die beabsichtigte Schaffung einer verfassungsrechtlich notwendigen gesetzlichen Regelung sowohl für die Datenverarbeitung beim Bundesverwaltungsamt als auch für die Kommunikation der Teilnehmer mit dem Ausländerzentralregister zu begrüßen. Schon jetzt stehen den Benutzern weit über 100 Millionen Daten von ca. 10 Millionen Ausländern zur Verfügung. Geplant ist, die Verwendbarkeit des Datenbestandes durch den potentiellen Teilnehmerkreis des AZR zu erhöhen.

Dient das AZR bis jetzt vorwiegend der Aufenthaltsermittlung von Ausländern und der Vorbereitung ausländerrechtlicher Entscheidungen, so sieht die geplante Regelung eine „stärkere Einbindung in das System zum Schutz der inneren Sicherheit" sowie eine verbesserte Nutzung zu statistischen Zwecken vor. So ist die Einstellung des polizeilichen INPOL-Fahndungsbestands in das AZR geplant.

Das Recht auf informationelle Selbstbestimmung steht auch den in der Bundesrepublik Deutschland und Berlin lebenden Angehörigen anderer Staaten zu. Eine Neuregelung muß daher vermeiden, daß besondere Vorschriften für diese Personengruppe zu einer allgemeinen Diskriminierung der Betroffenen als potentielle Rechtsbrecher führen.

II.

Von entscheidender Bedeutung für die datenschutzrechtliche Bewertung des Registers sind die Funktionen, die es erfüllen soll. Außer Frage steht seine Verwendung als Indexregister zum Zweck der Feststellung, ob eine — und wenn ja, welche — Ausländerbehörde Unterlagen über einen bestimmten Ausländer besitzt.

Damit soll das AZR den Zugang zu den eigentlichen Ausländer- und Meldedaten erleichtern; es kann und darf den Rückgriff auf die bei den örtlichen Behörden gesammelten Informationen nicht ersetzen. Allenfalls bei Eilentscheidungen sollten die im Register gespeicherten Daten unmittelbar für Maßnahmen der Verwaltung herangezogen werden. Keinesfalls darf das AZR zu einem bundesweiten zentralen Melderegister für Ausländer werden.

Für nichtöffentliche Stellen und Privatpersonen darf der Zugang zu den Daten des AZR nur in eng begrenzten Ausnahmefällen gewährt werden, die gesetzlich festzulegen sind.

III.

Das Urteil des Bundesverfassungsgerichts zur Volkszählung 1983 ist wesentlicher Anlaß für die gesetzliche Neuregelung. Aus Gründen der Normenklarheit, der Bestimmtheit und der Zweckbindung muß die Regelung das Ausmaß der vorgesehenen Datennutzung abschließend festlegen.

Das Register dient nicht dem Vollzug von Verwaltungsentscheidungen durch die Registerbehörde selbst. Wenn seine Hauptfunktion die Unterstützung der Tätigkeit der Ausländerbehörden und der Polizei ist — soweit diese Stellen ausländer- und allgemeinvollzugspolizeiliche Aufgaben erfüllen —, so muß der Gesetzgeber diesen Verwendungszusammenhang darstellen. Es ist zu begrüßen, daß nicht nur die Verwendung der Daten im Register selbst, sondern auch ihre Anlieferung und Weitergabe an andere Dienststellen gesetzlich geregelt werden sollen. Nur wenn die Datenverarbeitung klar und eindeutig festgelegt ist, kann der Betroffene den Eingriff in sein Recht auf informationelle Selbstbestimmung einschätzen. Allein ein Registergesetz genügt diesen Anforderungen nicht. Eine zeitlich parallele Novellierung des Ausländerrechts ist deshalb unabdingbar. Gleichzeitig muß auch der

Datenaustausch zu Fahndungszwecken und zur Erfüllung anderer polizeilicher Aufgaben in der Strafprozeßordnung und in den Polizeigesetzen geregelt werden.

IV.

Für den in das AZR aufzunehmenden Datensatz sind die vom Register zu erfüllenden Funktionen maßgeblich.

Entsprechend der Indexfunktion gehören in das AZR solche Daten über einen Ausländer, die das Auffinden bestimmter, zu einer Person angelegter Unterlagen zur Vorbereitung vor allem ausländerrechtlicher Entscheidungen ermöglichen.

Darüber hinaus ist geplant, den Benutzern unmittelbar Daten zur Verfügung zu stellen, um verschiedene Informationsansprüche zu erfüllen. Dadurch sollen zum Teil die Empfänger die Möglichkeit erhalten, auf die Beiziehung von Akten vor Entscheidungen zu verzichten.

Besonders problematisch ist die Speicherung und Verwendung des Datums „Einreisebedenken". Unter diesem Datum werden belastende Vorgänge im Umfeld des Ausländers erfaßt, die noch keine ausländerrechtlichen Maßnahmen ausgelöst haben. Damit erhält der Datensatz eine neue Qualität: Gespeichert werden nicht mehr Informationen über in einem formalisierten und rechtsstaatlichen Verfahren ergangene Maßnahmen der Ausländerbehörde, sondern auch unpräzise Angaben über ein vermutetes (Fehl-) Verhalten des Ausländers selbst.

Der Mangel an Genauigkeit dieses Datums bedingt es, daß z. B. ein bei einer Grenzpolizeibehörde beantragter Ausnahmesichtvermerk nicht ohne Hinzuziehung der zugrundeliegenden Akte versagt werden kann. Die Voraussetzungen der Entstehung dieses Datums sowie seiner Verwendung bedürfen wegen des verfassungsrechtlichen Gebots der Normenklarheit einer Präzisierung. Dabei wird nicht verkannt, daß sich diese Regelung in denjenigen Fällen positiv auswirken wird, in denen in diesem Datenfeld keine Eintragung vorliegt, und dies dürfte die große Mehrheit sein. Wenn nämlich das Datum „Einreisebedenken" nicht belegt ist, besteht die Möglichkeit, etwa über einen Ausnahmesichtvermerk in einem beschleunigten Verfahren zu entscheiden, ohne daß auf die Ausgangsunterlagen zurückgegriffen werden muß.

Die geplante Aufnahme von Daten aus dem INPOL-Fahndungsbestand macht die Funktionserweiterung in den Polizeibereich hinein deutlich. Die Notwendigkeit der Aufzeichnung von Fahndungsnotierungen im AZR ist bisher angesichts möglicher Alternativen — z. B. eines regelmäßigen Datenabgleichs — nicht ausreichend dargelegt.

Die Speicherung von Suchvermerken kann hingenommen werden, wenn sie nur für die Verfolgung im Gesetz selbst festgelegter Zwecke erfolgt und — wie im Bericht des Bundesministers des Innern vorgesehen — zeitlich begrenzt zugelassen wird.

Bei den Daten, die ausschließlich für statistische und Planungszwecke erhoben werden sollen, ist sicherzustellen, daß ihre Verwendung getrennt von derjenigen anderer Daten des Ausländers erfolgt und die Angaben derart anonymisiert werden, daß die Verbindung zu den personenbezogenen Daten nicht mehr hergestellt werden kann.

V.

Die Kommunikation zwischen AZR und den verschiedenen Behörden oder Privatpersonen ist gesetzlich so zu regeln, daß sie den Anforderungen des Bundesverfassungsgerichts an den bereichsspezifischen Datenschutz gerecht wird.

Eine gesetzliche Regelung ausschließlich des Teilnehmerkreises und des Datenumfangs wäre nicht ausreichend, solange nicht präzise festgelegt wird, für welche Zwecke die Behörden Daten abrufen dürfen, bzw. das AZR an sie übermitteln darf. Nur eine verwendungorientierte Regelung macht den potentiellen Verwendungszusammenhang transparent und würde den Anforderungen des Bundesverfassungsgerichts genügen.

Eine Festlegung, daß den Benutzern nur solche Daten übermittelt werden, die sie zur Aufgabenerfüllung benötigen, würde nicht ausreichen; es bedarf gerade der Festlegung derjenigen Aufgaben, zu deren Erfüllung Datenübermittlungen vorgenommen werden sollen. Auch eine Differenzierung nach Abfragearten, die jeweils verschiedene, stufenweise gestaffelte Datenmengen umfassen, wäre unge-

FFD 12/163

nügend, solange nicht feststeht, für welche Aufgaben welche Behörden die festgelegten Datenmengen abrufen können.

Der On-line-Zugriff auf die im AZR gespeicherten Daten stellt eine besonders intensive Form des Zugriffs auf personenbezogene Informationen dar. Er bedarf daher der besonderen Rechtfertigung, die in der Aufgabenstellung der beteiligten Behörden begründet sein muß.

Anlage 3

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 4./5. Mai 1987 zum Entwurf einer Fahrzeugregisterverordnung

Zu der von der Bundesregierung dem Bundesrat zugeleiteten Fahrzeugregisterverordnung hat der Innenausschuß des Bundesrates am 29. April 1987 Änderungen vorgeschlagen, die datenschutzrechtlich nicht akzeptiert werden können.
Danach sollen u. a.

— der Umfang der Auswahlprotokollierung zur Feststellung des konkreten Anlasses der Abrufe und der für die Abrufe verantwortlichen Personen von 5 Prozent auf ein Promille der Fälle reduziert werden.

  Für die künftige Praxis bedeutete dies, daß eine systematische Überprüfung des Abfrageverhaltens der abrufberechtigten Dienststellen nicht mehr möglich wäre. Denn nach dem erwarteten Umfang der ZEVIS-Nutzung und der vorgesehenen Zahl der abrufberechtigten Dienststellen würde bei der beabsichtigten Reduzierung durchschnittlich alle zwei Monate nur eine Protokollierung pro Dienststelle erfolgen.

  Außerdem brauchte bei einer solchen Protokollierungspraxis eine abrufende Person mit der Protokollierung gerade ihres Abrufes ernstlich nicht mehr zu rechnen.

— für den großen Bereich der Straftaten und Verkehrsordnungswidrigkeiten eine konkrete Angabe des Anlasses der Abrufe entfallen, wodurch deren Nachprüfbarkeit nicht mehr gewährleistet wird.

Sinn und Zweck des § 36 Abs. 7 des Straßenverkehrsgesetzes ist die Vermeidung oder Unterbindung von Mißbrauch und falscher Rechtsanwendung durch wirksame Kontrolle der Abrufe seitens der Fachaufsicht und der Datenschutzbeauftragten. Die vom Innenausschuß des Bundesrates vorgeschlagenen Änderungen der von der Bundesregierung vorgelegten Fahrzeugregisterverordnung wären daher mit dem Straßenverkehrsgesetz nicht vereinbar. Sie ließen eine wirksame Kontrolle des erstmals durch den Gesetzgeber geregelten automatisierten Abrufverfahrens nicht zu. Damit würde auch die vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellte Forderung nach einer effektiven Datenschutzkontrolle durch unabhängige Datenschutzbeauftragte mißachtet.

Die Datenschutzbeauftragten weisen daher nachdrücklich darauf hin, daß die zu erlassende Fahrzeugregisterverordnung keinen rechtlichen Bestand haben könnte, falls die beabsichtigten Änderungen übernommen würden.

Anlage 4

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. Dezember 1987 zur Speicherung personenbezogener Aids-Daten in polizeilichen Informationssystemen

In zwei gemeinsamen Sitzungen von Arbeitsgruppen der ständigen Konferenz der Innenminister und -senatoren sowie der Datenschutzbeauftragten des Bundes und der Länder wurde das Problem der Speicherung von personenbezogenen Aids-Hinweisen in polizeilichen Informationssystemen erörtert. Nach eingehender Beratung der Ergebnisse dieser Gespräche faßten die Datenschutzbeauftragten des Bundes und der Länder sowie die Datenschutzkommission des Landes Rheinland-Pfalz bei Gegenstimme des Bayerischen Landesbeauftragten für den Datenschutz folgenden Beschluß:

I.

Die Speicherung von HIV-Hinweisen soll die Eigensicherung von Polizeibeamten und evtl. auch den Schutz von Personen in Polizeigewahrsam gewährleisten, die mit HIV-Infizierten in Kontakt kommen. Die Datenschutzbeauftragten verkennen

nicht, daß Polizeibeamte bei der Berufsausübung spezifischen Gefahren ausgesetzt sind und die notwendigen Maßnahmen ergriffen werden müssen. Insbesondere ein direkter Blutkontakt oder eine Verletzung mit infizierten Injektionskanülen bei Kontakten mit Drogenabhängigen stellen eine solche spezifische Gefährdung dar. Dem Anspruch der Polizeibeamten auf einen weitestgehenden Schutz vor einer Infektion, die zu einer tödlichen Erkrankung führen kann, steht der Anspruch der Betroffenen gegenüber, daß Datenspeicherungen nur dann vorgenommen werden, wenn diese geeignet sind, die Gefährdung wirksam zu verringern, und sie dadurch nicht unverhältnismäßig belastet werden. Hierbei ist auch zu berücksichtigen, daß eine automatisierte Speicherung von medizinischen Daten eine schwerwiegende Beeinträchtigung für die Betroffenen darstellt. Ebenso sind auch die gravierenden sozialen Folgen für diesen Personenkreis zu bedenken, wenn die gespeicherten Daten an Dritte gelangen.

II.

Sowohl medizinische Experten als auch Fachleute aus dem Sicherheitsbereich und dem Gesundheitswesen haben wiederholt Zweifel daran geäußert, daß durch die Speicherung von Informationen über HIV-Infizierte in polizeilichen Informationssystemen die Gefährdung von Polizeibeamten abgewendet werden kann. Hierfür werden folgende Gründe vorgebracht: In vielen Situationen, wie z. B. bei der Hilfeleistung für verletzte Unfallopfer, der Festnahme unbekannter Personen oder auch der plötzlichen Konfrontation mit Straftätern oder Störern sei eine vorherige Überprüfung vorhandener Dateibestände ohnehin nicht möglich. Hinzu komme, daß der Polizei immer nur ein sehr geringer Teil der Infizierten bekannt sein werde, so daß die Polizei in jedem Fall und auch ohne besondere Hinweise Schutzmaßnahmen treffen müsse.

Angesichts dieser Zweifel, die von den Datenschutzbeauftragten geteilt werden, kann die Speicherung — wenn überhaupt — nur unter sehr eingeschränkten Voraussetzungen hingenommen werden. Möglich erscheint dies allenfalls für Situationen, in denen es mit hoher Wahrscheinlichkeit zu gewaltsamen Auseinandersetzungen mit infizierten Personen kommt. Keinesfalls darf eine „Aids-Datei" entstehen. Im übrigen wäre mindestens folgendes zu beachten:

1. Die Speicherung von HIV-Hinweisen im Datenfeld der „personengebundenen Hinweise" im bundesweiten Inpol-System und in vergleichbaren Landessystemen muß eingestellt werden, da diese Hinweise bei sämtlichen Abfragen erscheinen.

2. HIV-Hinweise dürfen allenfalls in solche Dateien aufgenommen werden, in denen sie als Grundlage für die Eigensicherung bei polizeilichem Einschreiten tatsächlich in Betracht kommen.

3. Die Speicherung von HIV-Hinweisen aufgrund von Verdächtigungen und ungeprüften Informationen verbietet sich in jedem Fall. Kommt die Information vom Betroffenen selbst, müßte dieser über die Tatsache und die Bedeutung der Speicherung aufgeklärt werden. Im übrigen kommt nur die Speicherung von ärztlich gesicherten Informationen in Betracht, die die Polizei rechtmäßig erlangt hat.

4. Auf die gespeicherten Daten darf nur ein besonders dazu befugter Benutzerkreis zugreifen, und dies nur zu Zwecken der Eigensicherung. Die Weitergabe an andere Stellen ist nur in besonders festzulegenden Fällen zulässig.

5. Es muß in jedem Fall erkennbar sein, wer wann den HIV-Hinweis in das System eingespeichert hat und hierfür verantwortlich ist, da nur so die Speicherungspraxis überprüft werden kann und notwendige Berichtigungen ermöglicht werden.

Anlage 5

Beschluß der Internationalen Konferenz der Datenschutzbeauftragten 1987 zu Datenschutz und Neue Medien

1. Die Internationale Konferenz der Datenschutzbeauftragten beobachtet seit Jahren die Entwicklung der Neuen Medien und die damit verbundenen Probleme des Datenschutzes. Sie hat mit ihren Entschließungen vom 18. Oktober 1983 in Stockholm und vom 26. September 1985 in Luxemburg Forderungen zur Verbesserung des Datenschutzes erhoben.

FFD 121163

2. Der Stand der Massenmedien und Telekommunikation im Jahre 1987 ist durch folgende Merkmale gekennzeichnet:

   — Die verschiedenen für die Telekommunikation genutzten analogen und digitalen Einzelnetze streben nach einer Vereinheitlichung der technischen Normen; zunehmend entstehen einheitliche nationale Infrastrukturen für die Telekommunikationsnetze.

   — Dienste für die Verbreitung von Massenmedien und für andere Telekommunikationsformen verschiedenster Art werden auf diesen Netzen national und international angeboten.

3. Die Internationale Konferenz der Datenschutzbeauftragten ist besorgt über die Sammlung einer zunehmend größeren Anzahl von personenbezogenen Daten durch Massenmedien und Telekommunikationsdienste. Die Risiken sind offensichtlich, die in einer derartigen Kumulation von Daten und deren möglichem Gebrauch zu Zwecken liegen, die nicht mit den Zwecken übereinstimmen, für die sie erhoben wurden. Soweit keine anonymen Nutzungsformen eingeführt werden, ermöglicht die über die ursprünglichen Kommunikationszwecke hinausgehende Verarbeitung derartiger Informationen den Aufbau von Daten über die Lebensführung und Interessen von Einzelindividuen und Familien. Eine solche Entwicklung wird als keineswegs wünschenswert angesehen.

   Die Informationen konzentrieren sich letztlich bei wenigen öffentlichen und privaten Netzbetreibern und Kommunikationsanbietern (Post, Teleports, internationale Serviceunternehmen). Die Risiken des Mißbrauchs, der Sabotage und Spionage sowie der Manipulation bürden diesen Institutionen eine erhebliche Verantwortung auf, ohne daß in den meisten Ländern die nationalen Gesetze hinreichende rechtliche Regelungen hierfür vorsehen.

4. Die Internationale Konferenz der Datenschutzbeauftragten fordert deshalb nachdrücklich die Entwicklung von Regelungswerken auf nationaler und internationaler Ebene. Für die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung sind internationale Normen anzustreben. Die Zusammenarbeit der nationalen Kontrollinstanzen ist zu verbessern.

Druck: Anker-Druck Bremen