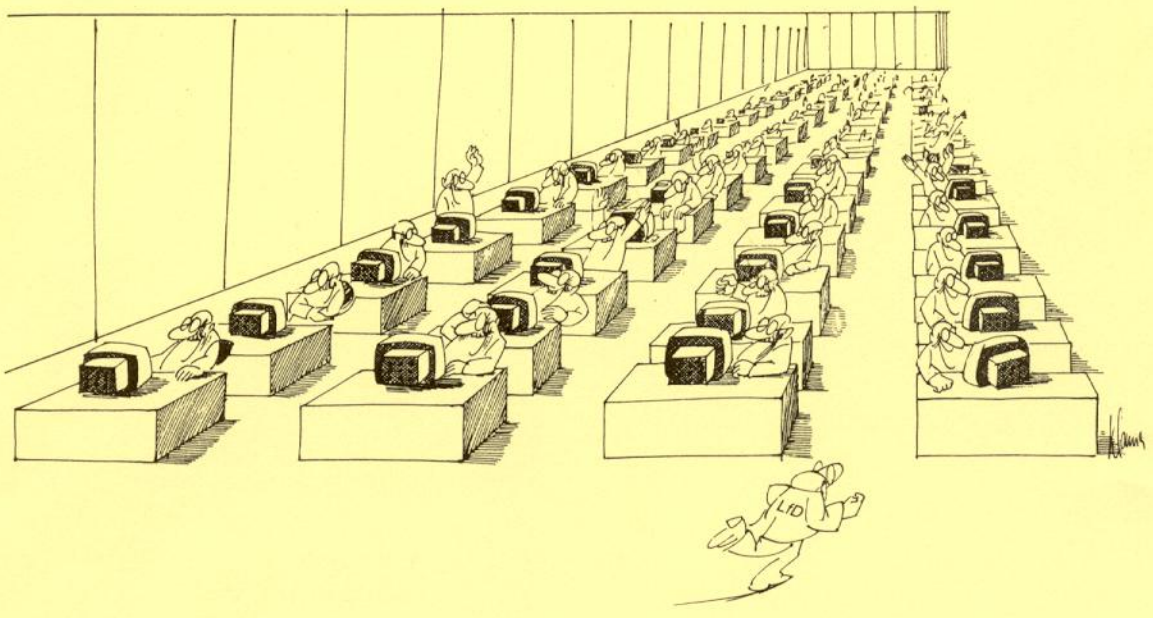
Freie Hansestadt Bremen

Landesbeauftragter für den Datenschutz

13. Jahresbericht



Vorgelegt zum 31. März 1991

BREMISCHE BÜRGERSCHAFT
Landtag
12. Wahlperiode

Drucksache 12/1187

Dreizehnter Jahresbericht des Landesbeauftragten für den Datenschutz

Hiermit erstattet der Landesbeauftragte für den Datenschutz der Bürgerschaft (Landtag), dem Präsidenten des Senats den 13. Bericht über das Ergebnis seiner Tätigkeit im Jahre 1990 zum 31. März 1991 (§ 33 Abs. 1 Bremisches Datenschutzgesetz).

Sven Holst, Vertreter des Landesbeauftragten für den Datenschutz

Inhaltsübersicht Seite

6. Anlagen

1. Überblick über das Berichtsjahr

1.1 Einleitung

Der Datenschutz steht für einen wichtigen Teil unserer freiheitlichen Ordnung, die Datenschutzkontrolle soll dazu beitragen, das Grundrecht auf freie Entfaltung der Persönlichkeit zu schützen. Der Datenschutz wird von der Erkenntnis getragen, daß der Bürger eine vom Staat und auch von anderen Menschen zu respektierende Privatssphäre braucht und der Einzelne grundsätzlich selbst entscheiden können soll, welche Informationen über ihn selbst andere besitzen sollen.

Mehr und mehr erkennen die Veranwortlichen in Politik und Wirtschaft, daß der Bürger verlangt, Datenschutz zum selbstverständlichen Bestandteil jeglicher Datenverarbeitung zu machen. Die Bürger wenden sich mittlerweile sehr selbstbewußt an den Landesbeauftragten für den Datenschutz und begreifen die Kontrolle durch den Datenschutzbeauftragten als eine ihnen selbstverständlich zustehende Rechtsausübung. Lange schon geht es nicht mehr bloß um die Überprüfung eklatanter Verstöße gegen Persönlichkeitsrechte der Betroffenen, sondern man betrachtet den Landesbeauftragten für den Datenschutz als Garantieinstitution dafür, daß eine rechtmäßige und ordnungsgemäße Datenverarbeitung stattfindet.

1.2 Eingaben von Bürgerinnen und Bürgern und datenschutzrechtliche Kontrollen

Das Datenschutzengagement der Bürgerinnen und Bürger ist immer ein guter Indikator dafür, welchen Stellenwert der Datenschutz in der Bevölkerung einnimmt und führt immer wieder in Bereiche mit datenschutzrechtlichen Defiziten. Einmal den Verfassungsschutz und die Nachrichtendienste im öffentlichen und die Auskunfteien im privaten Bereich ausgenommen, wenden sich die meisten Bürgerinnen und Bürger erst an mich, nachdem bereits eine Auseinandersetzung über die Datenschutzfragen mit der speichernden Stelle stattgefunden hat. Die Anfragen und Eingaben bezogen sich auf fast alle Bereiche der öffentlichen Verwaltung, eine auch nur globale Darstellung aller Eingaben würde den Bericht sprengen.

Daneben führe ich systematische Datenschutzprüfungen und Kontrollen auf der Grundlage vorher erarbeiteter Prüfkonzepte durch. Auch die Prüfergebnisse aus dieser Tätigkeit werden im Jahresbericht nur dargestellt, soweit gravierende Mängel bei der Datenverarbeitung festgestellt wurden oder strukturelle Probleme markiert werden sollen, die auch auf andere speichernde Stellen übertragbar sind.

Es ist nicht zu verkennen, daß in einigen senatorischen Bereichen bei der Behandlung des 12. Jahresberichts im Datenschutzausschuß ein Nachgeben und eine Änderung der Einstellung zur Datenschutzkontrolle stattgefunden hat. Gleichwohl kommt es trotz des klaren Wortlauts von § 27 BrDSG immer wieder vor, daß mir vor oder bei Prüfungen der Zugang zu Daten und Informationen streitig gemacht wird; in diesem Zusammenhang möchte ich alle speichernden Stellen auf die grundsätzlichen Ausführungen des Senators für Justiz und Verfassung (vgl. Pkt. 2.3.2 des Berichts) hinweisen.

1.3 Datenschutz und Parlament

Datenschutzrechtliche Fragen aus dem parlamentarischen Raum sind immer mit besonderer Behutsamkeit zu behandeln, stehen doch häufig Fragen des Informationszugangs und -umfangs der Bürgerschaft und Fragen der öffentlichen Behandlung im Vordergrund. Fragen also, die durchaus mit dem Recht auf informationelle Selbstbestimmung und dem Datenschutz kollidieren. Häufig bedarf es daher einer Einzelfallabwägung, um den widerstreitenden Interessen möglichst weitgehend Rechnung zu tragen.

So habe ich den Senat in seiner Entscheidung bestärkt, auf eine parlamentarische Anfrage hin nicht die Namen der vom Senat beauftragten Gutachter in der Drucksache mit zu veröffentlichen, sondern nur zur Einsicht für die Abgeordneten bereit zu halten. Auch im Zuge der Einsetzung des Untersuchungsausschusses „Hans-Wendt-Stiftung" standen datenschutzrechtliche Fragen an, so habe ich den Rechnungshof bei der Frage beraten, ob, in welchem Umfang und wem der Prüfbericht zugänglich gemacht werden darf.

Immer wieder werden auch Fragen von einzelnen Abgeordneten und Deputierten an mich herangetragen, denen von der Verwaltung die Akteneinsicht oder Auskünfte verweigert werden. Das Deputationsgesetz gibt hinreichend Auskunft

über Anspruch und Verfahren; das Auskunftsbegehren eines Fraktionsbüros reicht keinesfalls aus. Zu berücksichtigen ist in diesem Zusammenhang, daß Deputationen nach § 1 Abs. 3 Satz 2 des Deputationsgesetzes über Angelegenheiten ihres Verwaltungszweiges zu beraten haben. Dies wird oft nicht ohne Kenntnisnahme von personenbezogenen Daten möglich sein. Das Deputationsgesetz setzt also zwingend voraus, daß die Deputierten personenbezogene Daten zur Kenntnis nehmen. Die damit verbundenen Eingriffe in Persönlichkeitsrechte der Betroffenen müssen sich aber auf das nach Art und Umfang der Datenverarbeitung erforderliche Maß beschränken. Das mildeste Mittel ist auszuwählen. In diesem Zusammenhang bietet es sich an, auf Deputationsvorlagen, die sensible personenbezogene oder personenbeziehbare Daten enthalten, generell die Regeln anzuwenden, nach denen mit Personalvorlagen, etwa betreffend Stellenhebungen, verfahren wird. Diese Vorlagen werden nur den Deputationsmitgliedern zugesandt, nur diese und die für die jeweilige gesetzliche Aufgabe zuständigen Mitarbeiter/innen der Verwaltung sind bei der Behandlung dieses Tagesordnungspunktes anwesend, und die Deputationsmitglieder werden zur vertraulichen Behandlung der Unterlagen und des Inhalts der Beratungen verpflichtet.

Die Fraktionen der SPD und CDU haben mich Anfang bzw. Mitte Oktober im Rahmen der Beratung ihrer Gesetzentwürfe zur Weiterentwicklung des Petitionsrechts um datenschutzrechtliche Beratung gebeten.

Ich habe darauf hingewiesen, daß der Petitionsausschuß ein parlamentarischer Ausschuß ist, für den — anders als für die Deputationen — das Bremische Datenschutzgesetz (BrDSG) wegen der Regelung in § 1 Abs. 2 BrDSG keine unmittelbare Anwendung findet. Gleichwohl müssen die Bremische Bürgerschaft wie auch der Petitionsausschuß das Recht auf informationelle Selbstbestimmung beachten. Deshalb ist es auch erforderlich, in das Petitionsgesetz bereichsspezifische Datenschutzregelungen aufzunehmen.

Ich habe darauf hingewiesen, daß zwar das Handeln des Petitionsausschusses häufig von der konkludenten Einwilligung des Petenten bzw. der Petentin umfaßt sein wird. Gleichwohl ist aber nicht auszuschließen, daß der Petitionsausschuß es für notwendig oder richtig erachtet, sich auch an andere Stellen zu wenden. Deshalb habe ich eine Regelung empfohlen, die den Petitionsausschuß ermächtigt, sich zur Bearbeitung der Petitionen an alle im Gesetz genannten Stellen zu wenden. Dabei soll die Regelung den Petitionsausschuß berechtigen, die erforderlichen Angaben gegenüber diesen Stellen zu machen, und ihn berechtigen, um Informationen und Auskünfte nachzusuchen, die für die Behandlung der Petition geeignet und erforderlich erscheinen. Dabei sollte der erklärte oder erkennbare Wille der Petenten beachtet werden.

Zur Wahrung der Vertraulichkeit der im Zuge der Behandlung der Petitionen erlangten Informationen durch die Ausschußmitglieder und die berufsmäßig tätigen Gehilfen habe ich empfohlen, eine Schweigepflicht aufzunehmen, die auch nach Ausscheiden aus dem Petitionsausschuß fortgilt. Schließlich habe ich darauf verwiesen, daß auch das Verfahren der Bekanntgabe der Entscheidung des Petitionsausschusses in seinen Grundzügen gesetzlich zu regeln ist.

Weitere Datenschutzregelungen — z. B. die Frage der Aufbewahrungsfrist nach Abschluß der Petition — habe ich empfohlen, in einer Verfahrensordnung zu treffen.

Schließlich habe ich darauf hingewiesen, daß die öffentlichen Stellen, die gegenüber dem Petitionsausschuß auskunfts- und vorlagepflichtig sind, an die Bestimmungen des § 13 i. V. m. § 12 Abs. 2 Nr. 2 BrDSG (Zweckbindung) gebunden sind. Danach ist eine Zweckänderung nur zulässig, soweit eine Rechtsvorschrift sie erlaubt oder zwingend voraussetzt. Ich habe daher empfohlen, im Petitionsgesetz selbst festzuschreiben, daß von den im Gesetz genannten Stellen an den Petitionsausschuß zur Erfüllung seiner Aufgaben personenbezogene Daten von Petentinnen und Petenten sowie die mit dem jeweiligen Vorgang im Zusammenhang stehenden personenbezogenen Daten Dritter übermittelt werden dürfen.

Die inzwischen in die Bürgerschaft eingebrachten Gesetzentwürfe (BremDrs. 12/1036 und 12/1050) haben wesentliche Teile meiner Anregungen aufgegriffen.

1.4 Datenschutzrechtlich bedeutsame Gesetzgebung und Initiativen

Auch im letzten Jahr sind sowohl vom Landes- als auch vom Bundesgesetzgeber neue bereichsspezifische Datenschutzregelungen für verschiedene Lebens-

bereiche verabschiedet worden. In Bremen hat die Bremische Bürgerschaft das Vermessungs- und Katastergesetz sowie das Gesetz über das Friedhofs- und Bestattungswesen novelliert und hierbei auch normenklare Datenschutzregelungen erlassen. Durch eine Änderung der Bremischen Landesbauordnung wird dem Senator für das Bauwesen auferlegt, in einer Rechtsverordnung nähere Bestimmungen über Art, Umfang und Zweck der Datenverarbeitung im Baugenehmigungsverfahren zu erlassen. Die Änderungsanträge der Fraktion „Die Grünen" und der FDP zum Bremischen Datenschutzgesetz, die im wesentlichen die Stellung und Bestellung des Landesbeauftragten für den Datenschutz betrafen (vgl. Drs. 12/931 und 967 und den Bericht des Datenschutzausschusses dazu, Drs. 12/1086), wurden mit Mehrheit abgelehnt. Aus datenschutzrechtlicher Sicht begleite ich gegenwärtig u. a. die Entwürfe zu einem Bremischen Brandschutzgesetz sowie einem Bremischen Archivgesetz.

Auf Bundesebene ist die Novellierung des Bundesdatenschutzgesetzes hervorzuheben. Das Gesetz trägt zwar den Forderungen der Datenschutzbeauftragten und der Aufsichtsbehörden nicht im vollen Umfange Rechnung, gleichwohl ergeben sich für meine Tätigkeit als Aufsichtsbehörde nach dem BDSG für den privaten Bereich verbesserte Kontrollen und Aufsichtsbefugnisse. Des weiteren hat der Deutsche Bundestag neben dem neuen Ausländergesetz das Hochschulstatistikgesetz sowie das Mikrozensusgesetz novelliert. Außerdem wurden die Aufgaben für den Bundesnachrichtendienst, den Militärischen Abschirmdienst und den Verfassungsschutz und die damit zusammenhängenden Datenverarbeitungen auf eine gesetzliche Grundlage gestellt.

Fast sieben Jahre nach Erlaß des Volkszählungsurteils und nach Ablauf einer weiteren Legislaturperiode des Deutschen Bundestages sind wesentliche Gesetzesvorhaben des Bundes, die erforderliche Datenschutzregelungen für die Tätigkeit der Bundes- und der Landesverwaltungen treffen, immer noch nicht verabschiedet oder verabschiedungsreif. Wichtige Gesetzesvorhaben — wie z. B. die Änderung der Strafprozeßordnung sowie der Grundbuch- und Gewerbeordnung, die Schaffung eines Justizmitteilungsgesetzes sowie eines Gesetzes über das Bundeskriminalamt — sind bedauerlicherweise immer noch nicht abgeschlossen.

1.5 Unterrichtungspflicht über Planungen zum Aufbau automatisierter Informationssysteme

In vielen Jahren hat es Probleme mit der rechtzeitigen Beteiligung des Landesbeauftragten für den Datenschutz bei Gesetzgebungsvorhaben gegeben. Hier scheint sich in letzter Zeit eine Verbesserung abzuzeichnen, in vielen Bereichen gibt es mittlerweile intensive Zusammenarbeitsformen. Mit der Umsetzung der 1987 neu in das Bremische Datenschutzgesetz aufgenommenen Vorschrift des § 27 Abs. 4 BrDSG gibt es seitens der Verwaltung offensichtlich weiterhin Schwierigkeiten. Auch in diesem Berichtsjahr wurde dieser Vorschrift keine ausreichende Beachtung geschenkt. Gem. § 27 Abs. 4 BrDSG ist der Landesbeauftragte für den Datenschutz über Planungen zum Aufbau automatisierter Informationssysteme rechtzeitig zu unterrichten, sofern in den Systemen personenbezogene Daten verarbeitet werden sollen. Nur wenn der Landesbeauftragte für den Datenschutz über die Planung von DV-Verfahren frühzeitig unterrichtet wird, kann er bereits in der Phase der Gestaltung Überlegungen zum Datenschutz einfließen lassen. Der Datenschutzausschuß hat in seinem Bericht und Antrag zu meinem letzten Jahresbericht und der Stellungnahme des Senats festgestellt: „Der Ausschuß erwartet vom Senat, daß der Datenschutzbeauftragte bei Planungen zum Aufbau automatisierter Informationssysteme in gesetzeskonformer Weise beteiligt wird; eine Unterrichtung lediglich im ADV-Ausschuß ist in diesem Zusammenhang nicht ausreichend."

1.6 Datenschutz in den neuen deutschen Ländern und in Europa

Der aufgelöste Staatssicherheitsdienst der ehemaligen DDR hat Millionen von Akten hinterlassen. Neben Unterlagen über Organisationen und Personal, Auslandsspionage und Unterlagen zum nationalen und internationalen Terrorismus sind auch acht Millionen Personendossiers zu Tage gekommen. Diese Personendossiers, von denen auch zwei Millionen westdeutsche Bundesbürger betroffen sind, enthalten z. T. eine kaum vorstellbar große Menge von Einzelinformationen über das Leben der Zielperson. Da auch das Umfeld beobachtet wurde — wie z. B. Freunde oder Bekannte —,erhöht sich die Zahl der Betroffenen um ein vielfaches.

Es stellte sich die Frage, wie man mit den Unterlagen, deren sensible Daten zu einem großen Teil rechtswidrig erhoben wurden, umgehen sollte. Einerseits liegt es im Interesse der Betroffenen, die Akten so schnell wie möglich zu vernichten, damit die Verletzung der Persönlichkeitsrechte endlich aufhört. Dadurch wäre jedoch in vielen Fällen kein Rechtsfriede erreicht. Daher sprechen wesentlich mehr Argumente für eine — wenigstens längerfristige — Aufbewahrung der Stasi-Akten: Nur so können Betroffene ihre zivil- und strafrechtliche Rehabilitation betreiben und sich gegen ungerechtfertigte Angriffe verteidigen. Dieses setzt aber voraus, daß sie Einsicht nehmen können oder durch Auskunft erfahren, was über sie in den Akten gespeichert ist. Nicht zuletzt auch die Frage der Zulässigkeit der Auswertung der Akten durch Staatsanwaltschaft und Nachrichtendienste ruft datenschutzrechtliche Überlegungen hervor. Auch für die politische und historische Aufbereitung der Rolle des Staatssicherheitsdienstes für Staat und Gesellschaft der ehemaligen DDR ist die Aufbewahrung der Akten wichtig.

Die Aufbewahrung der Akten, insbesondere die Nutzung und Verwendung bedarf einer gesetzlichen Regelung. Sie steht noch aus. Im Dezember 1990 wurde von dem Sonderbeauftragten der Bundesregierung eine „vorläufige Benutzerordnung" für die personenbezogenen Stasiakten erlassen.

Mit Fragen des Datenschutzes im deutsch-deutschen Verhältnis hat sich auch die Konferenz der Datenschutzbeauftragten beschäftigt (vgl. Anlage 6 dieses Berichts).

Die Kommission der EG hat eine Initiative ergriffen, mittels einer allgemeinen Richtlinie zur Harmonisierung des Datenschutzes in den Mitgliedsländern beizutragen (vgl. Pkt. 3 des Berichts). Spätestens mit Erlaß der im Entwurf vorliegenden Richtlinie wird zu prüfen sein, welche Auswirkungen sich daraus für die Datenschutzgesetzgebung im Lande Bremen ergeben.

1.7 Technische Entwicklung

Datenschutz ist zugleich eine Antwort auf die Herausforderungen der neuen Informations- und Kommunikationstechniken (IuK-Techniken). Wenn die neuen IuK-Techniken in ihrer Anwendung von den Betroffenen in den verschiedenen Rollen (Bürger, Arbeitnehmer usw.) akzeptiert werden sollen, muß überzeugend dargelegt werden können, daß Staat und Wirtschaft bei der Einführung der Techniken und bei der Festlegung der Komponenten und der Regeln für den Umgang mit ihnen nicht nur die ökonomischen Aspekte und die Arbeitserleichterung berücksichtigt haben, sondern auch den notwendigen Schutz der Privatsphäre der Betroffenen beachtet haben. Vor dem Hintergrund der Einführung moderner Informations- und Kommunikationstechnik gewinnt der Datenschutz eine neue Bedeutung. Es geht nicht mehr allein darum, die Autonomie des Einzelnen in seiner Entscheidung zu schützen, sondern die gesellschaftliche Entwicklung vor einer Übertechnisierung zu bewahren, in der Entscheidungen durch effiziente und optimal durchstrukturierte Technik- und Informationssysteme gefällt werden, der Bürger hingegen nicht mehr beteiligt oder gar nicht mehr benötigt wird. Eine solche Entwicklung wäre unvereinbar mit einem auf Partizipation der Bürger angelegten demokratischen Rechtsstaat. In diesem Sinne trifft auch die Landesverfassung von 1947 — die in letzter Zeit wegen der darin enthaltenen überholten Regelungen in die Schlagzeilen gekommen ist — eine erstaunlich moderne und zukunftsweisende Regelung. Der Wortlaut des Artikel 12 BremLV: „Der Mensch steht höher als Technik und Maschine. Zum Schutz der menschlichen Persönlichkeit und des menschlichen Zusammenlebens kann durch Gesetz die Benutzung wissenschaftlicher Erfindungen und technischer Einrichtungen unter staatlicher Aufsicht und Lenkung gestellt sowie beschränkt und untersagt werden." Eine Ausprägung dieses Gedankens stellen das Bremische Datenschutzgesetz und die bereichsspezifischen Datenschutzregelungen im Lande dar.

Folgende zentrale Themen standen im Vordergrund meiner Tätigkeit im letzten Jahr:

- Die datenschutzgerechte Gestaltung der Telekommunikation unter ISDN. In diesem Kontext stehen auch die Beschlüsse der Datenschutzbeauftragten des Bundes und der Länder, die als Anlage 7 und 8 in diesem Bericht abgedruckt sind.
- Der PC-Einsatz in der Verwaltung hat im letzten Jahr erheblich zugenommen. Im Rahmen meiner Beteiligung im ADV-Ausschuß habe ich zu einer Vielzahl von PC-Anträgen datenschutzrechtliche Stellungnahmen abgegeben, ausgewählte Aspekte sind unter Pkt. 2.12 des Berichts zusammengefaßt.

— Wahrung des Datenschutzes und des Fernmeldegeheimnisses bei Telefax: Telefax ist ein von der Deutschen Bundespost — Telekom — angebotener Dienst zur Übertragung von Textkopien (Faksimiles) über das Telefonnetz. Nach Angaben der Deutschen Bundespost wartet dieser Bereich mit imposanten Zuwachsraten auf. Ende des letzten Jahres sollen weit mehr als eine halbe Million Telefax-Anschlüsse installiert worden sein. Auch die Behörden im Land Bremen nutzen diese Kommunikationstechnik im großen Umfang. Der Einsatz ist allerdings nicht ganz ohne Tücken. Da Telefax-Geräte wie Telefone an das öffentliche Fernsprechnetz angeschlossen sind, kann man sich genau wie beim Telefonieren verwählen. Während der Mensch aber am Telefon seinen Irrtum oder Fehler schnell erkennt und dem Gesprächspartner am anderen Ende der Leitung keine Mitteilung über sein inhaltliches Anliegen macht, reagiert ein Telefax-Gerät in einem solchen Fall völlig anders. Ist eine Verbindung zu einem anderen Telefax-Gerät erst einmal aufgebaut, dann gibt es kein Halten mehr. Auch dem falschen Adressaten wird in Windeseile die Nachricht übermittelt. Selbst wenn aber das richtige Faxgerät angesteuert worden ist, entzieht es sich häufig der Kenntnis des Absenders, wer auf der anderen Seite die Dokumente in Empfang nimmt und auf welchem Wege sie dem eigentlichen Adressaten zugeleitet werden. Die Probleme stellen sich im öffentlichen und privaten Bereich gleichermaßen, Mindestanforderungen für die Gewährleistung des Datenschutzes bei der Nutzung des Telefax-Dienstes sind unter Pkt. 4.5 dieses Berichtes zusammengestellt.

2. Öffentlicher Bereich

2.1 Personalwesen

2.1.1 Bewerbungen innerhalb der Stadtverwaltung

Das Bewerbungsverfahren der Stadtverwaltung Bremerhaven sieht die Verpflichtung der städtischen Bediensteten vor, bei Stellenausschreibungen innerhalb der Verwaltung Bewerbungen auf dem Dienstwege an das Personalamt zu senden, d. h. die Beschäftigten haben ihre Bewerbungen über die nächsthöheren Vorgesetzten dem jeweiligen Amtsleiter zuzuleiten. Dieser gibt die Bewerbungen an das Personalamt weiter. Das Personalamt leitet ebenfalls die Bestätigung des Eingangs der Bewerbung auf dem beschriebenen Dienstwege dem Bewerber zu.

Das bisherige Bewerbungsverfahren beeinträchtigt schutzwürdige Belange der Betroffenen. Aus Erfahrung ist bekannt, daß abgewiesene Bewerber sehr häufig mit mehr oder weniger hämischen Bemerkungen der Vorgesetzten und anderer Kollegen zu rechnen haben, insbesondere weil mehrere Personen innerhalb eines Amtes von der oder den Bewerbungen Kenntnis erlangt haben. Außerdem ist mir berichtet worden, daß bei Bewerbungen innerhalb eines Amtes aussichtsreiche Bewerber mit der Begründung abgewiesen werden, dieser Bewerber habe durch seine Bewerbungen auf Stellen anderer Ämter eine andere Orientierung oder ähnliches zum Ausdruck gebracht.

Ich habe den Magistrat darauf hingewiesen, daß die mit diesem Verfahren verbundene Datenverarbeitung unzulässig ist, weil nach den gesetzlichen Bestimmungen (§ 22 BrDSG) die Tatsache der Bewerbung und die damit zusammenhängenden personenbezogenen Daten der Bewerber nur den Stellen zugänglich gemacht werden dürfen, die am Bewerbungsverfahren zu beteiligen sind.

Nach der Geschäftsverteilung bzw. der Organisationsstruktur der Stadtverwaltung obliegt dem Personalamt die Entscheidung über die Besetzung einer freiwerdenden Stelle. Das Personalamt trifft seine Entscheidung nach Beteiligung des Amtes, in dem die Stelle zu besetzen ist. Darüber hinaus ist der zuständige Personalrat zu beteiligen. Da weitere Stellen am Auswahlverfahren nicht beteiligt sind, dürfen ausschließlich diese Kenntnis von den Bewerbungen erhalten.

Als datenschutzgerechte Lösung bleibt nur, daß städtische Bedienstete ihre Bewerbungen unmittelbar an das Personalamt senden. Die damit zusammenhängende Korrespondenz hat ebenfalls unmittelbar zu erfolgen. Eine Stellungnahme des Magistrats steht noch aus.

2.1.2 Datenerhebung bei der Feststellung eines Dienstunfalls

Nach Rundschreiben der Senatskommission für das Personalwesen (SKP) erfolgt die gutachterliche Feststellung der Körperschäden, die ein Beamter aufgrund

eines Dienstunfalles erlitten hat, einheitlich für die bremischen Beamten durch die berufsgenossenschaftlichen Unfallbehandlungsstellen und deren Durchgangsärzte. In diesem Fall hat der Beamte seinen unmittelbaren Dienstvorgesetzten unverzüglich zu unterrichten. Der Dienstvorgesetzte hat die sofortige Überführung des Verletzten zu einer berufsgenossenschaftlichen Unfallbehandlungsstelle oder einem Durchgangsarzt zu veranlassen. Dort wird von dem Beamten verlangt, eine Erklärung über die Entbindung von der ärztlichen Schweigepflicht zu unterschreiben. Aufgrund dieser Erklärung wird der SKP der Durchgangsarztbericht übersandt. Die SKP benötigt den Durchgangsarztbericht für die Entscheidung, ob ein Dienstunfall vorliegt.

Als Rechtsgrundlagen hat die SKP die Allgemeinen Verwaltungsvorschriften zum Beamtenversorgungsgesetz sowie die Heilverfahrensverordnung angegeben. Nach diesen Bestimmungen wird der einheitlich verwendete Durchgangsarztbericht für folgende Zwecke angefordert:

— Prüfung der Voraussetzungen eines Dienstunfalles,

— Untersuchung aller Unfälle, die den Dienstvorgesetzten bekannt werden,

— Durchführung eines Heilverfahrens.

Ich habe der SKP mitgeteilt, daß weder die vom Betroffenen erklärte Entbindung von der ärztlichen Schweigepflicht noch die Bestimmungen in den Verwaltungsvorschriften zulässige Einschränkungen des informationellen Selbstbestimmungsrechts darstellen.

Da die Aufgaben der öffentlichen Verwaltung grundsätzlich gesetzlich definiert sind und insoweit die dafür erforderliche Verarbeitung personenbezogener Daten ebenfalls gesetzlich normiert sein muß, ist eine über die gesetzliche Regelung hinausgehende Datenverarbeitung nicht zulässig. Die Übermittlung des Durchgangsarztberichts kann nicht mit der Einwilligung begründet werden, denn der Betroffene ist verpflichtet, der Weiterleitung des Berichtes zuzustimmen. Willigt der Betroffene nicht in die geforderte Entbindung von der ärztlichen Schweigepflicht ein, wird der Unfall nicht als Dienstunfall anerkannt. Der Betroffene wird somit mehr oder weniger gezwungen sein, eine derartige Einwilligungserklärung abzugeben. Eine wirksame Einwilligung liegt somit nicht vor.

Daraus ergibt sich, daß die Heranziehung eines ärztlichen Gutachtens zur Feststellung eines Dienstunfalles nur aufgrund einer verfassungsgemäßen Rechtsgrundlage zulässig ist. Es muß bereits im Gesetz normenklar geregelt werden, unter welchen Voraussetzungen und zu welchem Zwecke ein ärztliches Gutachten angefordert werden kann. Die von der SKP angegebenen Verwaltungsvorschriften zum Beamtenversorgungsgesetz genügen diesen Erfordernissen nicht.

Ich habe die SKP gebeten, sich auf Bundesebene für eine entsprechende Anpassung des Beamtenversorgungsgesetzes an die Vorgaben des Volkszählungsurteils einzusetzen und unterschiedliche Durchgangsarztberichte anzufordern, die auf die jeweiligen Zwecke unmittelbar abgestimmt sind (z. B. Prüfung der Voraussetzungen eines Dienstunfalles, Prüfung einer Maßnahme im Rahmen eines Heilverfahrens).

Die SKP hat sich bereiterklärt, das verwendete Formular unter Datenschutzgesichtspunkten zu überprüfen, im übrigen teilt sie meine Bedenken und will sich auf Bundesebene für eine Novellierung des Beamtenversorgungsgesetzes einsetzen.

2.1.3 Auskunftsersuchen des Dienstherrn gegenüber der Rentenstelle der Deutschen Bundespost

Versorgungsempfänger, die eine Leistung aus der gesetzlichen Rentenversicherung erhalten, sind nach dem Beamtenversorgungsgesetz verpflichtet, diese der Senatskommission für das Personalwesen (SKP) zu melden. Hierzu legen sie den Rentenbescheid sowie spätere Rentenänderungsbescheide zur Einsichtnahme vor. Die SKP entnimmt daraus die für die Rentenanrechnung erforderlichen Daten. Für den weiteren Vollzug der Rentenanrechnung (jährliche prozentuale Rentenanpassung) bedient sich die SKP seit dem 01. April 1979 des Rentenauskunftsverfahrens der Deutschen Bundespost, das die senatorische Behörde in die Lage versetzt, die Rentenanrechnung infolge prozentualer Erhöhung maschinell zu erledigen. Damit ist es der Behörde möglich, unverzüglich auf die jährlichen

Rentenerhöhungen zu reagieren, ohne daß beim Versorgungsempfänger Überzahlungen entstehen bzw. Nachzahlungen notwendig werden. Der Versorgungsempfänger erhält damit ohne Verzögerung die ihm zustehende aktuelle Zahlung. Nach Angaben der SKP kann dieses Ziel ohne das Rentenauskunftsverfahren der Deutschen Bundespost nicht eingehalten werden.

Ich habe der SKP mitgeteilt, daß eine derartige Datenerhebung nach dem Beamtenversorgungsgesetz nicht vorgesehen ist. Dieses Gesetz regelt ausdrücklich, daß der betroffene Versorgungsempfänger selbst verpflichtet ist, jede Leistungsänderung aus der gesetzlichen Rentenversicherung unverzüglich zu melden. Deshalb ist die SKP lediglich befugt, die erforderlichen Daten beim Betroffenen mit seiner Kenntnis zu erheben.

Gleichwohl bringe ich Verständnis für die von der SKP geschilderten praktischen Schwierigkeiten auf. Nach den Erfahrungen der senatorischen Behörde bringt eine Vielzahl der Leistungsempfänger — oft mit viel Mühe — die Rentenmitteilung persönlich; die zwangsläufig auftretenden Überzahlungen führen bei den Betroffenen zu Verunsicherungen. Nicht zuletzt bringt das Rentenauskunftsverfahren für die Versorungsempfänger eine erhebliche Erleichterung.

Aufgrund der geltenden Rechtslage besteht derzeit lediglich die Möglichkeit, es dem einzelnen Leistungsempfänger freizustellen, ob er seiner Anzeigepflicht nachkommt oder ob er der SKP die Einholung der erforderlichen Auskünfte überläßt.

Die SKP hat mir inzwischen mitgeteilt, daß sie entsprechend meinem Vorschlag die erforderlichen Auskünfte über das Rentenauskunftsverfahren der Deutschen Bundespost nur noch dann einholt, wenn die schriftliche Einwilligung des Leistungsempfängers vorliegt.

Darüber hinaus wird die senatorische Behörde im Arbeitskreis der Versorgungsreferenten die Frage aufwerfen, ob das Beamtenversorgungsgesetz um eine Erhebungsvorschrift zur Teilnahme am Rentenauskunftsverfahren ergänzt werden soll.

2.1.4 Weiterleitung einer Strafanzeige an die oberste Dienstbehörde

Bei einem Polizeirevier in Bremerhaven ist gegen einen Polizeibeamten wegen seines Verhaltens außerhalb des Dienstes eine Strafanzeige erstattet worden. Der Dienststellenleiter hat diese Anzeige zum Anlaß genommen, den Vorfall dem Magistrat als oberster Dienstbehörde schriftlich zu melden. Der Meldung ist eine Kopie der Strafanzeige beigefügt worden.

Der gesamte Vorgang ist auf dem Dienstweg dem Personalamt zugeleitet worden, so daß eine Vielzahl von Personen Kenntnis davon erhalten hat. Dem betroffenen Polizeibeamten ist daraufhin ebenfalls auf dem Dienstweg vom zuständigen Dezernenten mitgeteilt worden, daß gegen ihn disziplinarrechtliche Vorermittlungen eingeleitet worden seien. Der Betroffene hat mich um eine datenschutzrechtliche Prüfung gebeten.

Die Ortspolizeibehörde vertritt die Auffassung, die gegen den betroffenen Polizeibeamten erstattete Strafanzeige berühre nicht nur seine Privatsphäre. Vielmehr liege der begründete Verdacht nahe, daß das gezeigte Verhalten des Polizeibeamten dazu geeignet ist, das Ansehen der Polizei in der Öffentlichkeit massiv zu schädigen. Aus diesem Grunde habe die Strafanzeige nicht nur an die Staatsanwaltschaft, sondern auch an das Personalamt weitergeleitet werden müssen.

Nach Ansicht des Leiters der Ortspolizeibehörde ergibt sich die Verpflichtung dazu aus § 56 Bremisches Beamtengesetz (BremBG), wonach der Beamte verpflichtet sei, Vorgesetzte zu beraten und zu unterstützen. Diese Beratungs- und Unterstützungspflicht umfasse auch die Verpflichtung, vom Dienstherrn Schaden abzuwenden. Von daher habe der Revierleiter seiner Verpflichtung nachkommen müssen, um nicht selber Gefahr zu laufen, eine Dienstpflichtverletzung zu begehen. Auch der Weg der Weiterleitung der Strafanzeige sowie die Mitteilung des Dezernenten an den Betroffenen über die Einleitung disziplinaerechtlicher Vorermittlungen sei zwingend vorgeschrieben. Der Aufbau des Dienstweges ergebe sich aus § 4 Abs. 2 BremBG.

Entsprechend dieser Bestimmung habe der Schriftverkehr über den Wachhabenden und den Revierleiter zum Amtsleiter der Schutzpolizei verlaufen müssen. Von dort aus verlaufe er dann zum Behördenleiter und schließlich zur obersten Dienstbehörde (Magistrat). Die beamtenrechtliche Verpflichtung zur Einhaltung des Dienstweges ergebe sich aus § 159 BremBG.

Ich habe die Ortspolizeibehörde darauf hingewiesen, daß Daten grundsätzlich nur für die Zwecke verarbeitet werden dürfen, für die sie erhoben worden sind. Da der Polizeibeamte auf dem Revier die Strafanzeige als Hilfsbeamter der Staatsanwaltschaft aufgenommen hat, hat er ausschließlich die Befugnis und Verpflichtung, die Anzeige zum Zwecke der Strafverfolgung an die zuständige Staatsanwaltschaft weiterzuleiten. Eine Zweckänderung ist weder nach dem Bremischen Datenschutzgesetz noch nach der Bremische Disziplinarordnung zulässig. Im übrigen schreiben die zitierten beamtenrechtlichen Vorschriften keine Weitergabe personenbezogener Daten vor.

Meine Rechtsauffassung wird auch durch die „Anordnung über Mitteilungen in Strafsachen" (Mistra) unterstützt, auf die ich die Orstpolizeibehörde hingewiesen habe. Diese Anordnung ist von den Landesjustizverwaltungen aufgrund des Volkszählungsurteils übergangsweise bis zur Schaffung eines notwendigen Justizmitteilungsgesetzes erlassen worden. Mitteilungen über Strafsachen gegen Angehörige des öffentlichen Dienstes sind in Nr. 15 Mistra i. V. m. Nr. 4 Mistra ausdrücklich geregelt. Danach haben die Strafverfolgungsbehörden lediglich die Erhebung der öffentlichen Klage an den unmittelbaren Dienstvorgesetzten und an den Leiter der Aufsichtsbehörde weiterzuleiten. Die Gerichte haben das Urteil sowie den Ausgang des Verfahrens mitzuteilen.

Diese Regelung hebt auf ein späteres Verfahrensstadium ab, in dem gesicherte Erkenntnisse vorliegen. Zur Erhebung der öffentlichen Klage ist nur die Staatsanwaltschaft befugt (§ 152 StPO). Damit ist eine entsprechende Mitteilung an den Dienstvorgesetzten der Staatsanwaltschaft vorbehalten.

Ich habe die Behörde aufgefordert, ihrer Verpflichtung aus dem Bremischen Datenschutzgesetz nachzukommen, d. h. die unzulässigerweise übermittelten Daten in dieser Personalangelegenheit sind zu löschen bzw. zu vernichten. Die Ortspolizeibehörde bleibt bei ihrer Rechtsauffassung und will an der rechtswidrigen Praxis festhalten.

2.1.5 Eigenständiger Beihilfeanspruch für Angehörige

Nach dem geltenden Beihilferecht steht ausschließlich dem beihilfeberechtigten Angehörigen des öffentlichen Dienstes ein Beihilfeanspruch für seine Familienmitglieder zu; diese haben keinen eigenständigen Beihilfeanspruch. Daraus ergibt sich, daß die Familienangehörigen des Beihilfeberechtigten gezwungen sind, sämtliche dem Beihilfeantrag beizufügenden Arztunterlagen dem Familienmitglied zu übergeben, dem der Beihilfeanspruch zusteht.

Aus verschiedenen Eingaben ist mir bekannt, daß diese Verfahrensweise von getrennt lebenden Ehegatten sowie erwachsenen Kindern der Beihilfeberechtigten oft als problematisch empfunden wird, soweit für diese Beihilfe beantragt werden kann. Obwohl die familiäre Verbundenheit nicht mehr voll besteht, erfährt der Beihilfeberechtigte auch in diesen Fällen zum Teil intimste Krankheitsdaten seiner Familienangehörigen.

Eine vergleichbare Rechtslage bestand in der gesetzlichen Krankenversicherung vor Inkrafttreten des Gesundheitsreformgesetzes (SGB V). Nunmehr haben die Angehörigen eines Kassenmitgliedes einen eigenen Leistungsanspruch und sind insoweit auch im Hinblick auf die Erhebung, Speicherung und Löschung ihrer Daten und ihrer Auskunftsrechte dem Kassenmitglied gleichgestellt.

Ich habe daher gegenüber der Senatskommission für das Personalwesen (SKP) angeregt, durch eine Änderung der Bremischen Beihilfeverordnung den Familienangehörigen der beihilfeberechtigten Personen einen selbständigen Beihilfeanspruch einzuräumen, um diesem Datenschutzproblem Rechnung zu tragen. Die SKP hält dies aufgrund der derzeitigen Rechtslage nicht für möglich und möchte aus Gründen der Bundeseinheitlichkeit die Diskussionen dazu im Bund/Länder-Arbeitskreis abwarten.

2.2 Inneres

2.2.1 Verfassungsschutz

2.2.1.1 Beschränkung meiner Kontrollkompetenz beim Landesamt für Verfassungsschutz

Auch im vergangenen Jahr habe ich wieder ein gutes Dutzend Eingaben beim Landesamt für Verfassungsschutz (LfV) geprüft. Die Prüfungen liefen bisher in der

Regel wie folgt ab: Zunächst wurden Name und Geburtsdatum der Person in dem Informationssystem der Verfassungsschutzbehörden des Bundes und der Länder NADIS abgefragt. Der Antwortbildschirm enthielt dann die Auskunft, ob ein Datenbestand zur Person vorhanden ist und ggf. die Information, wo sich zugehörige Akten — also beim Bund oder in den Ländern — befinden.

Für den Fall, daß das Land Bremen ein Aktenzeichen zu der Person in NADIS gespeichert hat, überprüfte ich den Akteninhalt. Soweit Aktenzeichen des Bundes oder anderer Länder zur Person bestanden, habe ich den zuständigen Landes- oder Bundesbeauftragten um eine Überprüfung gebeten. Nach Abschluß konnte ich dann den Betroffenen das Prüfergebnis mitteilen. Dabei beschränkte sich die Auskunft nicht in jedem Fall darauf, man habe bei der Prüfung keine Verstöße gegen datenschutzrechtliche Bestimmungen festgestellt, sondern aufgrund der Überprüfung durch die eingeschalteten Datenschutzbeauftragten konnte den Petenten eine umfassende Auskunft erteilt werden.

Dieses Verfahren wird mir neuerdings vom LfV bestritten. Das LfV hat seine Praxis wie folgt geändert: Bei der Abfrage wird ein Bildschirmformat aufgerufen, das lediglich Auskunft darüber gibt, ob das Land Bremen in NADIS Daten zur Person gespeichert hat. Dadurch wird eine umfassende Prüfung nicht mehr ermöglicht. Dies hat zur Konsequenz, daß ich den Bürger in jedem Fall an die Datenschutzbeauftragten aller anderen Länder und des Bundes verweisen muß, denn es könnte auch bei den dortigen Verfassungsschutzämtern eine Speicherung vorliegen. Einmal davon abgesehen, daß die Verfassungsschutzämter selbst mit vermehrten Bürgereingaben zu rechnen hätten, stellt das Verfahren auch aus praktischen Gründen für den Bürger ein unnötige Belastung dar. Dieses Verfahren erschwert die Rechtswahrnehmung des Bürgers erheblich.

Rechtlich stützt das LfV seine neue Praxis auf die mit dem Bremischen Datenschutzgesetz geänderte Rechtslage. Nach dem früheren Bremischen Datenschutzgesetz galt schon das Bereithalten von Daten zum Abruf als Übermittlung. Damit galten alle in NADIS eingestellten zum Abruf bereitgehaltenen Daten als an das LfV übermittelt. Mein Kontrollrecht bezog sich deshalb auch auf die Kenntnisnahme der Daten, die das LfV abrufen konnte. Nach der neuen Vorschrift des § 2 Abs. 2 Nr. 4 BrDSG — diese Regelung korrespondiert mit § 3 Abs. 5 Nr. 3 des neuen Bundesdatenschutzgesetzes — gelten Daten erst dann als übermittelt, wenn zum Abruf bereitgehaltene Daten tatsächlich abgerufen werden. Das LfV behauptet nun, es würde in den von mir zu prüfenden Fällen lediglich auf die vom Land Bremen in NADIS eingespeicherten Daten zugreifen. Im übrigen beruft sich das LfV auf die Gesetzesänderung, die nach seiner Ansicht gerade auch das Verbundsystem NADIS im Auge gehabt habe.

Ich halte diese neue Praxis für eine Einschränkung meiner gesetzlichen Prüfkompetenz. Alle Abrufmöglichkeiten, die dem LfV zur Verfügung stehen, müssen überprüfbar sein. Anderenfalls wäre ich gezwungen, in jedem Fall auch für länger zurückliegende Zeiträume Protokollauswertungen über Zugriffe des LfV auf NADIS anzufordern.

Nachdem mir in einem konkreten Fall mein Recht zur umfassenden Prüfung verweigert wurde, obwohl das LfV auf den gesamten NADIS-Datensatz zugegriffen hatte, habe ich mich an den Senator für Inneres gewandt und um eine Entscheidung gebeten.

2.2.1.2 Löschungsreife Akten

Im letzten Jahr habe ich wieder eine Reihe von Eingaben beim LfV geprüft. Immer wieder befinden sich in den Akten des Verfassungsschutzes Dokumente, die ein Kopfschütteln auslösen. Ein Fall dieser Art soll hier einmal dargestellt werden.

Die Akte des Verfassungsschutzes begann mit einer umfangreichen polizeilichen Ermittlungsakte aus dem Jahre 1975. Gegen den Betroffenen war ohne sein Wissen ermittelt worden. Eine Mitbewohnerin einer Hochhausanlage hatte gegenüber der Polizei anonym Verdächtigungen in Bezug auf den Petenten geäußert, wegen der — wie sie sich ausdrückte — Zusammenkunft und Beherbergung undurchsichtiger Gestalten. Nachdem die Anruferin von der Polizei ermittelt werden konnte, äußerte sie weitere Verdachtsmomente gegen den Petenten. So würden noch spät abends Bücherkisten in die Wohnung des Petenten gebracht, zeitweilig rieche es abends im Hausflur nach Lötkolben — ein Indiz für Bomben basteln — und wenn Besucher gingen, werde häufig spät abends noch die Klo-

spülung betätigt, nach ihrer Ansicht, um den Weggang der Personen zu verschleiern. Eines Tages kam der Mitbewohnerin ein Besucher des Petenten so verdächtig vor, daß sie ihn bis zum Hauptbahnhof verfolgte, das Reiseziel beim Fahrkartenkauf erlauschte und sofort die zuständige Polizeidienststelle darüber informierte. Identität und Reiseziel der Person konnten ermittelt werden, weitere Polizeidienststellen anderer Länder wurden in die Ermittlungen mit einbezogen — ohne Erkenntnisse. Schließlich konnten keine hinreichenden Anhaltspunkte für weitere polizeiliche Maßnahmen gefunden werden. Gleichwohl wurde die Akte nicht geschlossen, sondern aufgrund des Verdachts anarchistischer Bestrebungen komplett an das LfV abgegeben.

Einige Jahre später hatte der Betroffene brieflichen Kontakt mit einem inhaftierten RAF-Mitglied unterhalten. Das LfV wurde hierüber unterrichtet, die dann getroffenen umfangreichen Maßnahmen blieben ohne weitere Erkenntnisse.

Im Jahre 1982 rückte der Petent dann erneut in das Blickfeld des Verfassungsschutzes. Das bayerische LfV hatte bei einer kommunistischen Gruppierung eine Adressenliste sichergestellt, in der mehrere Schwulen- und Lesbenverbände, entsprechende Mitgliedsorganisationen von großen politischen Parteien, Studentenvertretungen, aber auch der Petent aufgeführt waren. Eine Kopie davon erhielt das LfV. Das LfV Bremen hatte daraufhin mitgeteilt, daß es keinen Bedarf für weitere Ermittlungen sehe, gleichwohl wurde das Material zur Akte genommen, die in NADIS vorgesehene Löschungsprüfungsfrist verlängerte sich damit auf das Jahr 1992.

Der Vorgang zeigt — abgesehen von dem Briefkontakt zu einem inhaftierten RAF-Mitglied — einmal mehr, daß es Polizei und Verfassungsschutz schwerfällt, sich von Vorgängen zu trennen. Gleichzeitig wird deutlich, daß man — auch wenn man nicht Mitglied einer kommunistischen Organisation ist — bereits dann Beobachtungsobjekt werden kann, wenn im Umfeld kommunistischer Organisationen zufällig Informationen auftauchen. Die Akte wurde auf meine Empfehlung hin vernichtet, der Eintrag in NADIS gelöscht.

2.2.1.3 Beobachtung der PDS

Der Presse war zu entnehmen, daß die Innenministerkonferenz (IMK) am 16. 12. 1990 beschlossen hat, durch „offene Beobachtung" die Verfassungsmäßigkeit der PDS zu überprüfen. Den Zeitungsberichten zufolge hält der bayerische Innenminister die PDS wegen ihrer Programmatik für verfassungsfeindlich. Bayern wolle daher die geheimdienstliche Überwachung der PDS einleiten. Vertreter des Innensenators erklärten der lokalen Presse gegenüber, eine Überwachung der PDS mit nachrichtendienstlichen Mitteln sei in Bremen derzeit nicht beabsichtigt, man wolle aber alle allgemein zugänglichen Quellen über die PDS auswerten.

Ich habe die Zeitungsmeldungen zum Anlaß genommen, den Innensenator zu bitten, mich über den Beschluß zu unterrichten. Zwar ist der von der IMK erteilte Prüfauftrag nicht zwingend mit der Verarbeitung personenbezogener Daten verbunden, spätestens aber nach einer Beschlußfassung der IMK im Sinne der bayerischen Initiative stünde die Verarbeitung personenbezogener Daten durch die Verfassungsschutzämter an. Ich habe daher dem Innensenator begleitend meine datenschutzrechtlichen Überlegungen mitgeteilt:

Nach § 3 Abs. 1 des Gesetzes über den Verfassungsschutz im Lande Bremen (BremVerfSchG) ist die Sammlung und Auswertung von Auskünften, Nachrichten und sonstigen Unterlagen über Bestrebungen, die gegen die freiheitlich-demokratische Grundordnung gerichtet sind, Aufgabe des Verfassungsschutzes. Die Erlaubnis zur Sammlung und Auswertung von Materialien über Bestrebungen gegen die freiheitlich-demokratische Grundordnung setzt demnach Anhaltspunkte für den Verdacht voraus, daß von der PDS derartige Ziele angestrebt werden. Die evtl. bloße Ablehnung der freiheitlich-demokratischen Grundordnung durch die PDS reicht für sich nicht aus, sie zu beobachten. Nach meiner Einschätzung ist die derzeit in einer Agonie — zumindest in einer Sinnkrise — befindliche PDS zu Bestrebungen gegen die freiheitlich-demokratische Grundordnung nicht fähig und plant sie auch nicht.

Weiter habe ich darauf aufmerksam gemacht, daß der Staat nach dem Verfassungsauftrag (Art. 21 GG) erst dann eingreifen darf, wenn die demokratischen und anerkannten Handlungsspielräume durch die PDS deutlich überschritten sind und die Zielrichtung der Partei offensichtlich auf eine von der Verfassung nicht mehr tolerierte Entwicklung und Veränderung unserer Gesellschaft gerichtet ist. Die demokratische Auseinandersetzung mit der PDS erfolgt in unserer Gesellschaft

grundsätzlich ohne staatliche Eingriffe (dazu zählt auch ein Sammeln und Auswerten offenen Materials) u. a. durch Diskussion und durch Wahlen. Bei den jüngsten Wahlen zum Deutschen Bundestag erhielt die PDS im Lande Bremen 1.06 % der Stimmen. Dieses Wahlergebnis kann nur als Indiz dafür gewertet werden, daß die demokratische und gesellschaftliche Auseinandersetzung mit der PDS bewirkt hat, daß — wenigstens im Lande Bremen — eine Gefahr für die freiheitlich-demokratische Grundordnung von ihr nicht ausgehen kann.

Diese Prognose wird nicht zuletzt durch die politischen Veränderungen in der UdSSR und die demokratische Öffnung in den übrigen osteuropäischen Staaten gestützt. Weiter ist zu berücksichtigen, daß die PDS nicht — wie früher die DKP durch die SED — umfassend unterstützt wird.

Ein Beobachtungsauftrag durch die IMK in offener Form oder mit nachrichtendienstlichen Mitteln an die Verfassungsschutzbehörden stellt einen Eingriff in den Gestaltungsrahmen der Parteien, insbesondere einen Eingriff in die politische Gestaltungsfreiheit der betroffenen Bürger dar. In diesem Zusammenhang ist auf das Volkszählungsurteil des Bundesverfassungsgerichts hinzuweisen. Das Gericht hat ausgeführt, wer damit rechne, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird, und wer damit rechne, daß ihm dadurch Risiken entstehen, werde möglicherweise auf die Ausübung seiner Grundrechte verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des einzelnen beeinträchtigen, sondern auch das Gemeinwohl.

Unter diesen Gesichtspunkten ist ein strenger Maßstab an die Stigmatisierung von Parteien und deren Anhängern zu legen.

Ich würde es daher derzeit aus den genannten Gründen für datenschutzrechtlich unzulässig halten, Speicherungen von personenbezogenen Daten von Mitgliedern, Sympathisanten oder sonstigen Anhängern der PDS nach dem Bremischen Verfassungsschutzgesetz vorzunehmen. Auch die scheinbar von Vertretern des Innensenators getroffene Unterscheidung nach offener und nachrichtendienstlicher Beobachtung halte ich für unzulässig, solange die Voraussetzungen des § 3 Abs. 1 BremVerfSchG nicht vorliegen, denn maßgeblich für einen unterschiedlichen Arbeitsansatz kann allein der Grad der Gefährdung der freiheitlich-demokratischen Grundordnung und das konspirative (verdeckte) Verhalten der Anhänger einer solchen Organisation sein.

Ich habe den Senator für Inneres gebeten, diese Überlegungen bei seiner Entscheidung in der Innenministerkonferenz zu berücksichtigen.

2.2.2 Polizei

2.2.2.1 Fortentwicklung der polizeilichen Datenverarbeitung in Bremen

In meinem letzten Jahresbericht (S. 12) habe ich über die Planungen des Senators für Inneres berichtet, verschiedene Informationssysteme in ein Projekt ISA-Dezentral (ISA-D) zu integrieren und diese flächendeckend einer großen Zahl polizeilicher Organisationseinheiten zur Verfügung zu stellen.

Im letzten Jahr habe ich mehrere Gespräche mit Vertretern des Senators für Inneres, des Polizeipräsidiums und des Rechenzentrums der bremischen Verwaltung geführt. Dabei wurde ich über den jeweiligen Planungsstand informiert und hatte die Möglichkeit, datenschutzrechtliche Anforderungen zu markieren.

Die bisherigen Planungen der Polizei sehen folgendes vor:

Für 42 Organisationseinheiten der Polizei — das sind Kommissariate, Inspektionen und Polizeireviere — soll der dezentrale Zugriff auf die Systeme ISA (Informationssystem Anzeigen des Landes), FAZID (Kfz.-Halterdatei der Stadtgemeinde Bremen), EDAS (Einwohner-Meldedatei des Landes), INPOL (Fahndungsdatei des Bundes) und ZEVIS (zentrales Informationssystem des Kraftfahrtbundesamtes in Flensburg) hergestellt werden. Zu einem späteren Zeitpunkt soll der Zugriff auf das AZR (Ausländerzentralregister beim Bundesverwaltungsamt in Köln) hinzukommen. In einem ersten Schritt — über weitere Ausbaustufen hatte ich bereits berichtet — soll ein Standardauskunftverfahren eingeführt werden, so daß jede Organisationseinheit die Möglichkeit hat, über einen standardisierten Auskunftsbildschirm ausgewählt Datensätze von den genannten Systemen abzufragen. Hierzu werden die eingesetzten PC in lokale Netze eingebunden, die mittels eines Servers an die Landes- und Bundessysteme angebunden werden. Geplant ist, daß nahezu jeder Polizist zu jeder Zeit auf jedes der genannten Systeme zugreifen kann, um Informationen abzurufen.

Ein derartiges Verfahren wirft eine Vielzahl grundsätzlicher datenschutzrechtlicher Probleme auf, etwa ob die für die Landes- und Bundesanbindungen geplanten Strukturen sowie die lokalen Netze innerhalb der Organisationseinheiten hinreichend den datenschutzrechtlichen Anforderungen entsprechen. Wie bereits in meinem 11. Jahresbericht (S. 54) dargelegt, sind rechtliche Grundlagen für das geplante Verfahren nicht oder nur unzureichend gegeben.

Darüber hinaus ist zu berücksichtigen, daß die verwaltungspolizeilichen Systeme EDAS, ZEVIS und FAZID primär als Informationssysteme für die Aufgabenunterstützung der Einwohnermeldeämter bzw. der Kraftfahrzeugzulassungsbehörden konzipiert sind. Abrufe von Stellen des Polizeivollzuges sind nur in konkreten Fällen zulässig. Bei der Nutzung von ISA-D mit einer einheitlichen Benutzeroberfläche wird den Polizeibeamten nicht mehr deutlich, daß sie z. T. auf fremde Informationssysteme im Wege der Übermittlung zugreift. Vielmehr entsteht der Eindruck, es handele sich um eigene polizeiliche Informationssysteme. Die jeweiligen rechtlichen Grundlagen für die Übermittlung von Daten aus diesen Systemen (§ 36 StVG; § 30 BremMeldG) sehen hierfür enge Zweckbindungsgebote vor. Zur Übermittlungskontrolle sind in den jeweiligen Fachgesetzen Protokollierungen vorgeschrieben. Für Übermittlungen aus dem Melderegister gilt gem. § 30 Abs. 3 BremMeldG, daß die auskunftsersuchende Behörde den Namen und die Anschrift des Betroffenen unter Hinweis auf den Anlaß der Übermittlung aufzuzeichnen hat. Nach § 36 Abs. 7 StVG sind bei Abrufen von Fahrzeugdaten aus ZEVIS Aufzeichnungen durch die abrufende Stelle oder das Kraftfahrtbundesamt zu fertigen, die sich auf den Anlaß des Abrufs erstrecken und die Feststellung der für den Abruf verantwortlichen Personen ermöglichen. Dieses gilt auch für die örtlichen Fahrzeugregister. Um eine bundesweit einheitliche Auswertung über Abrufhäufigkeiten und -zwecke aus ZEVIS herbeizuführen, haben sich das Kraftfahrtbundesamt und der Bundesbeauftragte für den Datenschutz über ein Verfahren verständigt, mit dem mittels ZEVIS-Protokollen Auswertungen möglich werden. Dieses Verfahren ist darauf konzipiert, daß einzelne Terminals, die bestimmten Anwendern zuzuordnen sind, sich gegenüber ZEVIS als auskunftsberechtigt ausweisen und deren Abfragen in bestimmten Abständen protokolliert werden. Die ISA-D zugrundeliegende Gestaltung läßt die Zuordnung Terminal — Anwender nicht mehr zu, da nicht der einzelne PC, sondern die in einem lokalen Netz zusammengeführten Rechner sich gegenüber ZEVIS als einzelner Terminal ausweisen sollen, und jeder Polizeibeamte von jeden angeschlossenen PC zugreifen können soll.

Auch bei der technischen Ausgestaltung von ISA-D gilt es, Datenschutz zu beachten. Geplant ist, die Abwehr unberechtigter Benutzer dadurch sicherzustellen, daß alle abfrageberechtigten Polizisten Chip- oder Magnetkarten erhalten. Diese Karten werden mit einer Identifikationsnummer versehen. Ziel ist, daß mit Entnahme der Karte aus dem Kartenleser die Abfrage abgebrochen und der vernetzte PC bis zur erneuten Identifikation gesperrt bleibt. Dieses Verfahren wirft u. a. folgende Fragen auf: Was passiert mit verlorengegangenen Karten, wer ist für die Sperrung der Zugriffsberechtigung verantwortlich? Wie wird verhindert, daß Karten unberechtigt kopiert werden? Wie wird verhindert, daß Karten für den schnellen Zugriff an allgemein zugänglicher Stelle hinterlegt werden?

Eine weitere Frage ist, ob das geplante Netz datenschutzrechtlichen Anforderungen genügen kann. Die bisherige Terminalanbindung soll auf ein weitverzweigtes Datenkommunikationsnetz umgestellt werden. Die Übertragungsgeschwindigkeit würde um das tausendfache gesteigert werden. Damit ist es prinzipiell möglich, das Datenvolumen von ca. zehn Aktenordnern in einer Sekunde vom einen Endgerät zum anderen zu übertragen. Dieses ist jedoch nur ein Leistungsmerkmal des äußerst komplexen Datenkommunikationsnetzes. Es ist noch nicht abzusehen, daß dieser Übergang angemessen geplant, abgestimmt und vorbereitet ist. Der Übergang von „Trampelpfaden" für den Datentransport zu „Hochgeschwindigkeitsautobahnen" für die Unterstützung der Aufgaben bedarf einer Begleitung. Deshalb hat der ADV-Ausschuß eine Arbeitsgruppe eingerichtet, die diese Planung allgemein vorbereiten soll. Nach Stand der Diskussion in dieser Arbeitsgruppe gibt es folgende Problembereiche, die einer umfangreichen Analyse, Bewertung und Planung bedürfen: Bisher fehlte in der bremischen Verwaltung die Erfahrung, um den Betrieb der neuen Netzstrukturen zu planen oder zu betreiben. Es ist unklar, ob die bisherigen Systeme für die Verwaltung eines solch hochkomplexen Netzes überhaupt ausreichend sicher gestaltet werden können. Die Kommunikationssicherheit kann in solch einem Netz nur durch Von-Ende-zu-Ende-

Verschlüsselung gewährleistet werden. Auch dies bedarf einer Sichtung der Konzepte und Produkte vor Einsatz und Betrieb.

Die Frage, inwieweit die Nutzungsberechtigten in ihrer Zugriffsberechtigung auf einzelne Systeme beschränkt werden sollen, wird von den Verantwortlichen für das ISA-Projekt und von mir unterschiedlich bewertet. Das Polizeipräsidium ist der Auffassung, daß es aufgrund der Aufgabenstellung jedem Polizeibeamten möglich sein muß, alle zur Verfügung stehenden Abfragemöglichkeiten wahrzunehmen. Ich konnte diese Aussage noch nicht bewerten, da es hierzu erforderlich ist, für alle angeschlossenen 42 Organisationseinheiten zu untersuchen, ob die Aufgabenstellung den Zugriff auf alle Systeme erfordert. Ich habe Zweifel, ob mit der angestrebten Lösung das Zweckbindungsprinzip eingehalten werden kann. Unabhängig davon ist ein Verfahren zu entwickeln, das die nachträgliche Kontrolle ermöglicht, ob die abgerufenen Informationen tatsächlich zur Aufgabenerfüllung erforderlich waren. Die technisch-organisatorischen Maßnahmen wie auch Inhalt, Umfang, Ordnung, Aufbewahrungsdauer etc. der Protokollierung bedürfen noch weiterer Erörterung.

Zusammenfassend ist festzustellen, daß für das geplante ISA-D-Verfahren die rechtlichen Voraussetzungen nur unzureichend vorliegen und die technischen und organisatorischen Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zur Zeit noch nicht klar erkennbar sind.

2.2.2.2 Datenverarbeitung beim Staatsschutz: APIS/ISA

Bereits im 11. und 12. Jahresbericht (S. 57/S. 11) hatte ich darauf hingewiesen, welche datenschutzrechtlichen Probleme dadurch entstehen, daß der Staatsschutz des Landes Bremen das bundesweite Informationssystem APIS als Aktennachweissystem für alle anfallenden Vorgänge nutzt. Im letzten Jahr sind erfreuliche Fortschritte in den Verhandlungen mit dem Senator für Inneres erreicht worden. So ist mir bestätigt worden, daß alle in meinem Prüfbericht zur Löschung empfohlenen Fälle in APIS gelöscht seien. Insbesondere soll meiner Empfehlung gefolgt werden, nur noch dann Straftaten in APIS zu speichern, wenn es sich um die typischen schweren Staatsschutzdelikte oder terroristischen Gewalttaten und die diesen vergleichbaren Straftaten mit politischem Hintergrund handelt. Alle anderen, insbesondere die Bagatellstraftaten, bei denen nur die politische Motivation Anlaß für die Verfolgung durch den Staatsschutz ist, sollen — soweit erforderlich — in dem landeseigenen Informationssystem ISA gespeichert werden. Im ISA-Datenbestand soll dem Staatsschutz ein Bereich eingeräumt werden, in den er seine Fälle einstellt und verwaltet. Diese Datenspeicherungen sollen in der Deliktsschlüsselnummer durch eine Zusatzkennung gegen den allgemeinen Zugriff anderer Polizeiabteilungen gesichert werden. Bei der Staatsschutzabteilung soll ein PC/Terminal mit eigenen Zugriffs- und Auskunftsmöglichkeiten für ISA eingerichtet werden. Die Staatsschutzdelikte bilden dann im ISA-Verfahren einen eigenen, nach außen abgeschlossenen Bereich, wobei aber möglich bleibt, alle Funktionen des ISA-Verfahrens zu nutzen, insbesondere auch die Übernahme des Verfahrensausganges bei der Staatsanwaltschaft aus CANASTA.

Bei meinen Beratungen habe ich Wert auf die Entwicklung eines Verfahrens gelegt, das sicherstellt, daß die in APIS eingestellten Fälle parallel zu dem ISA-Datenbestand gepflegt werden. Die Polizei ist bereit, dem Rechnung zu tragen. Schließlich ist mir ein Verfahren zur Vergabe von Löschfristen zur Prüfung vorgelegt worden. Im Zuge der ADV-Beratungen setze ich mich dafür ein, bei der PC-Beschaffung eine sichere und nicht überdimensionierte Lösung zu erzielen.

2.2.2.3 Speicherung von Daten jugendlicher Demonstranten

Im November 1989 waren 26 überwiegend jugendliche Personen von der Polizei festgenommen worden, 23 von ihnen wurden erkennungsdienstlich behandelt. Anlaß für die polizeilichen Maßnahmen waren Ausschreitungen und Sachbeschädigungen im Zuge einer Spontan-Demonstration in Bremen anläßlich des Todes einer Studentin, die während eines Polizeieinsatzes gegen eine Demonstration in Göttingen ums Leben gekommen war. Gegen die Jugendlichen wurde vom Staatsschutz wegen des Verdachts eines Verstoßes gegen § 125 StGB (Landfriedensbruch) ermittelt.

Als die Vorfälle durch Presseberichte bekannt wurden, habe ich mich sofort an das Stadt- und Polizeiamt (jetzt Polizeipräsidium) gewandt und um Aufklärung gebeten. Bereits im Januar 1990 wurde mir seitens der Polizei erklärt, daß zu-

nächst insgesamt zu 22 Personen in der Datei des Staatsschutzes (APIS) Speicherungen vorgenommen worden seien, inzwischen seien die Ermittlungen soweit gediehen, daß sich nur noch gegen zwei Personen ein Tatverdacht aufrecht erhalten lasse. In 20 Fällen sei daher die APIS-Speicherung gelöscht worden.

Ende August wandten sich 15 Jugendliche, zum Teil mit ihren Eltern, an mich und baten um eine Überprüfung der polizeilichen Datenverarbeitung in diesem Zusammenhang. Sie erklärten, am 23. Dezember 1989 hätten ihnen der Innensenator und der Polizeipräsident in einem persönlichen Gespräch versichert, daß bei Einstellung der Verfahren alle Beteiligten schriftlich über die Löschung der Daten informiert würden. Die Verfahren seien im März eingestellt worden, man habe aber bisher noch keinen Beleg über die Löschung der Daten erhalten.

Eine Prüfung im staatsanwaltschaftlichen Informationssystem CANASTA hat ergeben, daß die Ermittlungsverfahren gegen die Jugendlichen eingestellt worden sind. Meine Prüfungen bei der Polizei in ISA, INPOL, APIS und der ED-Kartei hatten folgendes Ergebnis: In APIS waren noch zwei vollständige Personendatensätze sowie im Text der Name eines weiteren Beteiligten gespeichert. Das Stadt- und Polizeiamt hat hierzu erklärt, daß die Daten dieser Personen, deren Löschung in APIS vergessen worden waren, inzwischen getilgt und zu den Personen auch keine Akten mehr vorhanden seien. Der ED-Stelle sind die Namen der erkennungsdienstlich behandelten Personen im sogenannten ED-Buch unter dem Datum der vorläufigen Festnahmen aufgeführt, gleichfalls werden die Negative noch vorhanden sein. Ich habe verlangt, auch hier eine Löschung durchzuführen.

Im übrigen teile ich die Einschätzung des Polizeipräsidiums nicht, rechtlich sei die frühzeitige Speicherung der Jugendlichen in APIS nicht zu beanstanden. Wenn bereits kurze Zeit nach Einspeicherung in APIS 20 von 22 Fällen wegen fehlender Verdachtsmomente wieder gelöscht werden, noch bevor die Verfahrensakten der Staatsanwaltschaft zugeleitet sind, erscheint zweifelhaft, ob die Frage des hinreichenden Tatverdachtes vor der Einspeicherung in APIS geprüft worden ist. Bereits in meinem 11. Jahresbericht (S. 57) hatte ich darauf hingewiesen, daß Fälle minderer Schwere nicht in APIS — auf das bundesweit zugegriffen werden kann — gespeichert werden dürfen. Gleiches gilt für Speicherungen zu einem Verfahrenszeitpunkt, in dem der Tatbeitrag eines Verdächtigen noch nicht ausreichend geklärt ist.

2.2.2.4 Erkennungsdienst

Bereits im 12. Jahresbericht (S. 13) habe ich über Datenschutzprobleme bei der Lichtbildvorzeigekartei berichtet. Der Datenschutzausschuß der Bremischen Bürgerschaft hat sich meiner zu diesem Komplex ausgesprochenen Beanstandung angeschlossen (vgl. Drs. 12/1139). Der Senator für Inneres hat zwar erklärt, daß die Vorzeigekartei — also die Kartei, aus der Bilder z. B. Zeugen vorgelegt werden — bereinigt worden sei. Die mit der Vorzeigekartei verbundenen strukturellen Probleme (vgl. a. a .O. S. 16) sind aber noch nicht gelöst. Weiterhin sind die gegenüber dem Senator für Inneres im Prüfbericht vom Januar 1990 aufgeführten Falschspeicherungen im Bereich von ISA und der Kriminalaktenführung bisher nicht bereinigt.

Aufgrund mehrerer Prüfungen von Eingaben von Bürgern, die erkennungsdienstlich behandelt wurden, haben sich neue Datenschutzprobleme im Bereich der ED-Karteikartensammlung gezeigt. Eine Überprüfung dieser Kartei, die 106.000 Personen umfaßt, ist vom Senator für Inneres nicht in Aussicht gestellt. Nur vergleichsweise sei darauf hingewiesen, daß in Hamburg mit einem gegenüber Bremen größeren Einzugsgebiet in der entsprechenden Kartei ca. 60.000 Personen gespeichert sind.

Bei der Prüfung der Bürgereingaben habe ich den Eindruck gewonnen, daß bereits sehr frühzeitig von Seiten der Polizei eine erkennungsdienstliche Behandlung (Lichtbild und Fingerabdruck) angeordnet wird, so z. B. bei Ladendiebstahl als Ersttat. Nach herrschender Meinung sollte eine erkennungsdienstliche Behandlung nur dann erfolgen, wenn es nach der Persönlichkeit des Beschuldigten und der Art seiner Tat naheliegt, daß er noch weitere Straftaten begangen hat oder begehen wird. Jedenfalls ist die von der Polizei getroffene Entscheidung augenscheinlich dann falsch, wenn nach mehreren Jahren die ED-behandelten Personen, bei denen häufig das Verfahren wegen der Ersttat eingestellt worden ist, nicht wieder strafrechtlich in Erscheinigung getreten sind.

Da der Gesetzgeber diesen Bereich bisher nicht präzise geregelt hat, empfehle ich, den Polizeibeamten mittels Richtlinien Hilfestellung zu geben, damit bei der Entscheidung über die erkennungsdienstliche Behandlung der Grundsatz der Verhältnismäßigkeit gewahrt bleibt. Die Polizeibeamten haben bei ihrer Entscheidung auch zu berücksichtigen, daß die erkennungsdienstliche Behandlung neben der Aufnahme in die bremische ED-Datei zwangsläufig eine Aufnahme in die INPOL-Datei beim Bundeskriminalamt nach sich zieht und damit die Daten des Verdächtigen bundesweit im Zugriff der Polizeien stehen.

Eine Ergänzung der bestehenden ED-Richtlinien ist jederzeit möglich. Hierzu bedarf es keiner bundesweiten Abstimmung. Bremen hat schon früher in den ED-Richtlinien wie auch in den KpS-Richtlinien eigenständige Regelungen ergänzt.

Eine eingeschränkte Praxis bei der Anordnung der ED-Behandlung würde für die Zukunft viele der Datenschutzprobleme in diesem Bereich lösen.

Weiterhin ist festzustellen, daß entgegen der Bestimmung von § 36 BremPolG vom Senator für Inneres als zuständiger Fachaufsichtsbehörde für die ED-Dateien bisher keine Feststellungsanordnung erlassen und im Amtsblatt veröffentlicht worden ist.

Auch hatte ich Anfang 1990 neben der Herausnahme von Lichtbildern aus der Vorzeigekartei in vielen Fällen die Löschung dieser Vorgänge in der Hauptkartei (ED-Karteikartensammlung) verlangt. Leider wurde diese Anregung in mehreren Fällen nicht befolgt, obwohl zu den genannten Personen weder eine Kriminalakte noch ein ISA-Eintrag besteht. Die Polizei hat hierzu erklärt, eine Löschung sei nicht erforderlich, weil die 10jährige Aufbewahrungsdauer nach den KpS-Richtlinien noch nicht abgelaufen sei. Ich kann dieses Argument nicht akzeptieren. Zu berücksichtigen ist nämlich, daß die Vorgänge, die die Aufnahme in die Lichtbildkartei begründenden Tatsachen enhalten, bereits vernichtet bzw. gelöscht worden sind. Eine Aufbewahrung der Kriminalakte oder der Eintrag in ISA wurde somit von der Polizei selbst weder aus präventiven noch aus repressiven Gründen für notwendig erachtet. Damit entfällt aber auch die Speicherbefugnis in der ED-Datei. Die KpS-Richtlinien zwingen nicht zu einer 10jährigen Aufbewahrung, im Zuge der Ermessensentscheidung ist vielmehr eine frühzeitige Löschung möglich. Von dieser Möglichkeit wurde beim ISA-Eintrag und bei der Kriminalakte Gebrauch gemacht. Ich kann daher nicht nachvollziehen, daß die gleichen Gründe nicht zu einer Löschung in der ED-Datei führen. Prinzipiell ist daher ein Verfahren zu entwickeln, das in solchen Fällen sowohl die Löschung in der ED-Datei sicherstellt als auch die Löschung der zugehörigen Daten in der INPOL-Datei anregt.

Weiterhin hatte ich in dem Prüfbericht die Löschung des Vermerks „homosexuell" verlangt, weil sich weder aus dem ISA-Eintrag noch aus der Kriminalakte deliktische homosexuelle Handlungen feststellen ließen. Im übrigen habe ich darauf hingewiesen, daß nicht die homosexuelle Neigung von Straftätern zu vermerken ist, sondern der Straftatbestand. Der Polizeipräsident hat demgegenüber erklärt, die Klassifizierung „homosexuell" werde als kriminologisch zu begründendes Unterscheidungsmerkmal in der Lichtbildvorzeigekartei als zulässig und erforderlich angesehen.

Nur durch Zufall fiel mir anläßlich einer Prüfung in der ED-Stelle ein Formular in die Hände, das dort bereits in großer Auflage vorlag und in nächster Zeit verwendet werden sollte. Das Formblatt war nicht mit mir abgestimmt und berücksichtigt erneut nicht die datenschutzrechtlichen Anforderungen, wie ich sie in meinem 12. Jahresbericht ausgeführt habe. So sieht das Formblatt u. a. folgende Kategorien vor: Schwerverbrecher, Totschläger (unter diese Kategorie sollen Delikte wie gefährliche und schwere Körperverletzung gefaßt werden), Fixer (unter diese Kategorie sollen Kleindealer und Abhängige gefaßt werden) sowie die Differenzierung von Straftätern aufgrund besonderer Merkmale, wie Obdachlose, Prostituierte und Homosexuelle. Weder die Obdachlosigkeit noch Prostitution oder Homosexualität sind per se strafbar. Wie bereits im letzten Jahresbericht ausgeführt, halte ich eine Stigmatisierung dieser Gruppen, ohne daß typische Straftaten, wie z. B. unerlaubte Prostitution (§ 184 a StGB) oder homosexuelle Handlungen (§ 175 StGB) als konkrete Straftaten im Hintergrund stehen, für unzulässig.

Ich habe daher den Senator für Inneres gebeten, die Verwendung des Formulars zurückzustellen, bis eine datenschutzrechtliche Beratung des Vordrucks erfolgt ist. Gleiches gilt für das bereits eingeführte „Wahllichtbildvorlegeverfahren".

Schließlich ist weiterhin ungelöst, daß unabhängig von einer vorzeitigen Vernichtung der Lichtbildabzüge die Negative in jedem Fall erst nach zehn Jahren ver-

nichtet werden. Da auch die ED-Bücher mindestens zehn Jahre aufbewahrt werden und erst vernichtet werden, wenn die Lagerkapazität erschöpft ist, ist eine Zusammenführung der Negative mit dem Namen trotz Löschung der ED-Unterlagen jederzeit möglich.

Ich hatte bereits im März 1990 meine Gesprächsbereitschaft zu allen Fragen im Zusammenhang mit den ED-Dateien erklärt. Auch der Vertreter des Senators für Inneres hat im Datenschutzausschuß vorgeschlagen, gemeinsam mit mir zu prüfen, wie weit meinen Anregungen aus der Sicht der Polizei gefolgt werden kann. Erörterungen der Probleme haben bisher nicht stattgefunden.

2.2.2.5 Kriminalpolizeiliche Aktenverwaltung

Bei Prüfungen mußte ich in den letzten Jahren wiederholt feststellen, daß die vorgeschriebenen Aussonderungs- und Löschfristen überschritten wurden. Mir wurde häufig entgegengehalten, daß dies auch damit zusammenhänge, daß in der Kriminalaktenverwaltung noch sehr viele Altvorgänge aufzuarbeiten seien. Ich habe mir deshalb ein Bild über die Bestände und die Probleme in den Kriminalaktenverwaltungen der Polizeibehörden in Bremen und Bremerhaven verschafft.

Nach Angaben der Kriminalaktenverwaltung beträgt der Bestand an Kriminalakten in **Bremen** (Stadt) zur Zeit ca. 98.000 Akten. Die Aufgabenstellung der dort beschäftigten Mitarbeiter beinhaltet das Anlegen von Kriminalakten, die Aussonderung der Akten, die Herausgabe von Akten für die Sachbearbeitung sowie die Zuordnung von Vorgängen. Darunter fallen auch die Meldungen der Staatsanwaltschaft über den Ausgang des Verfahrens. Nach Angaben der Polizei ist es aber mangels Personalkapazität nicht möglich, alle diese Vorgänge den Kriminalakten zuzuordnen; so ist bisher ein Bestand von 12.000 nicht zugeordneter Formulare über den Ausgang des Verfahrens entstanden. In einem Schreiben vom Februar 1990 teilte mir das Stadt- und Polizeiamt mit, daß in der Kriminalaktenverwaltung sogar noch 90.000 Vorgänge aufgearbeitet werden müssen.

Aufgrund dieser Rückstände ist davon auszugehen, daß viele Kriminalakten nicht den aktuellen Stand wiedergeben und darüber hinaus der Kriminalaktenbestand Akten umfaßt, die auszusondern wären. Zwar ist seit einiger Zeit durch die Verbindung des staatsanwaltschaftlichen Informationssystems (CANASTA) und des polizeilichen Informationssystems (ISA) gewährleistet, daß der Ausgang des Verfahrens in ISA eingetragen und dort ein Aussonderungsprüftermin nach KpS-Richtlinien eingetragen wird; es ist jedoch nicht davon auszugehen, daß der die Kriminalakte bearbeitende Sachbearbeiter in jedem Fall den Ausgang des Verfahrens in ISA überprüft, sondern sich auf die in den Kriminalakten festgehaltenen Vorgänge verläßt. Damit besteht die Gefahr, daß über die Betroffenen ein falsches Bild entsteht und die kriminalpolizeiliche Sachbearbeitung von falschen Voraussetzungen ausgeht.

Auf das Problem der Aussonderung angesprochen, wurde mir erklärt, daß bei jeder Herausgabe einer Kriminalakte nachgeprüft werde, ob diese zur Aussonderung ansteht. Soweit diese Prüfung konsequent durchgeführt werden kann, ist damit zwar verhindert, daß unrechtmäßig aufbewahrte Kriminalakten genutzt werden; jedoch stellt die unzulässige Speicherung an sich schon eine nicht hinzunehmende Beeinträchtigung der schutzwürdigen Belange der Betroffenen dar. Ein neuentwickeltes Löschfristenverfahren soll diese Probleme entschärfen. Ein noch so ausgeklügeltes automatisiertes Verfahren läuft aber immer dann fehl, wenn nicht gewährleistet ist, daß die damit erreichten Ergebnisse manuell — durch Aussonderung oder Aktualisierung der Kriminalakten — umgesetzt werden können.

In **Bremerhaven**, wo es derzeit ca. 30.000 Akten geben soll, stellt sich das Problem im Prinzip genauso dar. Zwar wird von dort versichert, daß es möglich sei, die durch das Löschfristenverfahren erstellten Listen der zur Aussonderung anstehenden Akten abzuarbeiten, dieses kann aber nur durch eine Vernachlässigung der Zuordnung der Verfahrensausgänge zu den Kriminalakten erreicht werden. Diese werden nach dortigen Angaben seit einigen Jahren überhaupt nicht mehr zugeordnet, so daß mehrere tausend dieser Formulare als Altbestand angefallen sind. Die Prioritätensetzung wird damit begründet, daß die Zuordnung der Verfahrensausgänge zu den Akten überflüssig sei, da jeder Sachbearbeiter gehalten sei, sich über den Ausgang des Verfahrens in ISA zu unterrichten. Da ich aber festgestellt habe, daß auch Meldungen über Verfahrensausgänge aus den Jahren 1984 bis 1987 noch nicht abgearbeitet waren und die oben dargestellte Verbindung ISA/CANASTA in Bremerhaven erst seit 1987 besteht, habe ich Zweifel, ob die

in ISA enthaltenen Datensätze den richtigen Stand wiedergeben. Hierzu hätten die Verfahrensausgänge gesondert erfaßt werden müssen. Das ist nicht geschehen, vielmehr wurde mir mitgeteilt, daß aufgrund der KpS-Höchstspeicherdauer von zehn Jahren sich diese Altlasten von allein erledigen würden. Dieser Logik kann ich nicht folgen, denn sobald ein neuer Fall dazugespeichert wird, verlängert sich die Löschfrist um weitere zehn Jahre. In diesen Fällen bringt auch das sogenannte Löschfristenverfahren keine datenschutzrechtliche Verbesserung. Damit ist zu befürchten, daß ohne eine gezielte Aufarbeitung von Altfällen weit über das Jahr 2000 löschungsreife Kriminalakten und Datenspeicherungen in ISA verbleiben.

Ich habe daher meine Absicht an den Senator für Inneres herangetragen, den ISA-Bestand strukturell nach löschungsreifen Vorgängen zu durchforsten.

Aufgrund meiner bisherigen Prüfergebnisse beabsichtige ich mit ADV-Unterstützung Prüfkriterien zu entwickeln für strukturell löschungsfähige Altbestände.

Leider stehen hierfür bisher keine Programme bereit. Auch konnte im Hause des Senators für Inneres bisher nicht geklärt werden, ob die Kosten für eine solche Programmierung, die sich nach Schätzungen im Bereich unter einem Menschmonat bewegen, getragen werden können. Einmal davon abgesehen, daß sich ein solcher Betrag gering ausnimmt gegenüber den Kosten für die Bewirtschaftung, Pflege etc. der Daten und Akten, bin ich der Auffassung, daß diese Kosten von der speichernden Stelle zu tragen sind.

2.2.2.6 Räumliche Verhältnisse im 6. Polizeirevier Bremen

Abgeordnete aus dem Datenschutzausschuß haben mich vor einem Jahr auf Datenschutzmißstände im 6. Polizeirevier hingewiesen und um meine Überprüfung gebeten. Bei einer Begehung des 6. Polizeireviers habe ich festgestellt, daß die Verhältnisse in dem Wachraum, bei der Strafanzeigenentgegennahme und bei der Bearbeitung von Ladendiebstählen durch den Bezirksdienst den datenschutzrechtlichen Anforderungen nicht entsprechen. Ich habe dies gegenüber dem Polizeipräsidium moniert.

Hinsichtlich der beiden letztgenannten Bereiche haben sich die Verhältnisse zwischenzeitlich gebessert. Nach wie vor bestehen jedoch datenschutzrechtliche Probleme im Zusammenhang mit den Verhältnissen im Wachraum: So kommt es häufig vor, daß gleichzeitig mehrere Bürger den wachhabenden Beamten ihre Sachverhalte schildern, während nachkommende Personen auf die Bearbeitung ihrer Angelegenheit warten und die Schilderungen mithören können. Gleichzeitig gehen in dem Wachraum Funksprüche ein, die häufig personenbezogene Daten enthalten. Im Wachraum werden auch Telefonate geführt, bei denen intensive Orts- und Sachaufklärung betrieben wird. Dabei fallen selbstverständlich auch Namen.

Eine Trennung des Funkraumes, des Publikumsbereichs und des Warteraumes wäre daher aus datenschutzrechtlicher Sicht unerläßlich. Als unabdingbare Maßnahme habe ich die akustische Abtrennung des Wachraums gefordert. Eine Stellungnahme des Senators für Inneres steht noch aus. Ich habe den Senator für Inneres an meinen Vorschlag erinnert.

2.2.2.7 Weitere Prüfungen von Eingaben bei den Polizeibehörden

Im vergangenen Berichtsjahr hat sich wiederum eine große Anzahl von Bürgern an mich gewandt mit der Bitte, die Verarbeitung ihrer Daten durch die Polizeibehörden zu prüfen. In den meisten Fällen konnte mit den Polizeibehörden Einigung über die weitere Behandlung dieser Daten erzielt werden; eine Reihe von Vorgängen wurde aufgrund meiner Überprüfung gelöscht.

In einigen Fällen konnte jedoch keine Einigung erzielt werden. So bin ich z. B. der Eingabe eines Homosexuellenverbandes nachgegangen, die sich dagegen richtete, daß die Bremer Polizei Informationen im Zusammenhang mit Homosexualität sammele.

Meine Überprüfung hat ergeben, daß aufgrund einer Anfrage der Staatsanwaltschaft Bonn die Kriminalpolizei Bremen dieser einen Zeitungsausschnitt aus dem Jahre 1985 übersandte, der auch den Namen eines Bremer Bürgers enthielt. In diesem Artikel wurde berichtet, daß der namentlich genannte Bremer Professor auf einer Gründungsversammlung des Verbandes ein Referat gehalten habe. Auch

wenn der Zeitungsartikel einer öffentlichen Quelle entnommen wurde, habe ich gleichwohl gegen die Speicherung und Übermittlung der personenbezogenen Daten durch die Kripo datenschutzrechtliche Bedenken erhoben. Nach den Vorschriften der StPO sind derartige Maßnahmen zulässig, wenn ein Anfangsverdacht einer strafbaren Handlung vorliegt, nach den Vorschriften des bremischen Polizeigesetzes ist eine Datenverarbeitung nur zu Zwecken der Gefahrenabwehr und vorbeugenden Straftatenbekämpfung zulässig. Keine der Voraussetzungen lag zum Zeitpunkt der Erhebung und Speicherung des Zeitungsartikels vor. Zum gleichen Ergebnis führt auch das geltende Bremische Datenschutzgesetz, nach § 11 BrDSG ist das Speichern personenbezogener Daten nur zulässig, wenn es zur rechtmäßigen Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist. Ich habe daher die Kriminalpolizei aufgefordert, gem. § 20 Abs. 3 BrDSG den Vorgang zu löschen.

Das Stadt- und Polizeiamt Bremen ist dieser Forderung nicht nachgekommen. Zur Begründung hat es ausgeführt, der umstrittene Artikel enthalte keine personenbezogenen Informationen, im übrigen sei für ein Fachkommissariat in jedem Fall notwendig zu wissen, wer in bestimmten Fällen ggf. Ansprechpartner sein könne; dies habe nichts mit einer Verfolgung einer bestimmten Personengruppe zu tun. Solchen Ausführungen kann man einfach nichts mehr hinzufügen.

2.2.3 Meldewesen

2.2.3.1 EDAS-/DEMOS-Verfahren in Bremen

Die Ablösung des technisch veralteten und nicht dem geltenden Melderecht entsprechenden EDAS-Verfahrens durch das neue DEMOS- Verfahren (DEMOS = **D**ezentrales **E**inwohner-**M**elde-**o**nline-**S**ystem), die vom Senator für Inneres für das Jahr 1990 zugesagt war, ist bis heute nicht erfolgt. Die gesetzliche Anpassungsfrist war 1990 um drei Jahre überschritten.

Auch der Datenschutzausschuß der Bremischen Bürgerschaft hat mehrfach mißbilligt, daß entgegen § 38 Abs. 4 Meldegesetz das Verfahren der automatisiert geführten Melderegister immer noch nicht vollständig den Anforderungen des Meldegesetzes angepaßt worden ist. Mir ist es unverständlich, daß es einer Verwaltung nicht gelingt, in einem Zeitraum von mehr als acht Jahren bis heute gerechnet ein großes zentrales Datenverarbeitungsverfahren dem neuen Recht und den aktuellen systemtechnischen Erfordernissen anzupassen.

Da nicht absehbar ist, wann das veraltete EDAS-Verfahren durch das neue DEMOS-Verfahren ersetzt wird, habe ich vom Senator für Inneres gefordert, zu prüfen, ob nicht durch eine Anpassung des alten EDAS-Verfahrens ein rechtskonformer Zustand erreicht werden kann.

2.2.3.2 Meldedatenübermittlungsverordnung des Landes

In meinem letzten Tätigkeitsbericht hatte ich über beabsichtigte Änderungen der Bremischen Meldedatenübermittlungsverordnung (S. 187) berichtet, die neugefaßte Meldedatenübermittlungsverordnung ist Mitte des Berichtsjahres in der Fassung vom 09.06.1990 (BrGbl. S. 175) in Kraft getreten.

2.2.3.3 Suchvermerk im Melderegister

Sind Personen unter der im Bremer Melderegister eingetragenen Anschrift nicht mehr antreffbar, können öffentliche Stellen gem. § 3 Abs. 2 Nr. 7 Meldegesetz für zwei Jahre einen Suchvermerk im Melderegister eintragen lassen. Wird innerhalb dieses Zeitraumes eine neue Anschrift zu dieser Person bekannt, wird die öffentliche Stelle hiervon durch die Meldebehörde benachrichtigt. In der Praxis wird zum Datensatz der Person ein „SU", der Name und das Aktenzeichen der suchenden Behörde gespeichert.

Eine Prüfung der Meldebehörde hat ergeben, daß die gesetzlich vorgesehene Zwei-Jahres-Frist bisher nicht beachtet wurde. Da ein automatisiertes Löschverfahren nicht vorgesehen ist, ist übergangsweise verabredet worden, auch das Löschdatum des Suchvermerks mit aufzunehmen und per Dienstanweisung die Löschpflicht hervorzuheben. Bei der Prüfung mußte ich weiter feststellen, daß die Meldestelle zwar den Eintrag der suchenden Behörde löschen konnte, es gelang ihr aber nicht das „SU" zu löschen. Damit bleibt bisher über Jahre die Information zu einer Person bestehen, daß zu ihr einmal ein Suchauftrag bestanden hat. Die Meldebehörde hat mir zugesagt, dieses technische Problem mit dem RbV zu klären.

2.2.4 Straßenverkehrsangelegenheiten

Aufbewahrungsfristen von Verkehrsordnungswidrigkeitsunterlagen

Bereits im letzten Jahr habe ich gefordert, die von den Bußgeldstellen im Lande Bremen praktizierten Aufbewahrungsfristen von Verkehrsordnungswidrigkeitsunterlagen zu verkürzen, da diese zu lang und mit datenschutzrechtlichen Bestimmungen nicht zu vereinbaren seien. Zu der Verkürzung ist es bislang nicht gekommen. Die Aufbewahrungsfristen der Bußgeldakten betragen nach wie vor drei Jahre bei Ordnungswidrigkeiten, die mit einer Geldbuße unter 200 DM, und fünf Jahre bei Ordnungswidrigkeiten, die mit einer Geldbuße ab 200 DM belegt worden sind.

Zur Begründung verweist der Senator für Inneres auf § 30 Abs. 2 des Straßenverkehrsgesetzes (StVG), wonach das Kraftfahrt-Bundesamt Auskünfte aus dem Verkehrszentralregister an die auskunftsberechtigten Stellen so zu erteilen habe, daß die Akten über die den Eintragungen zugrundeliegenden Entscheidungen beigezogen werden können. Dies setze voraus, daß die Akten bei den auskunftsberechtigten Stellen, u. a. den Bußgeldstellen, vorhanden und nicht bereits vernichtet seien. Die Aufbewahrungsfristen der Bußgeldakten müßten deshalb der in § 13 a Abs. 3 Satz 2 der Straßenverkehrszulassungsordnung (StVZO) festgelegten Tilgungsfrist für Eintragungen im Verkehrszentralregister (fünf Jahre bei vorangegangener Hemmung der Tilgung infolge weiterer Eintragung) entsprechen. Sollen die Aufbewahrungsfristen verkürzt werden, so sei dies nur durch die Änderung der vom Bund erlassenen Verkehrsvorschriften möglich.

Dieser Auffassung kann ich mich nicht anschließen. Gemäß § 13 StVZO werden in das Verkehrszentralregister rechtskräftige Entscheidungen wegen einer Verkehrsordnungswidrigkeit nur eingetragen, wenn gegen den Betroffenen ein Fahrverbot angeordnet oder eine Geldbuße mit einem Regelsatz von mindestens DM 80,— festgesetzt wurde. Die Tilgungsfrist für derartige Eintragungen beträgt gemäß § 13 a Abs. 2 Nr. 1 StVZO grundsätzlich zwei Jahre. Nur wenn es während dieser zwei Jahre zu weiteren Eintragungen kommt, hindert dies gemäß § 13 a Abs. 3 StVZO die Tilgung der Daten des Betroffenen. Unterlagen über Verkehrsordnungswidrigkeiten, bei denen es nicht zu einer Eintragung im Verkehrszentralregister kommt, sollten so schnell wie möglich, d. h. spätestens sechs Monate nach Rechtskraft der Bußgeldentscheidung von den örtlichen Verkehrsbehörden vernichtet werden. Dies habe ich dem Senator für Inneres entsprechend mitgeteilt.

Der Senator für Inneres sagte zu, den Entwurf eines Erlaßes zur Neuregelung der Aufbewahrungsfristen von Bußgeldakten vorzulegen.

2.2.5 Amtliche Statistik

2.2.5.1 Landesstatistikgesetz

In meinem 12. Jahresbericht (S. 22) wies ich darauf hin, daß § 11 Landesstatistikgesetz (LStatG) noch durch Verwaltungsvorschriften ergänzt werden müsse. Der Senator für Inneres hat sich (— wie vom Datenschutzausschuß gefordert—) mittlerweile zum Erlaß derartiger Verwaltungsvorschriften bereit erklärt und einen Entwurf vorgelegt, in dem die aus meiner Sicht notwendigen Hinweise enthalten sind. Außerdem hat der Senator für Inneres ein Rundschreiben an die einzelnen Ressorts herausgegeben, in dem er zu einer § 11 LStatG entsprechenden Erstellung der Geschäftsstatistiken auffordert.

2.2.5.2 Hochschulstatistikgesetz

Im letzten Tätigkeitsbericht (S. 24) habe ich über die geplante Novellierung des Hochschulstatistikgesetzes berichtet. Im November 1990 ist das vollständig neu gefaßte Hochschulstatistikgesetz verabschiedet worden.

Das neugefaßte Hochschulstatistikgesetz trägt vielen Anregungen und Bedenken datenschutzrechtlicher Art Rechnung. Für die Hochschulstatistik besteht weiterhin — bis auf die wieder eingeführte Abiturienten-Befragung, die auf freiwilliger Grundlage erfolgen soll — Auskunftspflicht. Auskunftspflichtig sind nach der Neufassung des Hochschulstatistikgesetzes die Leiter der jeweiligen Einrichtungen, z. B. Hochschulen, Studentenwerke, nicht mehr die Betroffenen selbst

(Umstellung von einer Primärstatistik auf eine Sekundärstatistik). Die Auskunftspflicht kann sich bei einer sekundärstatistischen Erhebung nach meiner Auffassung immer nur auf solche Merkmale beziehen, die den Auskunftspflichtigen für ihre rechtmäßige Aufgabenerfüllung zur Verfügung stehen. Das Hochschulstatistikgesetz kann den durch Rahmenrecht des Bundes und durch Landesrecht abgesteckten Aufgabenkreis der Hochschulen und Studentenwerke nicht erweitern mit der Folge etwa, daß unter Hinweis auf die amtliche Statistik zusätzliche Daten bei oder über Betroffene erhoben werden.

Das neue Hochschulstatistikgesetz tritt allerdings erst am 01. Juni 1992 in Kraft, bis dahin gilt das alte, den datenschutzrechtlichen Anforderungen nicht mehr genügende Hochschulstatistikgesetz aus dem Jahre 1980. Der Vollzug dieses alten Hochschulstatistikgesetzes muß in der Übergangszeit bis Mai 1992 den datenschutzrechtlichen Anforderungen genügen, die das Bundesverfassungsgericht in seinem Volkszählungsurteil aufgestellt hat. Es sollte daher schon berücksichtigt werden, was der Bundesgesetzgeber in seiner Neufassung als Datenschutzverbesserung aufgenommen hat, z. B. Verzicht auf die Verlaufsstatistik, Anpassung der Erhebungsmerkmale, eindeutige Trennung der Datenverarbeitungsvorgänge zwischen Hochschulverwaltung und amtlicher Statistik bzw. Trennung von Verwaltung und Statistik.

Der bremische Gesetzgeber hat im Jahre 1988 das Hochschulgesetz des Landes geändert und dabei einen neuen § 44 a „Datenverarbeitung" in das Gesetz eingefügt. Hierüber habe ich in meinem 11. Jahresbericht (S. 9) berichtet. Meine Vorschläge, umfassende bereichsspezifische Datenschutzregelungen für die Hochschulen des Landes zu schaffen, wurden nicht aufgegriffen. § 44 a Bremisches Hochschulgesetz ermächtigt den Senator für Bildung, Wissenschaft und Kunst jedoch, durch Rechtsverordnung die von Studienbewerbern, Studenten und Prüfungskandidaten anzugebenden Daten und ihre Verarbeitungszwecke zu bestimmen. Diese Rechtsverordnung ist noch nicht erlassen. Ich rege an, diese Rechtsverordnung bis spätestens Mai 1992 zu erlassen und dabei nochmals die Frage nach Schaffung bereichsspezifischer Datenschutzregelungen im Bremischen Hochschulgesetz zu prüfen.

2.2.5.3 Mikrozensusgesetz

Am 01. Januar 1991 ist das neue Mikrozensusgesetz in Kraft getreten. Über dieses Gesetzesvorhaben hatte ich in meinem letzten Jahresbericht (S. 23) berichtet. Bei geringfügigen datenschutzrechtlichen Verbesserungen (z. B. Ausdehnung der freiwilligen Datenabfragen, Wegfall der sogenannten Wohnungserhebung) ist das alte Gesetz im wesentlichen fortgeschrieben worden. Im Hinblick auf den Wegfall der Wohnungserhebung bleibt abzuwarten, ob der neu gewählte Bundestag die Überlegungen zu einem eigenständigen Gebäude- und Wohnungsstichprobengesetz wieder aufgreift.

2.2.6 Ausländerangelegenheiten

2.2.6.1 Das neue Ausländergesetz

Mit dem Gesetz zur Neuregelung des Ausländerrechts vom 09. Juli 1990 (BGBl. I, S. 1354) wurde am 01. Januar 1991 auch das Ausländergesetz (Art. 1) in Kraft gesetzt. Dieses Gesetz löst das aus dem Jahre 1965 stammende Ausländergesetz ab. Zu dem Gesetzentwurf der Bundesregierung habe ich kritisch Stellung genommen (vgl. 12. Jahresbericht S. 27).

Während der parlamentarischen Beratung sind zwar einige Kritikpunkte berücksichtigt worden, aber insgesamt begegnen tragende Vorschriften des Gesetzes erheblichen datenschutzrechtlichen und verfassungsrechtlichen Bedenken. Sie beziehen sich insbesondere auf:

- die Datenübermittlungspflichten der öffentlichen Stellen (§ 76),
- die Datenerhebung und -speicherung (§ 75) und
- die Durchbrechungen des Sozialgeheimnisses, des Steuergeheimnisses und anderer Berufsgeheimnisse (§ 77).

§ 76 Abs. 1 des Gesetzes berechtigt die Ausländerbehörden, Ersuchen um Auskünfte an alle öffentlichen Stellen zu richten. Diese sind daraufhin ihrerseits verpflichtet, alle ihnen bekanntgewordenen Umstände zu übermitteln, ohne daß ihnen ein eigenes Prüfungsrecht zur Erforderlichkeit der abverlangten Angaben zusteht.

Problematisch ist auch der von Gesetz gewählte Begriff „Umstände", der nicht normenklar ausdrückt, welche personenbezogenen Daten zu übermitteln sind, so daß die Gefahr schrankenloser Datenübermittlung besteht.

§ 76 Abs. 2 des Ausländergesetzes schreibt vor, daß alle öffentlichen Stellen verpflichtet sind, von sich aus ihnen bekanntgewordene Daten an die Ausländerbehörde mitzuteilen, wenn der Ausländer nicht die erforderliche Aufenthaltsgenehmigung oder Duldung besitzt, gegen eine räumliche Aufenthaltsbeschränkung verstößt oder wenn ein sonstiger Ausweisungsgrund vorliegt.

Dieser Meldepflicht unterliegen neben Behörden (z. B. Schulen, Gesundheitsbehörden, Arbeitsämter, Sozialämter, Postämter, kommunale Kindergärten) auch die Körperschaften und Anstalten des öffentlichen Rechts (z. B. öffentlich-rechtliche Krankenkassen, Arbeitnehmerkammer), die beliehenen Unternehmer (z. B. Schornsteinfeger und die amtlich anerkannten Sachverständigen des TÜV) sowie unabhängige Träger öffentlicher Ämter (z. B. Notare). Dadurch werden fast alle Lebensbereiche berührt, in denen Daten über Ausländer anfallen. Besonders kritisch zu bewerten sind die Meldepflichten der öffentlichen Stellen, bei denen Ausländer um Rat und Hilfe nachsuchen. Dies sind z. B. Sozialämter, die anders als vorher, jede Gewährung von Sozialhilfe sofort der Ausländerbehörde melden müssen. Vergleichbare Meldepflichten gelten auch für Drogenberatungsstellen und Schulärzte.

Ja sogar für die Ausländerbeauftragte des Landes Bremen gelten derartige Melde- und Auskunftspflichten. Sie ist — nach § 76 Abs. 3 verpflichtet, auf Ersuchen der Ausländerbehörde ihr bekanntgewordene Umstände mitzuteilen. Darüber hinaus ist sie verpflichtet, von sich aus Kenntnisse über Ausländer, die gegen eine räumliche Aufenthaltsbeschränkung verstoßen oder deren Aufenthaltsgenehmigung abgelaufen ist, der Ausländerbehörde unverzüglich zu melden.

Die öffentlichen Stellen haben aber, wie oben ausgeführt, auch zu melden, wenn sie Kenntnis von Sachverhalten haben, die einen Ausweisungsgrund darstellen (§§ 45 und 46). Danach stellt neben anderen die Gefährdung der öffentlichen Sicherheit und Ordnung einen Ausweisungsgrund dar. Der verfassungsrechtlich ohnehin umstrittene Begriff „öffentliche Ordnung" ist durch einen Beispielkatalog ausgefüllt, demzufolge bereits ein Ausweisungsgrund vorliegt, wenn der Ausländer mehrfach oder nicht nur geringfügig gegen Rechtsvorschriften bzw. gegen gerichtliche oder behördliche Verfügungen verstößt. Ein solcher meldepflichtiger Verstoß ist z. B. erfüllt, wenn im Wiederholungsfalle gegen die Schulpflicht, gegen Bestimmungen des Arbeitserlaubnisrechts oder gegen Straßenverkehrsbestimmungen verstoßen wurde.

Bestimmte Behörden wie die Meldebehörden, die Polizei, die Arbeitsämter, die Sozial- und Jugendämter und die Justizbehörden sind darüberhinaus zu sog. regelmäßigen Datenübermittlungen verpflichtet, deren Umfang nach § 76 Abs. 5 durch eine Rechtsverordnung festgelegt werden soll. Diese Bestimmung begegnet verfassungsrechtlichen Bedenken, da die Ermächtigungnorm selbst nicht ausreichend konkret die vorgesehenen Datenübermittlungsfälle festlegt.

Die angesprochenen Datenübermittlungsregelungen sind unverhältnismäßig und nicht normenklar, da z. B. Datenübermittlungen erfolgen sollen, die für eine konkrete ausländerbehördliche Maßnahme nicht verwendet werden können oder dürfen. So darf z. B. ein anerkannter Asylberechtigter grundsätzlich nicht ausgewiesen werden. Entsprechendes gilt für den Fall, daß eine Aufenthaltsverfestigung eingetreten ist, die eine ausländerrechtliche Maßnahme nicht mehr erlaubt. Die übermittelten Daten werden in diesen Fällen somit auf Vorrat gespeichert. Nicht normenklar sind die Regelungen, da der Betroffene nicht erkennen kann, welche Stelle welche Daten für welche Zwecke übermitteln darf.

Des weiteren richten sich meine Bedenken gegen die weitgehende Durchbrechung des Sozialgeheimnisses, des Steuergeheimnisses und anderer Berufgeheimnisse.

So wurde § 71 SGB X dahingehend geändert, daß der Katalog der übermittlungsfähigen Daten, die dem Sozialgeheimnis unterliegen, für Datenübermittlungen an Ausländerbehörden unverhältnismäßig erweitert wurde (siehe Art. 8 des Gesetzes zur Neuregelung des Ausländerrechts). Ebenso ist die Steuerbehörde befugt, Daten, die dem Steuergeheimnis unterliegen, an die Ausländerbehörde zu übermitteln, wenn der Ausländer gegen eine Steuervorschrift verstoßen hat.

Noch gravierender sind die Durchbrechungen von Berufsgeheimnissen, die unter den Schutz des § 203 StGB fallen. Dieses betrifft z. B. Ärzte, Berufspsychologen

oder beschäftigte Personen in Schwangerschaftsberatungsstellen. Danach dürfen diese Geheimnisse in bestimmten Fällen durch eine öffentliche Stelle gegenüber der Ausländerbehörde offenbart werden, auch wenn diese die Kenntnis von einer schweigepflichtigen Person aufgrund einer anderen Rechtsvorschrift erhalten hat.

Kritisiert habe ich auch die Regelungen über die Datenerhebung. Eine generalklauselartige Erhebungsvorschrift erlaubt den Ausländerbehörden, fast jedes Datum zu sammeln. Die Ausländerbehörden bestimmen selbst, welche Daten für ihre Aufgabe erforderlich sind.

Zusammenfassend läßt sich sagen, daß durch die weitgefaßten Datenerhebungs- und -speicherungsbefugnisse sowie durch die vorgesehenen Datenströme von anderen öffentlichen Stellen (z. T. mehrfach) die Ausländerbehörden ein umfassendes Bild über ausländische Mitbürger erhalten, die damit für die Ausländerbehörde zu einem „gläsernen Menschen" werden. Dies ist mit dem durch die Verfassung garantierten Recht auf informationelle Selbstbestimmung nicht zu vereinbaren.

Nach dem Gesetz findet das Ausländergesetz auf EG-Ausländer nur Anwendung, soweit das Europäische Gemeinschaftsrecht und das Aufenthaltsgesetz/EWG keine abweichenden Bestimmungen enthalten, ich habe Zweifel, ob diese Vorschriften des Ausländergesetzes die in Art. 8 der Europäischen Menschenrechtskonvention garantierte Achtung der Privatsphäre und das Diskriminierungsverbot nach Art. 7 EWG-Vertrag hinreichend berücksichtigen. Folgt man dem aus Art. 7 und Art. 48 EWG-Vertrag resultierenden Grundsatz so sind EG-Bürger, die von ihrem Recht auf Freizügigkeit Gebrauch machen, grundsätzlich Deutschen gleichzustellen. Ausnahmen sind nur bei einer schweren Gefährdung des Mitgliedstaates erlaubt.

Die Bundesregierung hat es als ihr Ziel erklärt, dem Ausländer die Möglichkeit zur Integration zu verschaffen. Ich befürchte jedoch, daß Menschen, die einer dauernden und umfassenden Überwachung unterliegen, sich nicht in eine für sie feindlich erscheinende Gesellschaft integrieren. Es ist vielmehr zu befürchten, daß bei den Betroffenen Ängste entstehen, die zu einer Segregation der Ausländer oder zu einem angepaßten Verhalten führen.

2.2.6.2 Ausländerdateienverordnung

Mit dem Ausländergesetz ist am 01. 01. 1991 auch die vom Bundesminister des Inneren erlassene Verordnung über die Führung von Ausländerdateien durch die Ausländerbehörden und die Auslandsvertretungen (Ausländerdateienverordnung) vom 18. Dezember 1990 in Kraft getreten. Dieser Verordnung begegnen gleichermaßen erhebliche datenschutzrechtliche Bedenken. Die Ausländerdateienverordnung geht in ihrem Regelungscharakter weit über den Ermächtigungsrahmen hinaus. Denn die Ausländerdateienverordnung regelt die Einrichtung von Dateien bei den Ausländerbehörden und den Auslandsvertretungen, die nach dem Ausländergesetz nicht vorgesehen sind. Dieses betrifft die Ausländerdatei B und die Visaversagungsdatei. Ebenso sind die vorgesehenen Löschungsfristen insgesamt zu lang und damit unverhältnismäßig. Ich vermag z. B. nicht zu erkennen, welche Gründe dafür maßgeblich sind, die Daten eines verstorbenen Ausländers noch 5 Jahre oder eines fortgezogenen Ausländers noch 10 Jahre zu speichern.

2.2.6.3 Ausländerdatenübermittlungsverordnung

Mit dem Ausländergesetz ist am 01. 01. 1991 auch die vom Bundesminister des Inneren erlassene Verordnung über Datenübermittlungen an die Ausländerbehörden vom 18. Dezember 1990 auf der Grundlage des § 76 Abs. 5 Ausländergesetz in Kraft getreten. Die Ausländerdatenübermittlungsverordnung steht im datenschutzrechtlich bedenklichen Kontext des Ausländergesetzes. Die Datenübermittlungsverordnung verstößt gegen den verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit, denn es werden Datenübermittlungen angeordnet, die in der Mehrzahl der Fälle keine ausländerrechtliche Maßnahme begründen. Diese gespeicherten Daten dienen allein der lückenlosen und verknüpften Überwachung der ausländischen Mitbürger im Brennpunkt der Ausländerbehörde ohne Rücksicht auf ihren aufenthaltsrechtlichen Status. Darüber hinaus regelt die Ausländerdatenübermittlungsverordnung Rechtsbereiche, die von der Ermächtigungsnorm nicht abgedeckt sind.

2.2.6.4 Anschluß der Ausländerbehörde an das Ausländerzentralregister

Im Zusammenhang mit dem Umzug der bremischen Ausländerbehörde beantragte der Senator für Inneres einen Direktanschluß der Ausländerbehörde an das Ausländerzentralregister zur Verbesserung des Auskunftsverfahrens. Diesem Antrag habe ich aus datenschutzrechtlichen Gründen meine Zustimmung verweigert, da keine verfassungskonforme Datenübermittlungsregelung besteht. Ein geplantes Ausländerzentralregistergesetz, das derartige Datenübermittlungsregelungen vorsah (zur Kritik vgl. meinen 12. Jahresbericht, S. 27), wurde in der letzten Legislaturperiode vom Deutschen Bundestag nicht verabschiedet. Ohne neue Rechtsgrundlage dürfen die Ausländerbehörden keine neuen Abruf- und Datenübermittlungsverfahren einrichten. Nur die Fortführung des bisherigen Telex-Auskunftsverfahrens ist zulässig.

2.2.7 Feuerwehr

Bremisches Brandschutzgesetz

Im Berichtsjahr hat mir der Senator für Inneres Entwürfe zu einem Gesetz über den Brandschutz und die Hilfeleistung der Feuerwehren im Lande Bremen (Brandschutzgesetz) vorgelegt.

Ich habe auf die Notwendigkeit der normenklaren Beschreibung der vielfältigen Aufgaben und der erforderlichen Befugnisse hingewiesen und daran anknüpfend bereichsspezifische Datenschutzregelungen gefordert.

Es war daher zu regeln, welche Stellen für welchen Zweck in welchem Umfang personenbezogene Daten verarbeiten dürfen. Insbesondere habe ich angeregt, Vorschriften aufzunehmen, aus denen klar erkennbar ist, welche Maßnahmen beim vorbeugenden Brandschutz, bei den Brandverhütungsschauen und bei Feuerschutzübungen zu ergreifen sind.

Die Daten, die die Feuerwehr bei Brandbekämpfung und bei der Rettung benötigt, sollten grundsätzlich getrennt von den Daten, die bei sog. subsidiären Aufgaben der Feuerwehr anfallen, verarbeitet werden. Diese subsidiären Aufgaben sind neben dem vorbeugenden Brandschutz, den Brandverhütungsschauen und den Feuerschutzübungen insbesondere die Aufgaben der Berufsfeuerwehr in den bremischen Häfen nach dem Hafengesetz und beim Gefahrgutumschlag. Ein weiteres Problem war eine klare Abgrenzung der Zuständigkeiten von Landesfeuerwehrbehörde, der Gemeinden, der Berufsfeuerwehr, den Freiwilligen Feuerwehren und den Pflichtfeuerwehren.

Meine Vorschläge bezogen sich ferner auf Regelungen zur Datenverarbeitung, Zweckbindung und zum automatisierten Abrufverfahren.

Ende Dezember 1990 hat der Senator für Inneres einen geänderten Gesetzentwurf vorgelegt, der im wesentlichen meinen Anforderungen entspricht.

2.2.8 Veranstaltungsbüro Bremen

Der Senat hat Ende 1988 beschlossen, beim Senator für Inneres ein „Bremer Veranstaltungsbüro" einzurichten. Diese Einrichtung sollte folgende Aufgaben abdecken:

- Aufbau und Betreuung einer Informationsbörse unter Einsatz von EDV
- Öffentlichkeitsarbeit
- kurz- und langfristige Vorplanungen von Veranstaltungsschwerpunkten
- Regulierung des Antragsverfahrens für Veranstaltungen auf öffentlichen Plätzen und Straßen
- Einrichtung einer ressortübergreifenden Arbeitsgruppe „Freizeitpolitik"

Erst Ende 1990 wurde ich über das Vorhaben unterrichtet. Ich habe das Projekt dahingehend beraten, daß die Erhebungen, Verarbeitungen und Nutzungen von Daten für Aufgaben der Ortspolizeibehörde oder anderer Ordnungsbehörden nach dem Versammlungsgesetz, dem Landesstraßengesetz, der Straßenverkehrsordnung, der Landesbauordnung u. a. nur im Rahmen der Zweckbindung dieser Gesetze erfolgen dürfen und nicht für Aufgaben einer „Informationsbörse" ver-

wendet werden dürfen. Daraufhin hat das Veranstaltungsbüro die Konzeption entsprechend geändert und im übrigen zugesagt, daß Datenerhebungen und -verarbeitungen nur mit Zustimmung der Betroffenen erfolgen und die Daten nach Terminablauf der Veranstaltung unverzüglich anonymisiert bzw. gelöscht werden.

2.3 Justiz und Verfassung

2.3.1 Gesetzentwurf zur Bekämpfung organisierter Kriminalität

Die Landesregierungen von Bayern und Baden-Württemberg initiierten einen Gesetzentwurf des Bundesrates zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG) (BT-Drs. 11/7663). Die Forderung, organisierte Kriminalität — insbesondere den illegalen Rauschgifthandel — zu bekämpfen, stößt bei der Bevölkerung auf breite Zustimmung. Deshalb wird von der Öffentlichkeit auch solchen Vorschlägen viel Verständnis entgegengebracht, die den Strafverfolgungsorganen, insbesondere Staatsanwaltschaft und Polizei, weitergehende Befugnisse als bisher zur Verfolgung dieser Straftaten an die Hand geben wollen.

Das gesetzgeberische Vorhaben des OrgKG beschränkte sich aber nicht auf die schwerwiegenden Erscheinungsformen der organisierten Kriminalität, sondern hinter dem klangvollem Namen des Gesetzes verbarg sich der Versuch, über den Bundesrat, vorbei an der stockenden Novellierung der Strafprozeßordnung, besondere Fahndungs- und geheime Ermittlungsmethoden wie den Einsatz verdeckter Ermittler, heimliche Film- und Tonaufnahmen oder Rasterfahndung breit angelegt einzuführen und sich dabei nicht auf die mit dem Gesetzestitel benannten Bereiche zu konzentrieren. Einzig das Land Bremen hat im Bundesrat dem Gesetzentwurf nicht zugestimmt (vgl. Sitzungsprotokoll des Bundesrates vom 11. 05. 1990, S. 247).

Auch in der von der Presse sensibilisierten Öffentlichkeit wurde von vielen Seiten Kritik an dem Gesetzentwurf geübt. Die Datenschutzbeauftragten von Bund und Ländern trafen sich zu einer Sonderkonferenz, um ihre Bedenken zu formulieren (Konferenzbeschluß vgl. Anlage 3). Zwar ist nicht zu verkennen, daß bei bestimmten Erscheinungsformen von Kriminalität besondere Ermittlungsmethoden erforderlich sein können, auch mochte speziell zur Bekämpfung der organisierten Kriminalität besondere Eile geboten sein, doch der vorgelegte Entwurf ging weit über das erklärte Ziel hinaus, weil geheime, tief in die Privatsphäre der Bürger eingreifende Fahndungs- und Ermittlungsmethoden allgemein im Strafverfahrensrecht verankert werden sollten.

- So versucht der Gesetzentwurf nicht den Begriff der organisierten Kriminalität zu umschreiben, sondern es wurde der konturlose Begriff „Straftaten von erheblicher Bedeutung" verwendet.
- Der Entwurf sollte die Rasterfahndung für eine Vielzahl von Delikten außerhalb der organisierten Kriminalität ermöglichen, indem die Anwendung „auf dem Gebiet des Staatsschutzes" ebenso zugelassen werden sollte wie für alle Delikte, die „gewerbs- oder gewohnheitsmäßig" begangen werden. Auf diese Weise wären auch Fälle kleinerer Kriminalität von gewisser Häufigkeit betroffen.
- Nach dem Entwurf hätten sich Verfolgungs- und Ermittlungsmaßnahmen gegen Personen richten können, die nicht Beschuldigte oder Verdächtige sind. So sollten ohne Wissen der Betroffenen „Lichtbilder und Bildaufzeichnungen hergestellt sowie besondere Sichthilfen" und „sonstige besondere für Observationszwecke bestimmte technische Mittel" eingesetzt werden sowie „das nicht öffentlich gesprochene Wort mit technischen Mitteln abgehört und aufgezeichnet werden". Das hätte bedeutet, daß gegen diesen Personenkreis gezielt z. B. Wanzen, Richtmikrofone hätten eingesetzt und Videoaufzeichnungen hätten angefertigt werden können.
- Auch die Möglichkeiten der Überwachung des Fernsprechverkehrs sollten durch den Entwurf erheblich ausgeweitet werden. Die Telefonüberwachung sollte dabei bereits für bestimmte Zwecke der Gefahrenabwehr zugelassen werden.
- Bedenken richteten sich ferner dagegen, bei besonderen Ermittlungsmaßnahmen auf die vorherige richterliche Kontrolle zu verzichten und durch Eilkompetenzen die Entscheidungen über die Maßnahmen der durchführenden Polizei selbst zu übertragen. Nicht einmal die nachträgliche richterliche Kontrolle war in jedem Fall zwingend vorgesehen.

Das Bundesverfassungsgericht (BVerfGE 32, 373) hat festgestellt, daß das Interesse an der Aufklärung von Straftaten nicht jeglichen Eingriff in das informationelle Selbstbestimmungsrecht rechtfertigt. Dies hat der Gesetzentwurf zum OrgKG nicht berücksichtigt. Aus Sicht des Datenschutzes kann nur begrüßt werden, daß dieser Entwurf am Ende der Legislaturperiode des Bundestages der Diskontinuität zum Opfer gefallen ist. Es bleibt zu hoffen, daß die neuerlichen Bestrebungen, denselben Entwurf über den Bundesrat wieder einzubringen, zum Scheitern verurteilt sind.

2.3.2 Kontrollkompetenz im staatsanwaltschaftlichen Informationssystem CANASTA

Im Zuge der Bearbeitung einer Eingabe von 15 Jugendlichen war es erforderlich, eine Kontrolle gem. § 27 BrDSG im staatsanwaltschaftlichen Informationssystem CANASTA durchzuführen.

Dies wurde mir zunächst von der Staatsanwaltschaft Bremen mit der Begründung verwehrt, mir stünden keine Rechte aus § 27 BrDSG zu, da es sich um die Prüfung von Einzelfällen handele, ich könne daher wie jede andere Behörde Auskunft verlangen, die Staatsanwaltschaft werde dann nach den Nummern 182 ff. der RiStBV darüber entscheiden. Die Staatsanwaltschaft hat sich darüber hinaus darauf berufen, daß die Überprüfung einzelner Vorgänge aus Ermittlungsverfahren nicht auf § 27 BrDSG gestützt werden könne, da es sich um bundesrechtlich geregelte Verfahren (StPO) handele, für die das Landesrecht eine Kontrollkompetenz nicht begründen könne.

Da die Beschneidung meines Prüfungsrechts nur durch eine Erklärung des zuständigen Senators möglich ist (§ 27 Abs. 3 BrDSG), habe ich auf einer uneingeschränkten Prüfung bestanden und den Senator für Justiz und Verfassung gebeten, eine Entscheidung herbeizuführen.

Der Senator für Justiz und Verfassung hat für den geschilderten Fall mein uneingeschränktes Prüfrecht für CANASTA und für staatsanwaltschaftliche Ermittlungsakten bestätigt und seine Entscheidung mit grundsätzlichen Ausführungen begründet, die ich zusammengefaßt wiedergeben möchte, weil sie auch für andere öffentliche Stellen von Bedeutung sind.

Der Senator für Justiz und Verfassung hat u. a. festgestellt: „Nach § 27 Abs. 3 BrDSG hat der Landesbeauftragte für den Datenschutz das Recht, Dienst- und Geschäftsräume der in § 1 Abs. 2 BrDSG genannten Stellen zu betreten. Er kann dies sogar ohne Voranmeldung tun. Die Entscheidung, ob der Zutritt zu den Dienst- und Geschäftsräumen erforderlich ist, obliegt dem Landesbeauftragten für den Datenschutz. Die Auswahl, welches der in § 27 Abs. 3 BrDSG genannten Mittel zur Überprüfung geeignet und erforderlich ist, trifft der Landesbeauftragte für den Datenschutz. Ohne die dort (in § 27 Abs. 3 Satz 4 BrDSG) genannte Feststellung des zuständigen Senators kann die betroffene Behörde Zugang und Zugriff nicht verweigern.

Die bundesrechtliche Regelung des Strafverfahrensrechts schließt eine landesrechtliche Regelung über die Verarbeitung personenbezogener Daten bei Landesbehörden nicht aus. Landesbehörden unterliegen den datenschutzspezifischen Regelungen des Landesrechts auch dann, wenn sie Bundesrecht ausführen. Auch § 27 BrDSG hat einen spezifisch datenschutzrechtlichen Regelungsgehalt. Die Bestimmungen des Strafverfahrensrechts werden dadurch nicht berührt. Landesbehörden, die Bundesrecht ausführen, unterliegen gleichzeitig den datenschutzrechtlichen Bestimmungen des Landesrechts (und zudem bereichsspezifischen Datenschutzregelungen des Bundesrechts) und damit der datenschutzrechtlichen Überwachung nach § 27 BrDSG."

2.3.3 Einsatz moderner Informationstechnik am Dezernatsarbeitsplatz in der bremischen Justiz (BREMIT)

Nach Abschluß einer einjährigen Planungs- und Erprobungsphase im BREMIT-Projekt hat der Senator für Justiz und Verfassung im Berichtsjahr ein BREMIT-Konzept vorgelegt, auf dessen Grundlage in diesem und dem folgenden Jahr vierzig Personal-Computer für Dezernenten, sieben Modems und CD-ROM-Laufwerke zur Installation von juristischen Informationssystemen sowie 21 PC für den Schreibdienst der Gerichte und Staatsanwaltschaften beschafft werden sollen.

Dieses Konzept sieht vor, daß folgende juristische Tätigkeiten durch Informations- und Kommunikationstechnik unterstützt werden:

- Die Feststellung und Ordnung streitiger und unstreitiger Sachverhalte mit Hilfe von Datenbankprogrammen, mit dem Ziel, die Entscheidungsfindung zu erleichtern;
- die Erleichterung der Information über das anzuwendende Recht und über obergerichtliche Entscheidungen, indem eigenentwickelte Fundstellenverzeichnisse oder zentrale Rechtsprechungsdatenbanken zum Abruf bereitgestellt werden;
- das Schreiben von Texten durch den juristischen Anwender selbst, wobei je nach Organisation der Textproduktion vorbereitende oder nachbereitende Schreibarbeiten durch die Kanzlei durchgeführt werden sollen;
- die Durchführung ständig wiederkehrender Rechenvorgänge, besonders in den rechenintensiven Bereichen des Familien- und Zivilrechts sowie der Wirtschaftsstrafsachen.

Die im BREMIT-Konzept vorgesehenen Datenschutzmaßnahmen weisen noch eine Reihe offener Fragen auf. Dies ist nicht zuletzt darauf zurückzuführen, daß ich an der einjährigen Planungs- und Erprobungsphase im BREMIT-Projekt erst ganz zum Schluß beteiligt wurde. U. a. die folgenden Fragen konnten noch nicht geklärt werden:

- Sind die Datensicherungsmechanismen des hierfür eingesetzten Produktes geeignet, in der für das BREMIT-Projekt vorgesehenen Software-Umgebung ihre volle Funktionstüchtigkeit zu erreichen?
- Ist der im BREMIT-Konzept enthaltene Hinweis auf die Richtlinien für den Datenschutz am Arbeitsplatz ausreichend, um alle BREMIT-spezifischen Anwendungsbereiche und die damit in Zusammenhang stehenden technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit zu erfüllen?
- Sind angesichts der mit dem BREMIT-Projekt angestrebten Einführung flächendeckender Lösungen (Netzwerke, mittlere Datentechnik) die hierfür erforderlichen Datenschutzmaßnahmen bereits entwickelt worden?

Ich habe den Senator für Justiz und Verfassung gebeten, vor der Beschaffung und Installation der BREMIT-Komponenten ein Datenschutzkonzept zu erarbeiten und mit mir abzustimmen. Dies wurde zugesagt.

2.3.4 Weitere Eingaben

Ein Beschwerdeführer vermutete, daß Bremer Richter bzw. eine Rechtsanwältin unter Ausnutzung ihrer beruflichen Möglichkeiten aus dem Bundeszentralregister Daten über ihn abgerufen und im Privatkreis verwendet hätten. Die auf meine Bitte hin vom Bundesbeauftragten für den Datenschutz durchgeführte Protokollauswertung beim Bundeszentralregister ergab keine Hinweise.

Ein Bürger beschwerte sich darüber, daß zu löschende Eintragungen in Grundbüchern, nicht tatsächlich unlesbar gemacht, sondern lediglich durchgestrichen würden. Im Rahmen von Kreditverhandlungen mit einer Bank sei er gefragt worden, wo er denn das Geld aus einer zu seinen Gunsten eingetragenen Fremdgrundschuld gelassen habe. Der Beschwerdeführer war sehr erstaunt über die Kenntnisse der Bank. Wie sich nachträglich herausstellte, war das Grundstück nach Löschung der Grundschuld verkauft worden, die Bank hatte vor der Mitfinanzierung des Kaufs einen Grundbuchauszug angefordert. Die Eingabe macht prinzipiell deutlich, daß das im Rahmen von § 12 GBO durchgeführte Auskunfts- und Einsichtsverfahren, das lediglich ein „berechtigtes Interesse" des Auskunftsuchenden erfordert, nicht hinreichend die schutzwürdigen Belange der Betroffenen berücksichtigt. Eine Novellierung der Grundbuchordnung steht weiterhin aus.

2.4 Bildung, Wissenschaft und Kunst

2.4.1 Schülerverzeichnis Berufliche Schulen/BerufsschülerIndividualdatei

Der Senator für Bildung, Wissenschaft und Kunst informierte mich im Berichtsjahr darüber, daß er ohne Beteiligung des Rechenzentrums der bremischen Verwaltung und ohne vorherige Beschlußfassung im AADV ein DV-Verfahren „Schüler-

verzeichnis Berufliche Schulen" entwickelt habe, das den beruflichen Schulen zur Anwendung auf ihren Schulrechnern (PC mit MS-DOS Betriebssystem) angeboten werden soll. Mit Hilfe dieses DV-Verfahrens (Datenbankanwendung) können die beruflichen Schulen verschiedene Datenbanken (z. B. Schüler, Firmen/Betriebe, Klassen) aufbauen, pflegen und sichern und eine Vielzahl von listenmäßigen und sonstigen Auswertungen aus diesen Datenbanken — einzeln oder verknüpft — vornehmen. Dadurch soll die Verwaltungsarbeit in den beruflichen Schulen technisch unterstützt und insgesamt erleichtert und verbessert werden.

Ich habe mit dem Senator für Bildung, Wissenschaft und Kunst dieses praktisch fertig entwickelte und kurz vor der Einführung stehende DV-Verfahren ausgiebig erörtert und eine Reihe von Hinweisen und Anregungen datenschutzrechtlicher Art gegeben. Diese bezogen sich vor allem auf die Datensatzstruktur (Datenbankstruktur und Datenbankbeschreibung), die Erhebung und Beschaffung der Daten (vom Betroffenen im Wege der Einwilligung oder zwangsweise auf gesetzlicher Grundlage, durch Datenübermittlung von Dritten, durch Datenträgeraustausch oder Datenübertragung innerhalb des Bildungsressorts etc.), die Nutzung der Daten für schulische und statistische Zwecke, die Beachtung der Betroffenenrechte sowie auf Aspekte der Datensicherung und ordnungsgemäßen Datenverarbeitung (z. B. Einsatz einer speziellen Sicherungssoftware mit Verschlüsselungsroutine zur Abwehr unbefugter Daten- und Datenbankzugriffe, Aufbewahrungs- und Löschungsfristen).

Aufgrund dieser Erörterung ergab sich für den Senator für Bildung, Wissenschaft und Kunst die Notwendigkeit, das entwickelte Verfahren in einigen Punkten zu ändern. Die Einführung des Verfahrens an den beruflichen Schulen steht derzeit noch aus. Bemerkenswert an dieser Verfahrensentwicklung ist die Tatsache der Eigenentwicklung durch den Senator für Bildung, Wissenschaft und Kunst ohne Beteiligung des Rechenzentrums der bremischen Verwaltung und ohne vorherige Beschlußfassung im AADV, obwohl die bestehenden Verwaltungsvorschriften (ADV-Anweisung!) dies ausdrücklich anders regeln. Im Hinblick auf den zunehmenden PC-Einsatz in der bremischen Verwaltung und die Verbreiterung des Wissens zum Umgang und zur Nutzung dieser DV-Systeme scheint es mir dringend erforderlich, das Problem der Eigenprogrammierung auf den vorhandenen PC grundsätzlich zu erörtern und ggf. die ADV-Anweisung zu ergänzen oder zu ändern. Die vom Senat im August 1990 erlassenen Richtlinien zum Datenschutz am Arbeitsplatz (sog. PC-Richtlinien) sagen zu dieser Problematik nur so viel, daß die bestehenden Verwaltungsvorschriften unberührt bleiben. Daraus kann ich derzeit nur folgern, daß die Eigenprogrammierung auf den in der bremischen Verwaltung vorhandenen PC nicht zulässig ist; PC-Programmierarbeiten sind zentral vom Rechenzentrum der bremischen Verwaltung oder darüber vermittelt durch andere zu erledigen.

2.4.2 Richtlinien zur Führung der Schullaufbahnakten

Viele Schulen im Lande Bremen haben Probleme, die besonderen Datenschutzregelungen für den Schulbereich korrekt anzuwenden. So bin ich im Berichtsjahr häufiger mit Fragen konfrontiert worden, die sich mit der Führung der Schullaufbahnakten beschäftigen. Dabei wurde ich auf eine Reihe von Mängeln und Fehlern sowie auf Unsicherheiten bei der Anwendung der Richtlinien und auf Unklarheiten in den Richtlinien selbst aufmerksam. Als Beispiel seien hier folgende, dem Schulalltag entstammende Fälle genannt:

— Beim Übergang von Schülern von Privatschulen in öffentliche Schulen oder beim Wechsel von einer Schule außerhalb Bremens an eine öffentliche Schule im Lande Bremen werden Daten übermittelt, die nicht dem Bremischen Schuldatenschutzgesetz entsprechen. U. a. wurden in einer Schullaufbahnakte unzulässigerweise Unterlagen über ärztliche Untersuchungen und Eignungstests aufbewahrt, die von einer Privatschule zum Zwecke der Einschulung eines behinderten Kindes verlangt worden waren. Die Unterlagen waren anläßlich eines Schulwechsels des Kindes an die öffentliche Schule weitergegeben worden.

  Die Richtlinien sagen dazu nichts; die Praxis der Schulen ist vielgestaltig; meist werden die Daten bzw. Unterlagen unbereinigt und ohne nähere Prüfung in die neuangelegte Schullaufbahnakte übernommen mit der Folge, daß diese Schullaufbahnakte häufig nicht den datenschutzrechtlichen Bestimmungen entspricht.

- Weitergabe der kompletten Schullaufbahnakte an andere Schulen, obwohl einzelne Teile dieser Akte nach den Richtlinien nicht, zumindest nicht ohne ausdrückliche Einwilligung weitergegeben werden dürfen.

- Schulen fertigen zum Teil ohne Wissen und Kenntnisnahme der Eltern Lernentwicklungsberichte als Zeugnisersatz oder als Zeugnisergänzung an, die in die Schullaufbahnakte aufgenommen werden. Die Richtlinien sagen zu dieser Problematik ebenfalls nichts.

- Daten und Unterlagen in Schullaufbahnakten, die vor Inkrafttreten des Schuldatenschutzgesetzes und der neugefaßten Richtlinien aufgenommen wurden, befinden sich weiterhin in den Akten. Häufig wird eine Bereinigung der Schullaufbahnakte bei Weitergabe nicht vorgenommen. Auch dieses Problem ist in den Richtlinien unzulänglich geregelt.

Ich habe den Senator für Bildung, Wissenschaft und Kunst gebeten, die Richtlinien zur Führung der Schullaufbahnakten insgesamt zu überprüfen und dabei Lücken zu schließen und eventuelle Differenzen zum Schuldatenschutzgesetz zu beseitigen. Dieses Anliegen will ich im Gespräch mit dem Senator für Bildung, Wissenschaft und Kunst weiterverfolgen.

2.4.3 Änderung des Privatschulgesetzes

Im Zusammenhang mit den seinerzeitigen Diskussionen um das Schuldatenschutzgesetz wurde erörtert, vergleichbare Datenschutzregelungen auch für die Privatschulen im Lande Bremen zu schaffen. Zwei Möglichkeiten standen dabei zur Debatte: Erstreckung des Schuldatenschutzgesetzes auf die Privatschulen oder Aufnahme von Datenschutzbestimmungen in das Privatschulgesetz des Landes. Im Hinblick auf die Fragen im Zusammenhang mit der Gesetzgebungskompetenz des Landes für diese Regelungsmaterie wurde zunächst von diesem Vorhaben Abstand genommen.

Die vom Senator für Bildung, Wissenschaft und Kunst geäußerten Zweifel an der Kompetenz des Landes, auch für die Privatschulen umfassende Datenschutzregelungen zu schaffen, teile ich nicht. Das Land hat die alleinige Gesetzgebungshoheit für die Schulen, unabhängig davon, wer Träger der Schule ist. Dies schließt sachlogisch auch die Kompetenz ein, die Datenverarbeitungsvorgänge der Privatschulen und damit den Datenschutz dort zu regeln. Die Schulen der öffentlich-rechtlichen Religionsgesellschaften könnten dann von derartigen Datenschutzregelungen ausgenommen werden, wenn gleichwertige kirchliche Datenschutzregelungen für die spezifischen Verhältnisse der kirchlichen Schulen vorhanden sind. Einen ähnlichen Weg ist der Landesgesetzgeber beim Krankenhausdatenschutzgesetz gegangen.

Ich rege an, diesem Beispiel zu folgen und schulspezifisches Datenschutzrecht auch für die Privatschulen im Lande Bremen zu schaffen.

2.4.4 Entwurf eines Bremischen Archivgesetzes

Seit Jahren, zuletzt in meinem 12. Jahresbericht, weise ich auf die Notwendigkeit hin, ein Bremisches Archivgesetz zu erlassen. Auch Bürgerschaft und Senat haben mehrfach die Notwendigkeit einer solchen Gesetzgebung anerkannt.

Gegen Ende des Berichtsjahres erhielt ich vom Senator für Bildung, Wissenschaft und Kunst einen Gesetzentwurf zur abschließenden Stellungnahme. Diese Stellungnahme liegt dem Senator inzwischen vor. Geplant ist, den Gesetzentwurf rechtzeitig der zuständigen Deputation zur Beratung vorzulegen, damit eine Beschlußfassung der Bremischen Bürgerschaft noch vor Ablauf dieser Legislaturperiode erfolgen kann.

Mit dem Archivgesetz sollen die bisher nur auf Verwaltungsvorschriften beruhenden Aufgaben des Staatsarchivs Bremen und die der anderen öffentlichen Archive, wie z. B. Stadtarchiv Bremerhaven, gesetzlich festgelegt werden. Primäre Aufgabe des Staatsarchivs Bremen soll es sein, Unterlagen von Behörden, Gerichten und sonstigen Stellen des Landes und der Stadtgemeinde Bremen auf Archivwürdigkeit hin zu werten und die als archivwürdig erkannten Teile als Archivgut zu übernehmen. Archivwürdig sind nach dem Gesetzentwurf Unterlagen, die für die Erforschung und das Verständnis der Geschichte, insbesondere der bremischen Geschichte, die Sicherung berechtigter Belange der Bürger oder die Bereitstellung von Informationen für Gesetzgebung, Verwaltung oder Recht-

sprechung von bleibendem Wert sind. Über die Archivwürdigkeit soll das Staatsarchiv unter archivfachlichen Gesichtspunkten entscheiden.

Den öffentlichen Stellen des Landes und der Stadtgemeinde Bremen wird auferlegt, alle Unterlagen, die nicht mehr benötigt werden, 30 Jahre nach Entstehung dem Staatsarchiv zur Übernahme anzubieten. Im Hinblick auf die Unterlagen habe ich empfohlen, diese — wenn sie denn angeboten und evtl. übernommen werden sollen — einer besonderen Aufbewahrungs- und Nutzungsregelung zu unterwerfen.

Im Hinblick darauf, daß die Abgabe von archivwürdigen Unterlagen an das Staatsarchiv nach meiner Auffassung ein Surrogat für eine an sich erforderliche Vernichtung oder Löschung dieser Unterlagen darstellt, kommt natürlich den Aufbewahrungs- und Zugangs- bzw. Nutzungsregelungen besondere Bedeutung zu. Der Gesetzentwurf sichert den Betroffenen oder ihren Ehegatten, Kindern oder Eltern datenschutzrechtliche Auskunfts-, Einsichts- sowie Löschungs- und Berichtigungsrechte zu. Außerdem ist ein Gegendarstellungsrecht vorgesehen, falls die Richtigkeit oder Unrichtigkeit der Daten streitig sein sollte.

Nach dem Entwurf soll die abgebende Stelle — von wenigen Ausnahmen abgesehen — ein jederzeitiges Nutzungsrecht an ihren früheren Unterlagen haben. Ich vertrete hingegen die Auffassung, daß den Stellen nur im Rahmen der normalen Nutzungsrechte, wie sie für jedermann gelten, Zugriff gewährt werden darf, weil es sich um an sich zu löschendes Material handelt.

Bei den Nutzungsregelungen für jedermann bestehen unterschiedliche Auffassungen bzgl. der Sperrfristen für den Zugang zu personenbezogenem Archivmaterial. Der Gesetzentwurf sieht die Nutzung derartiger Unterlagen bereits zehn Jahre nach dem Tod des Betroffenen, und wenn der Todestag nicht feststellbar ist, 90 Jahre nach der Geburt, und falls das Geburtsdatum nicht feststellbar ist, 60 Jahre nach Entstehung der Unterlagen vor. Ich habe die Übernahme der längeren Sperrfristen des Bundesarchivgesetzes (30 Jahre nach Tod, 110 Jahre nach Geburt, 80 Jahre nach Entstehung der Unterlagen — falls auch das Geburtsdatum nicht feststellbar ist) empfohlen.

Für die anderen öffentlichen Archive im Lande Bremen sollen im Grundsatz ähnliche Aufgaben und Nutzungsregelungen bestehen. Insgesamt kann man feststellen, daß der überarbeitete Gesetzentwurf viele datenschutzrechtliche Anregungen aufgenommen hat und daß grundsätzliche Problempunkte der politischen Entscheidung vorbehalten bleiben.

2.4.5 Wahrung des Sozialgeheimnisses durch das Studentenwerk

Wiederholt haben sich Eltern an mich gewandt, deren Kinder Ausbildungsförderung beantragt hatten und die daraufhin vom Studentenwerk zur Offenlegung ihrer Einkommens- bzw. Vermögensverhältnisse aufgefordert worden waren. Einkommen und Vermögen der Eltern sind nach Maßgabe des § 11 BAFöG in der Regel auf die Ausbildungsförderung anzurechnen. Nach § 47 Abs. 4 BAFöG i. V. m. mit § 60 SGB I sind die Eltern genauso wie die Antragsteller selbst verpflichtet, die für die Entscheidung über den Antrag erheblichen Tatsachen über ihr Einkommen und Vermögen anzugeben. Das Studentenwerk kann ihnen hierfür eine angemessene Frist setzen, § 47 Abs. 6 BAFöG. Kommen die Eltern ihren Verpflichtungen nicht nach, handeln sie ordnungswidrig und können mit Bußgeld belegt werden, § 58 Abs. 1, 2 BAFöG. Das Studentenwerk seinerseits hat als Sozialleistungsträger nach § 35 SGB I sicherzustellen, daß die ihm anvertrauten Daten der Eltern als Sozialgeheimnis gewahrt und nicht unbefugt offenbart werden.

Die Eltern, die sich an mich wandten, beklagten sich insbesondere darüber, daß die an ihre Kinder gerichteten Bescheide ihre Einkommensverhältnisse, d. h. das monatliche Einkommen sowie Abzüge für Steuern und soziale Sicherung, enthalten hätten. In einem Fall hatten sich die Eltern zuvor geweigert, weiterhin Unterhalt zu zahlen. In einem anderen Fall erhielten auf diesem Umwege voneinander geschiedene Eltern Kenntnis vom Einkommen des jeweils anderen Teils.

Ich mußte die Eltern darüber informieren, daß § 50 Abs. 2 BAFöG vorschreibt, daß der Bescheid genau diese Angaben zu enthalten habe. Der Grund ist, daß der Antragsteller über die Entscheidungsgrundlagen zu unterrichten ist, um prüfen zu können, ob er ggf. mit Erfolg Rechtsmittel einlegen kann. Allerdings räumt § 50 Abs. 2 Satz 3 BAFöG den Eltern das Recht ein zu verlangen, daß der Bescheid mit

Ausnahme des Betrages ihres angerechneten Einkommens keine weiteren Angaben über ihr Einkommen enthält. Voraussetzung ist, daß die Eltern ihr Verlangen begründen und daß der Auszubildende seinerseits im Zusammenhang mit der Geltendmachung seines Anspruchs auf Ausbildungsförderung kein besonderes berechtigtes Interesse an der Kenntnis der darüber hinausgehenden pflichtgemäßen Angaben hat. Das Studentenwerk Bremen hat mir ein Merkblatt für Eltern von Antragstellern vorgelegt, das sie auch über diese Rechtsposition informiert.

In einem Fall allerdings richtete sich die Beschwerde dagegen, daß trotz eines ausdrücklichen Verlangens der Bescheid nicht nur das angerechnete Elterneinkommen, sondern auch darüber hinausgehende Angaben enthielt. Mir ist versichert worden, dies sei ein Einzelfall. Die Mitarbeiter und Mitarbeiterinnen seien über die Vorschriften unterrichtet und würden sie in der Regel auch beachten. Im Beschwerdefall werde noch eine gesonderte Belehrung des zuständigen Sachbearbeiters erfolgen.

2.5 Jugend und Soziales

2.5.1 Innerbehördlicher Datenschutz in den Sozialen Diensten

Meine Bemühungen, den Datenfluss innerhalb der Sozialen Dienste auf das mit dem gesetzlichen Schutz des Sozialgeheimnisses und den beruflichen Schweigepflichten der Mitarbeiter vereinbare Maß zu begrenzen, habe ich ausführlich in den beiden letzten Jahresberichten dargestellt. Das Ressort Jugend und Soziales arbeitet weiterhin an der Umsetzung der hierzu getroffenen Absprachen. Für das Verfahren zur Aufnahme in die heilpädagogische Tageserziehung der Kindertagesheime der Stadtgemeinde Bremen wird derzeit eine entsprechende Arbeitsanweisung entwickelt. Sie soll verbindlich datenschutzgerechte Verfahrensweisen festlegen, die zwar inzwischen weitgehend, aber noch nicht völlig einheitlich praktiziert werden:

- Zu den Hilfekonferenzen, auf denen über die Aufnahme bzw. die Verlängerung der Hilfe für einzelne Kinder beraten wird, dürfen nur die Mitarbeiter der Sozialen Dienste bzw. Freien Träger und die Sachverständigen eingeladen werden, deren Teilnahme zur Beratung des jeweiligen Einzelfalls erforderlich ist.

- Schriftliche Unterlagen dürfen nur soweit erforderlich personenbezogene Daten von Kindern und Eltern enthalten und dürfen nur an die im Einzelfall zu beteiligenden Personen übersandt werden.

- Für den innerbehördlichen Umgang mit Daten, die beruflichen Schweigepflichten unterliegen, sollen die für das Aufnahmeverfahren in das Betreute Wohnen entwickelten Regelungen übernommen werden (vgl. 12. Jahresbericht, S. 37). Es sollen Formblätter entwickelt werden, die gewährleisten, daß an den Kostenträger nur die Aussagen aus ärztlichen/psychologischen/pädagogischen Gutachten übermittelt werden, die er für seine Entscheidung benötigt, nicht aber die gesamten Gutachten.

- Es sollen Formulare für Schweigepflichtsentbindungen der Eltern entwickelt und verwandt werden, die sicherstellen, daß die Eltern über die Bedeutung ihrer Erklärung hinreichend aufgeklärt werden und daß die Daten nur für das laufende Aufnahmeverfahren an bestimmte Empfänger übermittelt werden.

Der Senator für Jugend und Soziales hat zugesagt, man werde die bereits entwickelten Verfahren für notwendige Neuregelungen gleichgelagerter Antragsverfahren nutzen.

Inzwischen ist zum 01.01.1991 das neue Kinder- und Jugendhilfegesetz (BGBl. I, 1990, S. 1163) in Kraft getreten, das in § 65 ausdrücklich bestimmt, daß personenbezogene Daten, die dem Mitarbeiter eines Trägers öffentlicher Jugendhilfe zum Zwecke persönlicher und erzieherischer Hilfen anvertraut worden sind, nur offenbart werden dürfen, wenn der Betroffene eingewilligt hat bzw. die Voraussetzungen vorliegen, unter denen z. B. Psychologen, Berater, Sozialpädagogen, Sozialarbeiter oder deren Gehilfen nach § 203 StGB zur Durchbrechung ihrer beruflichen Schweigepflichten befugt wären. Die Übermittlung von Klientendaten im Bereich der öffentlichen Jugendhilfe muß im Lichte dieser neuen Vorschrift überprüft werden.

2.5.2 Datenschutz im Anmeldeverfahren und Datensicherheit in den Kindertagesheimen

In Verbindung mit einer Gebührenerhöhung bereitete der Senator für Jugend und Soziales eine Änderung des Anmeldeverfahrens für die Kindertagesheime der Stadtgemeinde Bremen vor. Bisher legten die Eltern der Leitung des Kindertagesheims, für das sie ihr Kind anmelden wollten, ihre Einkommensunterlagen im Original vor. Sie wurden ihnen anschließend nach Prüfung und Verarbeitung der Daten durch die Leitung wieder ausgehändigt. Nunmehr sollte dieses Verfahren stichprobenweise überprüft werden. Jeder fünfte Vorgang (ausgenommen Höchstzahler und Empfänger von Sozialhilfe) sollte zwecks Nachberechnung an eine zentrale Stelle weitergeleitet werden. Zu diesem Zweck sollten alle Eltern ihre Einkommensunterlagen im Original und in Kopie vorlegen. Die Originale sollten sie nach der Berechnung durch die Heimleitung zurückerhalten, die Kopien sollten für die mögliche Nachberechnung zunächst einbehalten und spätestens nach drei Monaten zurückgegeben werden.

Gegen diese Regelung habe ich aufgrund von Beschwerden Betroffener Bedenken erhoben. Die Verpflichtung, Kopien der Unterlagen dem Amt zu überlassen, sollte alle nachweispflichtigen Eltern treffen, obwohl nur in jedem fünften Fall die Beiträge nachberechnet werden sollten. Die Datenerhebung wäre daher nicht auf das notwendige Maß begrenzt worden. Inzwischen ist eine Dienstanweisung in Kraft getreten, aufgrund derer nur die tatsächlich für die Nachberechnung ausgewählten Eltern zu einem Prüftermin eingeladen werden, zu dem sie noch einmal die Unterlagen vorlegen sollen.

Zugleich gingen Beschwerden bei mir ein, die sich gegen den Umfang der Datenerhebung zum Zwecke der Einkommensberechnung im Anmeldeverfahren zu den Kindertagesheimen der Stadtgemeinde Bremen wandten. Ich habe festgestellt, daß die von den Eltern abverlangten Angaben durch die Vorschriften des Bremischen Kindergarten- und Hortgesetzes und der zu ihm ergangenen Ausführungsbestimmungen abgedeckt sind. Das Kinder- und Jugendhilfegesetz, das am 01. 01. 1991 in Kraft getreten ist, hat in § 90 nunmehr eine insoweit inhaltlich identische bundeseinheitliche Regelung geschaffen: § 19 Abs. 1 Nr. 1 des Einkommensteuergesetzes, das über § 3 der Verordnung zur Durchführung des § 76 BSHG heranzuziehen ist, enthält detaillierte Regelungen über die Berechnung des anrechnungspflichtigen Einkommens aus nichtselbständiger Arbeit.

Schließlich waren Beschwerden eingegangen, daß in Kindertagesheimen der Stadtgemeinde Bremen mit personenbezogenen Daten von Eltern und Kindern ausgefüllte Anmeldebögen in unverschlossenen Schränken in Räumen aufbewahrt würden, die allen Mitarbeitern der Einrichtung zugänglich seien. Ich habe daraufhin vier Kindertagesheime aufgesucht und geprüft, wie dort mit den gespeicherten Daten von Eltern und Kindern umgegangen wird. Dabei ging es vor allem darum, wie bzw. wie lange die ausgefüllten Anmeldebögen und die ärztlichen/psychologischen/pädagogischen Stellungnahmen/Befunde insbesondere für behinderte bzw. entwicklungsgestörte Kinder aufbewahrt werden.

Dabei stellte ich fest, daß in den besuchten Einrichtungen die Vorkehrungen zur Sicherung der Unterlagen unterschiedlich gehandhabt wurden und nicht in jedem Fall ausreichend waren. So würden die Anmeldebögen in zwei Fällen in offenen Regalen aufbewahrt, wobei aber die erwähnten Stellungnahmen/Befunde getrennt davon und gesichert untergebracht waren. Eine Verwaltungsanweisung über Aufbewahrungsfristen und die Tatsache, daß jede der vier Regionalabteilungen des Amtes für Soziale Dienst über einen Schredder zur Vernichtung von amtlichen Unterlagen verfügt, waren nicht in allen besuchten Einrichtungen bekannt. Im Anschluß an meinen Prüfbericht hat das Amt für Soziale Dienste zugesichert, daß in städtischen Kindertagesheimen

- Anmeldebögen nur noch in abschließbaren Schränken aufbewahrt werden sollen und daß diese Schränke nach Feierabend oder bei sonstiger längerer Nichtbesetzung des Büros tatsächlich abgeschlossen werden sollen,
- ärztliche/psychologische/pädagogische Stellungnahmen/Befunde getrennt von den übrigen Unterlagen in abgeschlossenen Fächern (etwa im Schreibtisch der Heimleitung) aufzubewahren sind,
- die Mitarbeiter auf die Aufbewahrungsfristen und darauf hingewiesen werden sollen, daß Unterlagen mit personenbezogenen Daten ausschließlich in den bereitstehenden Schreddern vernichtet werden sollen.

2.5.3 Programmierte Sozialhilfe (PROSOZ)

Im 11. Jahresbericht (S. 81) hatte ich zuletzt über die datenschutzrechtlichen Aspekte dieses Projekts berichtet, auf dessen Grundlage die Berechnung und Zahlbarmachung der laufenden Sozialhilfe auf ADV umgestellt werden soll. Nachdem meine Fragen beantwortet wurden, habe ich dem Datenschutzkonzept zugestimmt. Insbesondere ist zugesichert worden, daß neben dem bisher für das gesamte Ressort Jugend und Soziales zuständigen Beauftragten für den Datenschutz im Bereich Wirtschaftliche Hilfen ein weiterer Beauftragter bestellt werden soll. Dieser soll auch die ordnungsgemäße Verarbeitung personenbezogener Daten im PROSOZ-Verfahren überwachen. Daneben ist sichergestellt worden, daß für innerbehördliche Planungszwecke nur anonymisierte Sozialhilfedaten übermittelt werden.

Als eine Grundlage der zur Einführung von PROSOZ vorgesehenen Qualifizierung der Sozialhilfesachbearbeiter wird ein unter meiner Mitwirkung erarbeiteter Arbeitsleitfaden über Datenschutz im Sozialhilfeverfahren verwandt. Die Vorbereitung von PROSOZ wurde zum Anlaß genommen, die Teilnehmer mit den für ihre Praxis grundlegenden Regelungen zum Schutz des Sozialgeheimnisses ihrer Klienten vertraut zu machen, z. B. mit

- dem Umfang der zulässigen Datenerhebung bzw. mit den Grenzen der Mitwirkungspflichten der Antragsteller,
- den Grenzen für Anfragen bei anderen Stellen,
- den Grenzen der Befugnisse zur Offenbarung von Sozialdaten an andere Stellen, sei es innerhalb oder außerhalb der Sozialverwaltung.

Diese notwendigen Qualifizierungsveranstaltungen sollen fortgesetzt werden und möglichst alle Sachbearbeiter erreichen.

2.5.4 Offenbarung von Sozialgeheimnissen durch das Sozialamt Bremerhaven zum Zwecke der Leistung von Sozialhilfe

Veranlaßt durch verschiedene Beschwerden habe ich mit dem Sozialamt Gespräche über einen verbesserten Schutz seiner Klienten gegenüber Übermittlungen ihrer Daten an Dritte geführt.

Das Sozialamt ist dazu übergegangen, einmalige Beihilfen — etwa zur Anschaffung von hochwertigen Elektrogeräten wie Waschmaschinen, aber auch von Farben und Tapeten zur Wohnungsrenovierung — als Sachleistung zu gewähren. Es verwies die Hilfeempfänger an bestimmte Firmen, mit denen es Rabatte vereinbart hatte. Das Amt stellte unter seinem Namen Wertgutscheine aus, in denen Name, Adressen und Aktenzeichen der Hilfeempfänger verzeichnet waren. Begründet wurde dieses Verfahren mit der erreichten Kostenersparnis und damit, daß die Vertragsfirmen einen guten Kundendienst gewährleisteten. Ich habe dagegen angeführt, daß das Amt auf diese Weise den Lieferfirmen die Tatsache, daß ein bestimmter Klient Sozialhilfe beziehe, also ein Sozialgeheimnis, offenbare, ohne daß dies zur Aufgabenerfüllung des Amtes erforderlich sei, wie es § 69 Abs. 1 Nr. 1 SGB X voraussetze. Zweck der Sozialhilfe sei es, dem Empfänger der Hilfe die Führung eines Lebens zu ermöglichen, das der Würde des Menschen entspreche, § 1 BSHG. Dann müsse ihm aber im Rahmen der ihm nach dem Gesetz zustehenden Hilfen die Möglichkeit gelassen werden, wie jedermann mittels Bargeld am Wirtschaftsleben teilzunehmen und seine Bedarfsdeckung zu gestalten. Dies habe jedenfalls so lange zu gelten, als nicht konkrete Anhaltspunkte auf die Gefahr einer zweckwidrigen Verwendung der Mittel hindeuteten. Auch dieser Gefahr müsse zunächst einmal durch die Auflage begegnet werden, Rechnungen bzw. Quittungen vorzulegen. Erst wenn dieser geringere Eingriff sich als nicht ausreichend erweise, dürfe das Amt dazu übergehen, die Hilfe in Form von Sachleistungen, verbunden mit der Offenbarung von Sozialgeheimnissen an Dritte, zu gewähren.

Das Amt hat sich demgegenüber auf das Urteil des Verwaltungsgerichts Bremen vom 04. 10.1990 — 3 A 323/88 — berufen, in dem die kritisierte Praxis gebilligt wurde. Das Gericht hat dies vor allem damit begründet, daß auch das Sozialamt nach der Landeshaushaltsordnung verpflichtet sei, bei der Ausführung des Haushaltsplans wirtschaftlich und sparsam zu verfahren. Deshalb habe das Amt mit der Entscheidung, die Hilfe als Sachleistung zu gewähren, das ihm für die Auswahl von Form und Maß der Leistung zustehende Ermessen sachgerecht ausgeübt.

Dieser Argumentation kann ich nicht folgen, weil sie zum einen die oben dargestellten Ziele der Sozialhilfe außer acht läßt und weil zum anderen die Pflicht der Verwaltung zu wirtschaftlichem Verhalten fehlende gesetzliche Befugnisse nicht ersetzen kann.

Dennoch habe ich davon abgesehen, eine Beanstandung auszusprechen. Das Sozialamt hat sich bereit erklärt, seine durch das Gericht bestätigte Praxis der Gewährung von Sachleistung zu modifizieren und mehr als bisher darauf zu achten, daß die damit verbundenen Offenbarungen auf das geringstmögliche Maß beschränkt bleiben. Dies soll vor allem dadurch erreicht werden, daß in Zukunft Formulare verwandt werden, die nicht erkennen lassen, daß das Sozialamt sie ausgestellt hat, und die auch nicht auf den Namen des Empfängers ausgestellt sind.

In der Vergangenheit hat das Sozialamt Bremerhaven — zum Teil nach mündlich erklärter Einwilligung, zum Teil aber auch ohne Einwilligung der Betroffenen — die Mieten der in ihren Wohnungen lebenden Sozialhilfeempfänger direkt an die Städtische Wohnungsbaugesellschaft Bremerhaven überwiesen. Entsprechend sind auch Erstattungen von zuviel gezahlten Nebenkosten direkt von der Vermieterin an das Amt zurück überwiesen worden. Ich habe demgegenüber darauf hingewiesen, daß nach § 67 Abs. 2 SGB X Einwilligungen in die Offenbarung von Sozialgeheimnissen grundsätzlich der Schriftform bedürften und daß Wohnungshilfe grundsätzlich als Geldleistung zu gewähren sei mit der Folge, daß die Sozialhilfeempfänger und nicht das Sozialamt Mieter seien. Daher sei der Geldverkehr über die Leistungsempfänger abzuwickeln, es sei denn, diese hätten in eine andere Form der Abwicklung eingewilligt oder es bestehe der Verdacht, daß die Empfänger die Geldleistung nicht bestimmungsgemäß für die Mietzahlung verwendeten. Die Tatsache, daß die Empfänger eine Erstattung erhalten hätten, hätten sie nach § 60 Abs. 1 Nr. 2 SGB I dem Sozialamt mitzuteilen. Nur bei Verdacht der Verletzung dieser Obliegenheit habe das Amt das Recht zur Ermittlung beim Vermieter.

Darauf hat das Sozialamt erklärt, es werde künftig nur nach Unterzeichnung einer schriftlichen Einwilligung oder bei Verdacht der nicht bestimmungsgemäßen Verwendung der Hilfe bzw. der Erstattung die Miete direkt an den Vermieter zahlen bzw. Erstattungen entgegennehmen. Das Amt hat mir den entsprechenden Vordruck vorgelegt.

Ein Beschwerdeführer — ein arbeitsloser Sozialhilfeempfänger — hatte sich dagegen gewandt, daß das Sozialamt Bremerhaven seine Anschrift ohne sein Wissen an einen Träger der beruflichen Weiterbildung übermittelt habe, worauf ihn dieser zu einem Gespräch eingeladen habe. Das Sozialamt hat mir auf Anfrage versichert, es werde künftig in jedem Fall die Einwilligung des betreffenden Hilfeempfängers einholen, bevor es seine Daten zu Beratungs- oder Vermittlungszwecken an einen Träger beruflicher Qualifikationsmaßnahmen übermittle.

2.6 Gesundheit

2.6.1 Durchführung des Gesundheitsreformgesetzes (SGB V)

Das Gesundheitsreformgesetz legt wesentlich präziser, als es vor ihm die Reichsversicherungsordnung getan hat, die Befugnisse der an der Gesundheitsversorgung beteiligten Stellen zur Verarbeitung von Versicherten- bzw. Patientendaten fest. So enthält es etwa bereichsspezifische Regelung zur Datenverarbeitung der Kassenärztlichen Vereinigungen, der gesetzlichen Krankenkassen und ihrer medizinischen Dienste zur Erfüllung ihrer Aufgaben sowie zur Befugnis von Ärzten und Krankenhäusern zur Übermittlung der hierfür benötigten Daten. Allerdings ist festzustellen, daß diese Regelungen manche Unklarheiten bzw. Unstimmigkeit enthalten. Außerdem scheint es das Bestreben einiger Stellen zu sein, auch über den erklärten Willen des Gesetzgebers hinaus in dem Maße Daten zu verarbeiten, wie dies ihnen geboten erscheint bzw. wie sie es aus der Zeit gewohnt sind, in der noch die Reichsversicherungsordnung galt. Demgegenüber ist daran festzuhalten, daß z. B. § 301 Abs. 1 SGB V die Befugnisse von Krankenhäusern zur Übermittlung von Patientendaten an die Krankenversicherungen abschließend regelt. Die Kassen können nicht verlangen, daß ihnen darüber hinaus Daten übermittelt werden, und dies etwa damit begründen, sie benötigten diese Daten zur Erfüllung ihrer Aufgaben. Auch durch vertragliche Regelungen können die gesetzlichen Befugnisse nur konkretisiert, nicht aber erweitert werden.

Maschineller Datenträgeraustausch zwischen Krankenhäusern und Krankenkassen

§ 301 Abs. 1 SGB V befugt die Krankenhäuser nach dem eindeutigen Wortlaut seiner Ziffer 1 lediglich dazu, die Krankenversichertennummer ihrer Patienten, nicht aber dazu, deren Grunddaten wie Name, Anschrift und Geburtsdatum an die Kassen zu übermitteln. Die Praxis sieht anders aus. Vertreter der Kassen und des Senators für Gesundheit haben mir hierzu vorgetragen, daß die Übermittlung der Grunddaten weiterhin erforderlich sei, weil die Krankenversichertennummer noch gar nicht durchgängig eingeführt sei, weil nur auf diese Weise Übermittlungsfehler zuverlässig ausgeschaltet werden könnten und weil die Krankenversichertennummer nicht bei allen Kassen nach einem übereinstimmenden Schema gebildet werde. Ich habe daraufhin in Abstimmung mit den Datenschutzbeauftragten des Bundes und der anderen Länder befristet bis zu der von der Bundesregierung in Aussicht gestellten Nachbesserung des Gesundheitsreformgesetzes der Erweiterung des Katalogs zugestimmt. Entscheidend war dabei die Erwägung, daß die Übermittlung der Grunddaten ebenso wie die der Krankenversichertennummer der Identifizierung des Versicherten dienen soll.

Prüfung ungewöhnlich langer Verweildauern in Krankenhäusern durch die Krankenkassen

Wird ein Patient länger als drei Wochen stationär behandelt, so erstattet im Lande Bremen das Krankenhaus der zuständigen Kasse Bericht über die voraussichtliche Dauer und die Gründe hierfür. Diese Übermittlung von Patientendaten ist durch das Gesetz nicht gedeckt: Im Datenkatalog des § 301 Abs. 1 SGB V fehlt die Befugnis zur Berichterstattung bei Überschreiten einer bestimmten Verweildauer („Verlängerungsanzeige"). In Ziffer 2 ist lediglich die Rede von der Befugnis zur Übermittlung des Grundes der Aufnahme und der Aufnahmediagnose. In Ziffer 4 geht es nur um den Grund der Entlassung oder Verlegung sowie um die Entlassungsdiagnose. Allenfalls kann man aus dem Regelungszusammenhang heraus eine Berichterstattung bei Veränderung der Diagnose („Veränderungsanzeige") als zulässig interpretieren. Im Falle eines längeren Krankenhausaufenthaltes bei unveränderter Diagnose dagegen kann lediglich im Einzelfall der Medizinische Dienst im Rahmen seiner Befugnisse nach §§ 275, 276 SGB V prüfend tätig werden. Auch auf § 100 SGB X kann die praktizierte routinemäßige Datenübermittlung nicht gestützt werden.

Ich habe die Landesverbände der Krankenkassen darauf hingewiesen, daß ich die gegenwärtige Praxis für unzulässig halte. Die Verbände berufen sich in ihrer gemeinsamen Antwort darauf, daß diese Praxis erforderlich sei, damit sie ihre gesetzlich vorgeschriebene Verpflichtung der Prüfung der Leistungsvoraussetzungen erfüllen könnten. Insbesondere leiten sie dies daraus ab,

- daß nach § 39 Abs. 1 SGB V die Versicherten nur dann einen Anspruch auf Behandlung in einem Krankenhaus hätten, wenn die Aufnahme erforderlich sei, weil das Behandlungsziel nicht durch ambulante Behandlung einschließlich häuslicher Krankenpflege erreicht werden könne,
- und daß sie das Wirtschaftlichkeitsgebot des § 12 SGB V einzuhalten hätten.

Der Datenkatalog des § 301 Abs. 1 SGB V werde von ihnen lediglich als Mindestmaß der zu übermittelnden Daten angesehen. Diese Argumente haben mich nicht überzeugt. Da die Landesverbände erklärt haben, sie sähen sich im Einklang mit den Spitzenverbänden der Krankenkassen, werde ich mich darum bemühen, zusammen mit dem Bundesbeauftragten und den Landesbeauftragten für den Datenschutz eine bundeseinheitliche Klärung herbeizuführen.

2.6.2 Datenschutz im öffentlichen Gesundheitsdienst

Im 12. Jahresbericht (S. 40) habe ich darauf hingewiesen, wie dringlich es sei, eine bereichsspezifische Rechtsgrundlage für die Datenverarbeitung im öffentlichen Gesundheitsdienst im Lande Bremen zu schaffen. Der Senat hat in seiner Stellungnahme zu dem Bericht mitgeteilt, der Senator für Gesundheit habe mit der Erarbeitung eines Entwurfs eines Gesetzes über den öffentlichen Gesunheitsdienst begonnen, in dem auch datenschutzrechtliche Regelungen aufgenommen werden sollten.

Vorläufig sind folgende Verbesserungen in der Praxis des öffentlichen Gesundheitsdienstes erreicht worden:

Das **Gesundheitsamt Bremerhaven** hat zugesagt, künftig in seine Zentralkartei keine Vermerke mehr über die Inanspruchnahme von Beratungs- oder Therapieangeboten des Sozialpsychiatrischen Dienstes aufzunehmen. Etwas anderes soll nur für die Fälle gelten, in denen gesetzliche Pflichtaufgaben mit Rechts- oder Kostenfolgen wahrgenommen werden oder in denen Gutachten für andere Stellen erstattet werden. Dies hat zur Folge, daß im Sozialpsychiatrischen Dienst eine getrennte Aktenführung eingerichtet werden muß. Außerdem soll künftig gewährleistet sein, daß Aufzeichnungen, die Mitarbeiter des Sozialpsychiatrischen Dienstes über Inhalte von Beratung/Therapie, insbesondere über das, was ihre Klienten ihnen anvertraut haben, anfertigen, anderen Personen, auch solchen innerhalb des Amtes, nur mit Einwilligung der Betroffenen zugänglich gemacht werden. Anderes soll hier nur für die aus organisatorischen Gründen gespeicherten Grunddaten des Klienten sowie für Vermerke/Berichte der Mitarbeiter gelten, in denen sie ihre Arbeit dokumentieren. In diesem Zusammenhang habe ich darauf hingewiesen, daß sorgfältig geprüft werden müsse, inwieweit es überhaupt erforderlich sei, nicht anonymisierte personenbezogene Daten zu verarbeiten. Ich habe empfohlen, den Inhalt dieser Vermerke/Berichte soweit möglich mit den jeweiligen Klienten abzusprechen. Schließlich hat das Gesundheitsamt erklärt, sein amtsärztlicher Dienst greife bei der Erstattung von gutachterlichen Stellungnahmen auf frühere Vorgänge nur mit ausdrücklicher Einwilligung des Betroffenen zurück.

Das **Hauptgesundheitsamt Bremen** will seine Gesundheitskartei, in der Vorgänge des amtsärztlichen Dienstes registriert sind, entsprechend den mit dessen Tätigkeit verfolgten Zweckbestimmungen ordnen. Die Vorgänge sollen in vier „Blöcke" eingeteilt werden:

— Untersuchungen im Rahmen dienstrechtlicher Maßnahmen,

— Untersuchungen im Rahmen des Sozialhilfeverfahrens,

— Untersuchungen im Rahmen von Berufsausbildungen,

— Untersuchungen für andere Zwecke.

Die hiernach geordneten Vorgänge sollen in der Kartei getrennt registriert werden, die Vorgänge selbst sollen getrennt abgeheftet werden, nach Einführung der EDV sollen die Daten getrennt gespeichert werden. Existieren für einen Betroffenen Vorgänge in mehreren dieser „Blöcke", so soll der Amtsarzt nur Zugriff zu den Vorgängen der Kategorie erhalten, in deren Rahmen er tätig wird. Auch innerhalb einer Kategorie soll aber die Einbeziehung früherer Gutachten unterbleiben, wenn der Betroffene dem widerspricht. Ich halte dagegen eine Einwilligung des Betroffenen für erforderlich. Innerhalb der vierten Kategorie soll zusätzlich nach den einzelnen unterschiedlichen Zweckbestimmungen unterschieden werden.

Damit ist **in beiden Ämtern** ein Fortschritt in der Wahrung der beruflichen Schweigepflicht nach § 203 StGB und bei der Begrenzung der Datenverarbeitung auf die mit der Erhebung verfolgten Zwecke (§§ 12 Abs. 2, § 13 Abs. 1, 5 BrDSG) erreicht. Die zugesagten Verbesserungen des Verfahrens ersetzen jedoch nicht gesetzliche Regelungen für diesen Bereich, denn nur daraus können die Betroffenen einen Rechtsanspruch herleiten.

2.6.3 Kooperation zwischen Sozialpsychiatrischem Dienst und Psychiatrischer Klinik — Sektorarzt und Datenschutz

Im Rahmen der Psychiatriereform ergeben sich immer wieder schwierige Probleme für den Schutz der Patienten-bzw. Klientendaten und für die Einhaltung beruflicher Schweigepflichten (vgl. 12. Jahresbericht, S. 41). Im Berichtsjahr wurde ich darauf aufmerksam gemacht, daß geplant sei, die Kooperation des Sozialpsychiatrischen Dienstes (SpsD) im Hauptgesundheitsamt Bremen mit dem Zentralkrankenhaus Bremen-Ost (ZKH Ost) dadurch zu intensivieren, daß die Leiter der bezirklichen Beratungsstellen des SpsD jeweils zugleich die Funktion des Oberarztes für die psychiatrische Station im ZKH Ost übernehmen sollten, die die Patienten aus dem jeweiligen Bezirk aufnimmt („Sektorarzt"). Damit soll — so die Begründung — die notwendige langfristige personelle und konzeptionelle Kontinuität der Behandlung chronisch psychisch Kranker gewährleistet werden. Gegen diese Personalunion werden von Mitarbeitern des ZKH fachliche Bedenken erhoben: Der Kranke werde mit einem geschlossenen System konfrontiert, ihm werde die Möglichkeit genommen, in verschiedenen Institutionen auf neue unvoreingenommene Gesprächspartner zu stoßen.

Diese fachliche Kontroverse birgt auch datenschutzrechtliche Aspekte in sich. Der Patient/Klient, der den SpsD zur Beratung/Therapie aufsucht, ist in seinem Vertrauen darauf zu schützen, daß sein Gegenüber seine Daten, die ihm in diesem Rahmen anvertraut werden, nur mit seiner Einwilligung bzw. Entbindung von der Schweigepflicht an andere Stellen übermittelt, vgl. § 203 StGB. Dies muß auch im Verhältnis zum ZKH Ost gelten, zumal Klinikärzte auch im Verfahren zur Unterbringung von psychisch Kranken mitwirken, vgl. etwa §§ 4 bis 6, 23, 27, 29 PsychKG. Dem steht eine möglicherweise gegenläufige Rolle von Sozialarbeitern des SpsD als Vertreter des Betroffenen im Unterbringungsverfahren gegenüber, §§ 20 und 22 PsychKG.

Ich habe Vorschläge zum Schutz der Vertraulichkeit der Beratungs-/Therapiegespräche im SpsD gemacht, die im Rahmen der geplanten Neustrukturierung durchweg berücksichtigt werden sollen. Die Vorschläge sollen gewährleisten,

- daß die Einwilligung/Entbindung von der Schweigepflicht durch den Klienten eingeholt wird, bevor der SpsD an andere Stellen, auch an das ZKH Ost, personenbezogene Daten des Klienten übermittelt,

- daß der SpsD dem Klienten eigene Leistung nicht deshalb vorenthält, weil dieser Einwilligung/Entbindung von der Schweigepflicht verweigert bzw. widerruft,

- daß der Klient über die Kooperationsbeziehungen des SpsD insbesondere zum ZKH Ost und auch über seine eigenen Rechte ausreichend informiert wird.

Auch die Sektorärzte sollen ausdrücklich in jeder der beiden Funktionen, die sie in Personalunion vereinen, auf die Wahrung des ärztlichen Berufsgeheimnisses verpflichtet werden. Auch sie dürfen Daten des Klienten/Patienten aus dem einen ihrer Tätigkeitsbereiche in den anderen nur dann übermitteln, wenn der Betroffene sie zuvor von ihrer Schweigepflicht entbunden hat. Es ist zu befürchten, daß die Sektorärzte in ihrer Doppelfunktion in schwierige Situationen gestellt sein werden. Sie werden damit umgehen müssen, daß sie Daten, die ihnen aus einer Beratung im SpsD bekannt sind, nicht ohne weiteres an die Mitarbeiter der Klinik weitergeben dürfen. Ebenso wenig werden sie alle ihre Kenntnisse aus der Beratung für ärztliche Zeugnisse nach Maßgabe des PsychKG verwerten dürfen.

Das PsychKG bietet hierfür mangels normenklarer Befugnisnormen keine ausreichende Rechtsgrundlage. Die Beibehaltung der gegenwärtigen personellen Trennung zwischen Beratungsstelle und Krankenhaus ist im Interesse der Wahrung der beruflichen Schweigepflichten der beteiligten Psychologen und Ärzte vorzuziehen. Mir ist aber von Seiten des SpsD und von Seiten des ZKH versichert worden, daß es möglich sein werde, die beruflichen Schweigepflichten trotz der geplanten Personalunion zu wahren.

Es bleibt abzuwarten, ob die zu diesem Zweck getroffenen Vorkehrungen sich in der Praxis bewähren werden.

2.6.4 Verarbeitung personenbezogener Daten Krebskranker

Angeregt durch eine Forderung der 4. Großen Krebskonferenz vom Dezember 1989 bereitet der Bundesminister für Jugend, Familie, Frauen und Gesundheit den Entwurf eines **Bundeskrebsregistergesetzes** vor. Es soll Rechtsgrundlage für ein flächendeckendes Netz von regionalen Krebsregistern sein. Auf der einen Seite würde ein solches Gesetz der von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in den Jahren 1981 und 1982 erhobenen Forderung entsprechen, daß Krebsregister nur auf einer gesetzlichen Grundlage geschaffen werden dürften. Auf der anderen Seite aber hat die Konferenz auf ihrer Sitzung im Oktober 1990 ihre Bedenken gegen ein Gesetz bekräftigt, das den Ärzten die Befugnis einräumt, die Daten der Betroffenen ohne deren Einwilligung an ein solches Register zu melden (siehe Anlage 5). Die Datenschutzbeauftragten sind nach wie vor der Auffassung, daß Krebsregister nur mit Einwilligung der Betroffenen oder auf anonymer Basis geführt werden dürfen. Für beides gibt es bereits praktizierte Modelle, die Einwilligungsmodelle in Nordrhein-Westfalen und in Hamburg und das dezentralisierte Verschlüsselungsmodell in Baden-Württemberg. Leider hat es bisher den Anschein, als würden von Seiten der anwendungsorientierten epidemiologischen Forschung, aber auch im zuständigen Bundesministerium diese Modelle nicht ernsthaft in Erwägung gezogen. Ich habe den Senator für Gesundheit gebeten, die Position der Datenschutzbeauftragten zu unterstützen.

Im Lande Bremen sind die Bemühungen zur Einrichtung einer **Tumordokumentations- und Nachsorgeleitstelle** erneut aufgenommen worden. Ich habe besonderen Wert darauf gelegt, daß in jedem Fall vor Speicherung personenbezogener Daten die Einwilligung/Entbindung von der ärztlichen Schweigepflicht durch die betroffenen Patienten eingeholt werden müsse und daß die Leitstelle Patientendaten lediglich im Auftrag von Krankenhäusern und niedergelassenen Ärzten zur Unterstützung von deren Behandlung verarbeiten dürfe. Für darüber hinausgehende Zwecke, vor allem der Forschung, dürften nur aggregierte und anonymisierte Daten bereitgestellt werden. Dabei geht es mir auch darum zu verhindern, daß ein Krebsregister ohne die erforderliche Rechtsgrundlage errichtet wird. Der Übernahme der Trägerschaft durch den Landesverband Bremen der Deutschen Krebsgesellschaft e. V. habe ich unter der Voraussetzung zugestimmt, daß sie sich verpflichtet, die Regelungen des Bremischen Datenschutzgesetzes zu beachten, und sie sich auf dieser Grundlage meiner Kontrolle unterwirft. Der Senator für Gesundheit und der Landesverband Bremen der Deutschen Krebsgesellschaft haben ein Datenverarbeitungs- und Datenschutzkonzept, ein Informationsblatt und einen Vordruck zur Einwilligung bzw. Entbindung von der ärztlichen Schweigepflicht mit mir abgestimmt.

2.6.5 Patientendatenschutz in kirchlichen Krankenhäusern

Das bremische Krankenhausdatenschutzgesetz gilt auch für die kirchlichen Krankenhäuser, es sei denn die öffentlichrechtlichen Religionsgesellschaften erlassen eigene bereichsspezifische Bestimmungen, die den Zielen des bremischen Krankenhausdatenschutzgesetzes entsprechen. Die betreffenden Religionsgesellschaften haben rechtzeitig zum 01. April 1990 Rechtsnormen über den Patientendatenschutz in kirchlichen Krankenhäusern erlassen. Hierbei handelt es sich um,

- die Verordnung zum Schutz von Patientendaten in kirchlichen Krankenhäusern vom 15. März 1990 der Bremischen Evangelischen Kirche,
- die Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Hildesheim vom 01. März 1990 und
- die Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Osnabrück vom 21. März 1990

Mit Vertretern der Kirchen habe ich bestehende Unklarheiten bei der Auslegung dieser Rechtsvorschriften geklärt und sie in der Absicht beraten, einen Vollzug zu gewährleisten, der den Regelungen des Bremischen Krankenhausdatengesetzes entspricht. Dabei konnte ein zwar in Nuancen unterschiedlicher, aber insgesamt vergleichbarer Datenschutzstandard erreicht werden.

2.7 Umweltschutz

Altlastenkataster

Der Senator für Umweltschutz und Stadtentwicklung hat mir dargelegt, daß als Grundlage wirksamer Umweltschutzmaßnahmen Informationen über die Umwelt und die schädigenden Einflüsse auf die Umwelt unentbehrlich sind. Immer häufiger und in immer größerem Umfange werden Informationen über Art und Ausmaß der Umwelteinwirkungen sowie über Gesundheits- und Umweltgefährdungen systematisch gesammelt und in Dateien, besonderen Verzeichnissen, Katastern oder Kartierungen nachgewiesen. Die Nutzung derartiger Datensammlungen und die Verfügbarkeit der Daten sollen durch den Einsatz der automatisierten Datenverarbeitung effizient gestaltet werden. Aus diesem Bereich sind insbesondere die sogenannten Altlasten-, Altstandort- und Altdeponienkataster zu erwähnen. Derartige Kataster enthalten grundstücksbezogene, personen- oder betriebsbezogene Informationen. Bereits in meinem 12. Jahresbericht (S. 43) habe ich über eine vollständiger Übersicht kontaminierter Altstandorte (Altlastenkataster) berichtet.

Die vielen Anfragen von Grundstückskäufern und Eltern machen deutlich, daß Altlasten als eine besondere Gefährdung für die Umwelt und damit auch für die Menschen wahrgenommen werden. Ich stimme mit der Auffassung des Senators für Umweltschutz und Stadtentwicklung überein, wonach das Altlastenkataster nur dann einen Sinn erfüllt, wenn es in einem gewissen Rahmen der Öffentlichkeit zugänglich gemacht wird. Aber auch öffentliche Stellen der bremischen Verwaltung benötigen für ihre Aufgabenerfüllung Daten aus dem Kataster.

Die Übermittlung der im Altlastenkataster enthaltenen Daten an Interessierte wirft erhebliche datenschutzrechtliche Probleme auf, da diese Daten nach § 12 Abs. 1 BrDSG der strikten Zweckbindung unterliegen. Eine Zweckänderung ist nur unter den Voraussetzungen des § 12 Abs. 2 BrDSG zulässig, insbesondere wenn hierdurch erhebliche Nachteile für das Gemeinwohl oder schwerwiegende Beeinträchtigungen der Rechte Einzelner verhindert oder beseitigt werden sollen. Diese Voraussetzungen liegen jedoch nicht in jedem Fall vor, wenn der Allgemeinheit und den interessierten Behörden (z. B. Bauamt Bremen-Nord, Bauordnungsamt, Planungsamt, Wasserwirtschaftsamt, Grundstücksamt sowie die Kataster- und Vermessungsverwaltung) in einem großen Umfange Altlastendaten zur Verfügung gestellt werden sollen. Um den verschiedenen Interessen in einem ausgewogenen Maße Rechnung tragen zu können, bedarf es bereichsspezifischer Datenverarbeitungsregelungen.

Ich habe daher der senatorischen Behörde empfohlen, im Abfallrecht normenklar und abschließend zu regeln, unter welchen Voraussetzungen sowohl öffentliche Stellen als auch Privatpersonen Auskünfte aus dem Altlastenkataster erhalten dürfen.

2.8 Bauwesen

2.8.1 Änderung der Bremischen Landesbauordnung

In meinem 12. Jahresbericht (S. 45) habe ich auf die Notwendigkeit zur Schaffung von Datenverarbeitungsregelungen, insbesondere zur Durchführung des Baugenehmigungsverfahrens, in der Bremischen Landesbauordnung hingewiesen. Im Sommer 1990 ist die Bremische Landesbauordnung in Kraft getreten (Brem.GBl. S. 147). Meine Anregungen wurden berücksichtigt. Danach sind die Bauordnungsbehörden befugt, zur Wahrnehmung ihrer Überwachungsaufgaben bei der Errichtung, Änderung, dem Abbruch, der Nutzung sowie der Unterhaltung baulicher Anlagen einschließlich der Erhebung von Gebühren, zur Führung des Baulastenverzeichnisses sowie zur Verfolgung von Ordnungswidrigkeiten die erforderlichen personenbezogenen Daten von den am Bau verantwortlich Beteiligten, Grundstückseigentümern, Nachbarn, Baustoffproduzenten sowie sonstigen am Verfahren zu Beteiligenden zu verarbeiten.

Eine Übermittlung personenbezogener Daten an Personen und Stellen ist nur unter den im Gesetz genannten Voraussetzungen zulässig. Eine regelmäßige Datenübermittlung ist nur zulässig unter Festlegung des Anlasses und des Zwecks der Übermittlung, der Datenempfänger und der zu übermittelnden Daten.

Aufgrund der Vielzahl der unterschiedlichen an Baugenehmigungsverfahren zu beteiligenden Behörden war es nicht möglich, im Gesetz zu regeln, welche einzelnen personenbezogenen Daten zu welchem einzelnen Zweck erhoben und übermittelt werden dürfen. Aus diesem Grunde enthält die Bremische Landesbauordnung nunmehr eine Regelung, wonach der Senator für das Bauwesen durch Rechtsverordnung nähere Bestimmungen über Art, Umfang und Zweck der Datenerhebung, der Datenübermittlung und regelmäßiger Datenübermittlungen erläßt.

Ich erwarte, daß der Senator für das Bauwesen mich gem. § 14 Abs. 2 BrDSG vor Erlaß der Rechtsverordnung beteiligen wird.

2.8.2 Vermessungs- und Katastergesetz

In meinem 11. Jahresbericht (Seite 96) habe ich im Zusammenhang mit der beabsichtigten Einführung eines automatisierten Liegenschaftsbuches festgestellt, daß die bisherigen Datenverarbeitungsregelungen im Bremischen Vermessungs- und Katastergesetz den datenschutzrechtlichen Anforderungen angepaßt werden müssen. Nachdem der Senator für das Bauwesen einen Novellierungsentwurf vorgelegt hatte, ist das weitere Gesetzgebungsverfahren von mir datenschutzrechtlich begleitet worden. Ende 1990 ist das neue Vermessungs- und Katastergesetz (Brem.GBl. S. 313) von der Bremischen Bürgerschaft verabschiedet worden.

Das Gesetz entspricht nunmehr den datenschutzrechtlichen Anforderungen und enthält folgende wesentliche Regelungen:

Zweck des Liegenschaftskatasters ist es, den Anforderungen des Rechtsverkehrs, der Verwaltung und der Wirtschaft an ein Basis-Informationssystem gerecht zu werden. Dabei sind insbesondere die Bedürfnisse der Planung und Bodenordnung,

die Ermittlung von Grundstückswerten sowie der Umwelt und Naturschutz angemessen zu berücksichtigen. Aus dieser präzisen Zweckbestimmung ergibt sich bereits der Rahmen für die Zulässigkeit und den Umfang der Datenverarbeitung.

Das Gesetz enthält nunmehr eine Regelung, wonach die Katasterbehörden befugt sind, die für die Zwecke des Liegenschaftskatasters erforderlichen und geeigneten personenbezogenen Daten zu verarbeiten.

So ist normenklar aufgelistet und festgelegt worden, welche Sachdaten und persönlichen Daten erhoben und gespeichert werden dürfen.

Darüber hinaus enthält das Gesetz eindeutige Regelungen, unter welchen Voraussetzungen Daten aus dem Liegenschaftskataster an andere öffentliche Stellen und sonstige Personen und Stellen übermittelt werden dürfen. Da es sich bei dem Liegenschaftskataster um ein „halböffentliches" Kataster handelt, dürfen im Einzelfall an sonstige Personen und Stellen personenbezogene Daten durch Einsichtnahme oder Auskunft bekannt gegeben werden, wenn die Empfänger ihr berechtigtes Interesse aufgrund ihrer Bedürfnisse im Rechtsverkehr, in der Verwaltung oder der Wirtschaft glaubhaft darlegen und schutzwürdige Belange des Eigentümers oder Erbbauberechtigten nicht beeinträchtigt werden. Dabei ist die Bekanntgabe auf die erforderlichen Daten zu beschränken, und die Empfänger der Daten sind verpflichtet, diese nur für den Zweck zu nutzen, zu dem sie übermittelt worden sind.

Die wesentliche Änderung des Vermessungs- und Katastergesetzes war deshalb notwendig geworden, weil beabsichtigt ist, in Zukunft ein automatisiertes Liegenschaftsbuch zu führen. Das neue Gesetz enthält deshalb eine Regelung, wonach bei automatisierter Führung des Liegenschaftskatasters u. a. Grundbuchämter, Finanzbehörden sowie planende und bauende öffentliche Stellen mit Hilfe automatisierter Abrufverfahren das Liegenschaftskataster einsehen und daraus Auszüge erhalten können. Ein derartiges Abrufverfahren darf jedoch nur durch eine Rechtsverordnung des Senators für das Bauwesen eingeführt werden, in dem die Datenempfänger, die Datenart und der Zweck des Abrufs festzulegen sind. Hierbei bin ich gem. § 14 Abs. 2 BrDSG vorher zu beteiligen.

2.8.3 Gesetz über das Friedhofs- und Bestattungswesen

Am 01. Januar 1991 ist das Gesetz über das Friedhofs- und Bestattungswesen in Kraft getreten (Brem.GBl. 1990, S. 303). Das Gesetz berücksichtigt meine Anregungen.

So trägt es dem Grundsatz Rechnung, daß das allgemeine Persönlichkeitsrecht auch Wirkungen über den Tod hinaus entfaltet. Das Gesetz enthält präzise Regelungen, zu welchem jeweiligen Zwecke welche personenbezogenen Daten der Verstorbenen, der Angehörigen der Verstorbenen, der Nutzungsberechigten sowie der im Friedhofs- und Bestattungsgewerbe Tätigen verarbeitet werden dürfen.

Zu folgenden Zwecken dürfen personenbezogene Daten der jeweiligen Personengruppen erhoben und gespeichert werden:

- Bewirtschaftung und Verwaltung der Friedhöfe, insbesondere Festsetzung und Einziehung von Gebühren,
- Klärung der Nutzungsrechtsnachfolge,
- Genehmigungsverfahren über Erd- und Feuerbestattungen außerhalb von Friedhöfen.

Darüber hinaus regelt das Gesetz, welche personenbezogenen Daten zu welchen Zwecken an andere Stellen übermittelt werden dürfen.

2.8.4 Verarbeitung personenbezogener Daten von Einwendern bei Bauleitplanungen und Planfeststellungsverfahren

Vielfach ist die Frage erörtert worden, unter welchen Voraussetzungen und in welchem Umfange personenbezogene Daten von Einwendern bei Bauleitplanungen und Planfeststellungsverfahren verarbeitet werden dürfen. Hintergrund ist, daß die einschlägigen Gesetze (z. B. Baugesetzbuch, Bundesimmissionschutzgesetz und Luftverkehrsgesetz) keine ausreichenden Datenverarbeitungsregelungen enthalten (vgl. 10. Jahresbericht, S. 94).

Das Bundesverfassungsgericht hat mit Urteil vom 24. Juli 1990 — 1 BvR 1244/87 nunmehr für diesen Zusammenhang die grundsätzliche Entscheidung getroffen, daß Daten einer besonderen Zweckbindung unterliegen, die ein Einwendungsführer der Planfeststellungsbehörde preisgibt, um ihr eine sachgerechte Beurteilung der geltend gemachten Einwendungen zu ermöglichen. Das Gericht hat festgestellt, daß die Zweckbindung durch eine öffentliche Bekanntmachung der nichtanonymisierten Daten unterlaufen und im Ergebnis aufgelöst wird.

Des weiteren hat das Bundesverfassungsgericht ausgeführt, daß es sich bei einer solchen Bekanntmachung datenschutzrechtlich um eine Datenübermittlung „auf Vorrat" handelt, weil weder vorhersehbar noch bestimmbar ist, wer von diesen Daten Kenntnis erlangen wird und wie diese Daten verwendet werden.

Mit diesem Urteil hat das Bundesverfassungsgericht erneut allgemeine Grundsätze aus dem Volkszählungsurteil bestätigt. Dieses Urteil bedeutet, daß die im Lande Bremen noch geübte Verwaltungspraxis, die namentliche Nennung von Einwendern in Mitteilungen des Senats an die Bremische Bürgerschaft zu veröffentlichen, geändert werden muß.

2.9 Wirtschaft, Technologie und Außenhandel

Wirtschaftsstrukturpolitisches Aktionsprogramm

Der Senator für Wirtschaft, Technologie und Außenhandel beabsichtigt zur Umsetzung und Kontrolle des Wirtschaftsstrukturpolitischen Aktionsprogramms (WAP) verstärkt die automatische Datenverarbeitung einzusetzen. Die Wirtschaftsförderungsausschüsse der Deputation für Wirtschaft, Technologie und Außenhandel sowie die Finanzdeputation haben am 19. 07. 1989 der Erteilung eines Auftrags zur Entwicklung eines DV-Rahmenkonzepts für die Umsetzung und die Kontrolle des WAP zugestimmt.

Mit der Entwicklung des DV-Rahmenkonzepts wurde eine Software-Entwicklungsfirma beauftragt, die Ende Februar 1990 ein DV-Rahmenkonzept vorgelegt hat. Dieses DV-Rahmen-Konzept geht von einem zukunftsicheren und komfortablen Anwendungssystem aus, das neben der Textverarbeitung, Tabellenkalkulation, Geschäftsgrafik und ergänzende DV-Anwendungen, sowie eine prozeßorientierte Vorgangsbearbeitung enthält. Diese DV-Anwendungen enthalten Module für

- ein Haushalts-, Planungs- und Kontrollsystem
- eine integrierte Antragsbearbeitung
- ein integriertes Vorlagen-, Erstellungs- und Bearbeitungsverfahren
- ein wirtschaftsstrukturpolitischen Planungs- und Kontrollsystem
- eine Projekt- und Terminverwaltung und
- ein Dokumenten- und Archivierungssystem.

Der Senator für Wirtschaft, Technologie und Außenhandel beabsichtigt, in mehreren Schritten die Realisierung des DV-Konzepts umzusetzen. Das Ziel ist eine behördenweite vernetzte DV-Struktur. Diese DV-Struktur soll zunächst mit Standard-Software ausgestattet und für Standard-Anwendungen zur Verfügung stehen. Des weiteren soll eine DV-Unterstützung der Haushaltssachbearbeitung realisiert werden. Danach sollen die Haushaltsüberwachung und die Mittelabflußplanung kontrolliert, Haushaltsansätze und die Finanzplananansätze ermittelt und eingegeben, sowie die Haushaltsmittel zahlbar und nachgewiesen werden. Als nächster Schritt ist die Erstellung von Individual-Software zur integrierten Antragsbearbeitung vorgesehen. Diese integrierte Antragsbearbeitung soll eine DV-gestütze Antragsbearbeitung und -prüfung unter referatsübergreifenden Bedingungen gewährleisten. Es würden dann allen Anwendern alle Daten aus dem Dokumenten- und Archivierungssystem einschließlich der Haushaltsdatei zur Verfügung stehen. Ebenso sollen die Vorlagen für die Entscheidungen der Behörden und die Beteiligung anderer Stellen (z. B. Wirtschaftsförderungsausschüsse) erstellt, verändert und überwacht werden.

Die damit einhergehenden Vorschläge zur DV-Architektur sehen eine Vernetzung aller DV-Geräte und deren Steuerung durch einen Hauptrechner innerhalb der senatorischen Behörde vor. Außerdem soll die Möglichkeit des Datenaustausches z. B. mit anderen Behörden, Gesellschaften und Kammern über öffentliche Telekommunikationsnetze, wie DATEX-P, Mailbox, ISDN oder ähnliches, geschaffen werden.

In dem gesamten DV-Konzept ist der Datenschutz auf die Aussage reduziert, „ein entsprechendes Feinkonzept für den Datenschutz und die Zugriffsberechtigung sei zu erstellen und später zu implentieren". Auf die Planung zum Ausbau dieses automatisierten Informationssystem bin ich erst im Mai 1990 durch Zufall gestoßen. Spätestens mit dem Beschluß der Deputation, über die Erteilung des Entwicklungsauftrags hätte ich über das Vorhaben unterrichtet werden müssen. Dieses ist unterblieben und stellt einen Verstoß gegen § 27 Abs. 4 BrDSG dar.

Das vorstehend nur skizzierte umfangreiche DV-Konzept wirft eine Reihe von datenschutzrechtlichen Fragen auf, die hier auch nur angerissen werden können.

Im Rahmen des wirtschaftsstrukturpolitischen Aktionsprogramms werden nicht nur die Daten von juristischen Personen, sondern auch, insbesondere bei der Förderung der mittelständischen Gewerbebetriebe, die von natürlichen Personen verarbeitet werden. Daß es sich hier um sehr sensible Daten, wie Vermögens- und Besitzverhältnisse, Steuerdaten, Erträge und Planungsvorhaben handelt, liegt auf der Hand. Um diese Daten zu erheben, zu verarbeiten und zu nutzen, bedarf es gem. § 3 des BrDSG einer Rechtsgrundlage. In einem Gespräch stand der Senator für Wirtschaft, Technologie und Außenhandel auf dem Standpunkt, daß es einer Rechtsvorschrift nicht bedürfe, da der Antragsteller regelmäßig in die Datenverarbeitung einwilligen würde. Ich habe darauf hingewiesen, daß eine solche Einwilligung nicht „freiwillig" sei, da die Nicht-Einwilligung dazu führe, daß eine Wirtschaftsförderungsmaßnahme nicht bearbeitet und damit bewilligt werden kann. Diese Einwilligung wäre damit nicht freiwillig, sondern gebunden. Ich halte deshalb die Schaffung einer ausreichenden bereichsspezifischen Rechtsnorm für den Datenschutz im Bereich der Wirtschaftsförderung für unerläßlich.

Insbesondere wegen der vorgesehenen Vernetzung muß die Nutzung der Daten und die Zweckbindung geregelt sein. Auch die geplante Möglichkeit des Datenaustausches mit anderen Behörden, Gesellschaften und Kammern über öffentliche Netze bedarf einer grundsätzlichen Entscheidung des Gesetzgebers. Ebenso sind die Voraussetzungen nach § 14 BrDSG von ihm zu schaffen.

2.10 Finanzen

2.10.1 Änderung der Abgabenordnung

Im Berichtszeitraum erhielt ich einen Entwurf zur Änderung der Abgabenordnung (Entwurf), mit dem neben anderem, auch bereichsspezifische Regelungen zum Datenschutz in die Abgabenordnung aufgenommen werden sollen. Ich habe den Senator für Finanzen auf folgendes hingewiesen:

Nach dem Entwurf sollen meine Kontrollrechte zwar nicht mehr in dem Maße begrenzt, wie es nach den bisherigen Entwürfen vorgesehen war, es soll jedoch meine Kontrollkompetenz der des Bundesbeauftragten angeglichen werden. Dieses würde dazu führen, daß meine Rechte hinsichtlich der Kontrolle von Akten auf die Fälle beschränkt werden, in denen der Betroffene eine Datenschutzverletzung geltend macht oder hinreichende Anhaltspunkte für eine derartige Verletzung vorliegen. Diese Kontrollbeschränkung halte ich für unakzeptabel, denn § 27 BrDSG ermächtigt mich – ohne Anlaß – sowohl die Dateien als auch die Akten hinsichtlich einer ordnungsgemäßen Datenverarbeitung zu kontrollieren. Den Kontrollumfang seiner Behörden regelt der Landesgesetzgeber.

Nach dem Entwurf verletzt ein Amtsträger das Steuergeheimnis, wenn er geschützte Daten, die ihm in einem Steuerverfahren bekannt werden, unbefugt offenbart oder verwendet oder im automatischen Verfahren unbefugt abruft. Der Schutzbereich des Gesetzes wird durch eine solche Vorschrift nicht weit gezogen, vielmehr muß auch der Gefährdung des Steuergeheimnisses mit gesetzlichen Mitteln entgegengewirkt werden. Eine Gefährdung des Steuergeheimnisses tritt z. B. auch dann ein, wenn technische und organisatorische Sicherungsmaßnahmen bei dem automatiserten Abrufverfahren nicht getroffen werden. Dieses könnten sein, die nicht ordnungsgemäße Vergabe von Zugriffsrechten oder die nicht ausreichend Protokollierung der Abrufe.

Des weiteren bin ich der Auffassung, daß die Offenbarungsbefugnisse zu weit gefaßt sind, denn die Steuerverwaltung sieht darin, neben dem Einzelauskunftsfall der von dem zuständigen Amtsträger zu entscheiden ist, die Befugnis und Verpflichtung Steuerdaten in einem bundeseinheitlichen Informationssystem – zum Abruf für alle Finanzbehörden – zu speichern. Dieses würde die Steuerdaten in

den Zugriff aller anderen Amtsträger (praktisch aller Steuerbeamten) stellen. Ein bundesweit umfassendes Überwachungssystem wäre geschaffen. Gegen ein solch undifferenziertes System habe ich grundsätzliche Bedenken. Zumindest wäre die Zurverfügungstellung von Steuerdaten normenklarer zu fassen und wären die Anlässe und Zwecke, für die offenbart werden darf, eindeutiger zu regeln.

Ebenso sieht der Entwurf vor, daß Steuerdaten auch zur Gewinnung von Vergleichsdaten verarbeitet und genutzt werden. Soweit diese Vorschrift eine „Rasterung" der Steuerpflichtigen beabsichtigt, um abweichendes steuerliches Verhalten von Steuerpflichtigen festzustellen und auswerten zu können, ist sie abzulehnen. Dieses Verfahren wäre mit der Würde des Menschen nicht zu vereinbaren.

Darüber hinaus sieht der Entwurf vor, daß die Steuerverwaltung befugt sein soll, die Daten anderer Personen, die der Steuerpflichtige z. B. in seiner Steuererklärung angibt, auch für deren Besteuerung zu verwerten. Diese Norm würde gegen den datenschutzrechtlichen Grundsatz verstoßen, daß die Daten grundsätzlich beim Betroffenen zu erheben sind, denn nur so kann er sein informationelles Selbstbestimmungsrecht wahrnehmen. Durch die vorgesehene Vorschrift würde jede andere Informationsquelle in der Steuerverwaltung verwertbar und ein umfassendes Datennetz geknüpft.

2.10.2 Steuerdatenabrufverordnung

In meinem 10. Jahresbericht (S. 90) habe ich bereits ausführlich über den Entwurf einer Steuerdatenabrufverordnung auf der Grundlage des § 30 Abs. 6 Abgabenordnung (AO) berichtet. Der Senator für Finanzen hat mich im Berichtshalbjahr über zwei neue Entwürfe unterrichtet. Diese Entwürfe stellen eine datenschutzrechtliche Verbesserung im Bereich der Abgabenordnung dar, allerdings wurden meine grundsätzlichen Bedenken nicht ausgeräumt. Sie bestehen insbesondere für folgende Problembereiche fort:

Ich bin nach wie vor der Auffassung, daß die Ermächtigungsnorm des § 30 Abs. 6 AO eine so weitreichende Regelung nicht deckt.

Die vorgesehenen Abrufregelungen zur Wahrnehmung der Dienst- und Fachaufsicht, der Bearbeitung von Beschwerden und Billigkeitsmaßnahmen und der Rechnungsprüfung sind für die Steuerverfahren nicht erforderlich.

Die Begriffsbestimmung „offenbaren" setzt nach dem allgemeinen Sprachgebrauch ein Tätigwerden des offenbarenden Amtsträgers voraus. Von der AO wird sie in der Steuerdatenabrufverordnung dergestalt abgeändert, daß alle Abrufberechtigten, und das wären bei den bremischen Finanzämtern alle Finanzbeamte, legitimiert wären alle Steuerdaten aus fast allen Veranlagungsbereichen der Steuerverwaltung abzurufen.

Der Senator für Finanzen hat zugesagt, meine Bedenken in die Erörterung der zuständigen Finanzreferenten von Bund und Ländern einzubringen.

2.10.3 Fortfall der Kontrollmitteilungen an Finanzämter

In meinem 12. Jahresbericht (S. 48) habe ich über die Kontrollmitteilungen an die Finanzämter gem. § 93 der Abgabenordnung (AO) berichtet. Danach waren insbesondere öffentliche Stellen verpflichtet, die Steuerverwaltung über die Gewährung von Vergütungen und Zuwendungen zu unterrichten. Die sog. Kontrollmitteilungen haben in § 93 AO keine ausreichende Rechtsgrundlage. Der Senator für Finanzen hat verfügt, daß die Kontrollmitteilungen nicht mehr abgegeben werden müssen und darüber hinaus zugesagt, daß die Finanzbehörden angewiesen werden, evtl. noch meldende Stellen über den Fortfall der Verpflichtung zur Abgabe einer Kontrollmitteilung zu unterrichten. Damit ist meinem Datenschutzanliegen entsprochen worden.

2.10.4 Dozentendaten zur Prüfung der Gemeinnützigkeit

In meinem 12. Jahresbericht (S. 48) habe ich darüber berichtet, daß ich die von den Finanzämtern geforderten Angaben des Honorarempfängers im Antragsformular zur Prüfung der Gemeinnützigkeit gem. §§ 51 ff. Abgabenordnung für unzulässig halte. Nach einer Erörterung im Datenschutzausschuß wurde vom Vertreter des Senators für Finanzen zugesagt auf die Angabe der Dozentendaten zu verzichten und die Formblätter entsprechend neu zu gestalten.

2.10.5 Weitere Eingaben

Vor kurzem wurde ich von einem Bürger, der in seiner Wohnung ein Büro unterhält, um Auskunft gebeten, ob das Finanzamt von ihm die Aufzeichnung aller Telefongespräche fordern könne, um zu überprüfen, welche Gespräche beruflichen oder privaten Charakter hätten, weil nur letztere bei der Einkommensteuer berücksichtigt werden könnten. Der Steuerbeamte verlange dieses unter Hinweis auf das zukünftige ISDN-Verfahren der Deutschen Bundespost-Telekom, wonach jeder Teilnehmer einen Ausdruck seiner geführten Ferngespräche erhalten könne, wie das in den Vereinigten Staaten von Amerika bereits üblich sei. Ich habe den betroffenen Bürger dahingehend beraten, daß eine Aufzeichnungspflicht über private Telefongespräche nicht bestehe und diese eklatant in das informationelle Selbstbestimmungsrecht eingreife. Im übrigen verletze dieses Verlangen auch das Fernmeldegeheimnis der Telefonpartner. Aufgrund dieser Auskunft hat der Bürger das Verlangen des Finanzamtes zurückgewiesen. Ich beabsichtige, diesen Fall mit der Steuerverwaltung prinzipiell zu erörtern.

In mehreren Fällen erreichten mich Beschwerden von Bürgern, die sich über die Adressierung von Briefen aus dem Bereich des Senators für Finanzen beklagten. In allen Fällen waren im Adressfeld Angaben enthalten, die für eine ordnungsgemäße Zustellung nicht erforderlich waren. In einem Fall konnte aus diesen Angaben entnommen werden, daß der Empfänger eine Erbschaft gemacht hatte und wer der Erblasser war. Ich habe dieses gegenüber den verursachenden Stellen bekanntgemacht, die dieses zum Anlaß nahmen, die Sachbearbeiter über die korrekte Adressierung zu belehren.

Ein Bürger wandte sich mit einer Eingabe zu einem besonderen datenschutzrechtlichen Problem an mich. Er fühle sich in seinem informationellen Selbstbestimmungsrecht betroffen, da seine Schwägerin beim Finanzamt seine Steuerangelegenheiten und deren Ehemann bei der Bank seine Geld- und Kreditangelegenheiten bearbeite. Nach Rücksprache mit dem Finanzamtsvorsteher wurde erreicht, daß die Schwägerin nicht mehr mit den Steuerangelegenheiten des Betroffenen betraut wird. An sich hätte die Schwägerin als Steuerbeamtin sich selbst gem. § 83 i. V. m. § 82 Abgabenordnung für befangen erklären müssen. Einen gleichartigen Einfluß habe ich nicht auf die Bank, deshalb habe ich dem Hilfesuchenden nahegelegt, sich selbst mit der Bitte um Abhilfe an seine Bank zu wenden oder ggf. das Kreditinstitut zu wechseln.

2.11 Durchführung der §§ 6 — 9 und 28 BrDSG

2.11.1 Datenverarbeitung im Auftrag öffentlicher Stellen

In der Vergangenheit habe ich festgestellt, daß die von öffentlichen Stellen erteilten Fremdverarbeitungsaufträge oftmals nicht mit den Bestimmungen des Bremischen Datenschutzgesetzes und der Allgemeinen Verwaltungsvorschriften zum Bremischen Datenschutzgesetz in Einklang standen (vgl. 12. Jahresbericht S. 50). Zur Verbesserung habe ich vorgeschlagen, z. B. durch vorgefertigte Vertragstexte und ein zentrales Vergabeverfahren, die Praxis zu standardisieren. Verarbeitungsaufträge über Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, sollen gem. Nr. 8.1.2 der AVV zu § 8 BrDSG nicht vergeben werden.

In seiner Stellungnahme zum letzten Jahresbericht hat der Senat erklärt, er wolle Verträge für Auftragsverarbeitung generell so gestalten, daß die Belange des Datenschutzes noch stärker beachtet werden. Die SKP sei beauftragt worden, Musterverträge zu erarbeiten. Diesen Auftrag hat die SKP bisher nicht erfüllt. Weiterhin hat der Senat sich bereit erklärt zu prüfen, inwieweit eine zentrale Vergabe zweckmäßig und durchführbar sei. Über den Verlauf und das Ergebnis dieser Prüfung bin ich bislang nicht in Kenntnis gesetzt worden.

2.11.2 Dateibeschreibung und Geräteverzeichnis (§ 7 BrDSG)

Im 11. Jahresbericht (S. 43) hatte ich bereits Vorschläge zur Umsetzung der Verpflichtungen aus § 7 BrDSG gemacht. In seiner Stellungnahme zum Jahresbericht hat der Senat damals erklärt, daß „ein zentrales Verfahren mit dezentraler Pflegemöglichkeit entwickelt werden" soll und daß das „Konzept eines förmlichen Antragsverfahrens beim ADV-Ausschuß . . . von der Senatskommission für das Personalwesen und dem Rechenzentrum der bremischen Verwaltung erarbeitet" werde. „Sobald Ergebnisse vorliegen, werden sie mit dem Landesbeauftragten für

den Datenschutz abgestimmt". Auch hat der Senat in den Allgemeinen Verwaltungsvorschriften zur Durchführung des Bremischen Datenschutzgesetzes geregelt, daß das Geräteverzeichnis zentral beim Rechenzentrum der bremischen Verwaltung zu führen und zu verwalten sei. Die Möglichkeit dezentraler Ergänzungen und Änderungen sei vorzusehen. Diese Regelung gilt auch für die Dateibeschreibung.

Bis heute liegen mir weder ein Konzept für die Gestaltung des Antragsverfahrens noch ein ADV-Antrag vor. Bei gelegentlichen Prüfungen hat sich vielmehr gezeigt, daß speichernde Stellen ihren Verpflichtungen aus § 7 BrDSG nicht nachkommen. So wurde versucht, ein Geräteverzeichnis ad hoc durch Kopieren zu erzeugen. Meine Vorschläge zur Umsetzung von § 7 BrDSG liegen seit langem vor und sollten endlich aufgegriffen werden.

2.11.3 Dateienregister (§ 28 BrDSG)

Nach § 28 BrDSG hat der Landesbeauftragte für den Datenschutz ein allgemeines (öffentliches) und ein besonderes (nichtöffentliches) Register der Dateien zu führen, in denen personenbezogene Daten gespeichert sind. Die Behörden und sonstigen öffentlichen Stellen des Landes, der Gemeinden und die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen sowie die sog. Wettbewerbsunternehmen der öffentlichen Hand sind verpflichtet, ihre Dateien zu diesem Register anzumelden. Ich habe festgestellt, daß das Register der Dateien unvollständig und nicht aktuell ist, weil die Änderungsmeldungen an das Rechenzentrum der bremischen Verwaltung nicht ordnungsgemäß erfolgen.

Das Meldeverfahren und der Inhalt der Meldungen werden in einer Rechtsverordnung, der Datenregisterverordnung, geregelt. Diese Datenregisterverordnung vom 05. Februar 1979 ist dringend novellierungsbedürftig, da sie nicht mehr dem geltenden Bremischen Datenschutzgesetzes entspricht. Ich habe im Berichtsjahr einen Entwurf einer Verordnung über das Register nach § 28 BrDSG (Dateienregisterverordnung) erarbeitet und dem Senator für Justiz und Verfassung, der Senatskommission für das Personalwesen, dem Rechenzentrum der bremischen Verwaltung und der Senatskanzlei vorgelegt. Dem Entwurf beigefügt habe ich zugleich konzeptionelle Überlegungen zu einer möglichen Datenstruktur für das neue zentrale Registerverfahren.

Auf meine Vorschläge habe ich bis heute keine Antwort erhalten. Auch der Datenschutzausschuß hat in seinem letzten Bericht den Senat aufgefordert, die Datenregisterverordnung unverzüglich den Anforderungen des novellierten Bremischen Datenschutzgesetzes anzupassen.

2.11.4 Übersicht über den Inhalt des Dateienregisters

Im Berichtsjahr habe ich eine Broschüre zum (allgemeinen) Dateienregister herausgegeben und damit meiner Pflicht aus § 28 Abs. 1 BrDSG genügt. Für jede speichernde Stelle wurden in dieser Broschüre die gemeldeten Dateien und im Anhang einzelne Dateimeldungen in vollständiger Fassung wiedergegeben. Diese Übersicht über das Dateienregister wurde von mir auf der Basis eines Datenträgers (Diskette) erstellt, den mir das Rechenzentrum der bremischen Verwaltung aus dem zentralen Registerverfahren heraus zur Verfügung gestellt hat. Nur mit erheblichem Arbeitsaufwand war es möglich, eine neue Gliederung zu erstellen und die einzelnen Angaben in bürgerfreundlicher Form für die Broschüre aufzubereiten. Die Neustrukturierung des veralteten Registerverfahrens soll diese Arbeiten erheblich erleichtern und vereinfachen.

2.12 PC-Einsatz in der Verwaltung

2.12.1 Der PC-Arbeitsplatz

Aufgrund der Planzahlen der Senatskommission für das Personalwesen und Schätzungen für den Magistrat der Stadt Bremerhaven ist davon auszugehen, daß bis Ende 1991 mehr als 1000 PC-Arbeitsplätze in der Verwaltung geschaffen sein werden. In vielen Bereichen sind oder werden die eingesetzten PC vernetzt. Die Anzahl dieser sogenannten lokalen Netze und der damit vernetzten PC ist mir nicht bekannt. Daneben gibt es erste Ansätze für die Planung eines landesweiten Datennetzes für die direkte Kommunikation von PC zu PC.

In der Vergangenheit beschränkte sich der Einsatz eines PC zumeist auf den Schreibdienst. Im Laufe der letzten Jahre ist die Anzahl der Anträge, in denen komplexe Aufgaben mit einem PC unterstützt werden sollen, stark angestiegen. Im folgenden soll dies am Beispiel eines ADV-Antrages verdeutlicht werden. Beantragt wird die Beschaffung eines einzelnen isolierten PC mit Standard-Software, der von zwei Mitarbeitern genutzt werden soll.

Der erste Mitarbeiter soll den PC für die Aufgaben der allgemeinen Verwaltung, der Haushalts- und Personalverwaltung nutzen und die Aufgabe des PC-Koordinators für seine Behörde wahrnehmen. Der PC-Einsatz umfaßt im einzelnen:

- Allgemeine Textverarbeitung
- Vordruckerstellung
- Erstellen von Tabellen und grafischen Darstellungen
- Berechnung von Verwaltungsgebühren
- Fortbildungsplanung
- Datei der Dienst-Kfz.
- Fundstellendatei
- Führung eines Inventarverzeichnisses
- Datei der Zugriffsberechtigten
- Verzeichnis der ausgegebenen Schlüssel
- Übersicht über die im Amt geführten Dateien/Karteien
- Geschäftsverteilungsplan
- Prioritätenlisten für Bau- und Renovierungsmaßnahmen,
- Termin- und Wiedervorlagekalender
- Grafische Darstellungen und Aktualisierung des Organisationsplanes
- Berechnung und Aufteilung der Reinigungsflächen
- Aktualisierung des Aktenplanes

Die Aufgabenunterstützung des zweiten Mitarbeiters umfasst:

- Allgemeine Textverarbeitung
- Vordruckerstellung
- Materialverwaltung
- Raumverteilung
- Telefonverzeichnis

Außerdem soll der zweite Mitarbeiter im Vertretungsfall Aufgaben des ersten übernehmen.

In diesem Beispiel werden hauptsächlich personenbezogene Daten der bei der speichernden Stelle Beschäftigten verarbeitet. Aus anderen ADV-Anträgen wird deutlich, daß auch bei der Verarbeitung von Bürgerdaten eine ähnlich komplexe ADV-Unterstützung eingesetzt wird.

Grund für die Zunahme derartiger ADV-Beschaffungen ist einerseits die stark gestiegene Leistungsfähigkeit der PC (Verarbeitungsgeschwindigkeit, Speicherkapazität, Kompaktheit des Gerätes, Fehlerresistenz) und andererseits der Einsatz universell anwendbarer, komplexer Standard-Software (z. B. zur Dateiverwaltung, Tabellenkalkulation, Grafikerzeugung, Netzeverwaltung). Diese Programme bieten neben den unterschiedlichen Anwendungsfunktionen auch eine eigene Programmentwicklungsumgebung mit effizienten Entwicklungswerkzeugen für die Eigenprogrammierung.

Die Software-Produkte zeichnen sich durch schnelle Erlernbarkeit, einfache Bedienung zum Teil ohne Handbuch und einfache Programmierung aus. Ein typischer Einführungsprozeß läuft folgendermaßen ab:

Nachdem der PC und die Programme für Textverarbeitung, Tabellenkalkulation und Datenbankverwaltung angeschafft sind, verschafft man sich einen Überblick über die Anwendung der bei Kollegen schon vorhandenen Programme, wählt die aus, die sich für die eigene Aufgabenstellung am besten eignen und beginnt mit der Anpassungsprogrammierung an die eigenen Bedürfnisse.

Um Mißverständnissen vorzubeugen: Programmieren in diesem Sinne meint nicht das Erstellen von Programmen mit Hilfe der Maschinensprache oder einer zusätzlichen Programmiersprache sondern die Nutzung (Parametrisierung) der durch die Standard-Software vorgegebenen Instrumente, die es ermöglichen, mit wenigen Befehlen alle gespeicherten Daten zueinander in Beziehung zu setzen, auf bestimmte Fragestellungen hin auszuwerten, Datenstrukturen zu ändern, neue Datenstrukturen aufzubauen usw. Der Benutzer ist je nach Vorbildung nach kurzer Zeit in der Lage, diese Art der Programmentwicklung durchzuführen.

Gerade die hohe Flexibilität und die universelle Nutzbarkeit dieser Programme führen zu vielfältigen Datenschutzproblemen. Der ihr innewohnende Grundgedanke einer nahezu unbegrenzten Verarbeitung vorhandener Daten und die relativ einfache Weiterentwicklung für die Verarbeitung von immer mehr Daten steht im krassen Gegensatz zu dem, was der Datenschutz fordert. Um Transparenz für betroffene Bürger und Beschäftigte schaffen zu können, ist es notwendig, Art und Umfang der gespeicherten Daten explizit festzulegen und zu bestimmen, wer für welchen Zweck welche zum Einsatz freigegebenen Anwendungen einsetzt und wer dazu auf welche Daten zugreifen darf.

Gerade dies ist durch diese Programme in Frage gestellt, da z. B. Datenbankverwaltungssysteme es ermöglichen, mit Hilfe der Abfragesprache jedes Datum mit jedem Datum in Beziehung zu setzen. Tabellenkalkulationsprogramme zeichnen sich dadurch aus, daß Tabellen einfach erweitert, verändert und mit anderen Tabellen in Beziehung gesetzt werden können. Unbefugte Auswertungen von gespeicherten Daten und Manipulationen sind nicht mehr ohne weiteres kontrollierbar.

Um diesen Risiken zu begegnen, skizziere ich im folgenden einige Lösungsmöglichkeiten:

Für den Anwender ist ein System einzurichten, das ihm ausschließlich die für seine Aufgabenstellung benötigten Daten und Programme zur Verfügung stellt. Der **Zugang zum PC-Betriebssystem** ist in der Regel zu verhindern, da auf dieser Ebene die Verarbeitung von Daten und Programmen nicht mehr kontrollierbar ist. Um dem zu begegnen, ist die Nutzung des Betriebssystems zu regeln und zwischen verschiedenen Rollen aufzuteilen: Einem Installateur, der die Hardware- und Softwarekomponenten installiert und einem Systemverwalter, der die allgemeine Funktionsfähigkeit von Hard- und Softwarekomponenten sicherstellt. Darüber hinaus ist in geeigneten Fällen ein Benutzerverwalter einzusetzen, der für die Vergabe von Zugriffsrechten zuständig ist.

Neben der Verschlüsselung, die vom Anwender mit einem eigenem Schlüsselwort durchgeführt werden kann, gibt es heute kaum noch ein PC-Sicherheitsprodukt, das nicht auch die online-Verschlüsselung von Daten ermöglicht. Der Anwender merkt von diesem Schutz nichts. Die **Verschlüsselung der Festplatte** ist eine Grundvoraussetzung für den Schutz der Daten vor dem Zugriff Unberechtigter.

Die praktische Anwendung von multifunktionalen Programmen ist dadurch gekennzeichnet, daß der Anwender seine Anwendungen selbst entwickelt. Die Phase des Betriebs — der Anwendung — vermischt sich immer wieder mit der Phase der Neu- und Weiterentwicklung. Deshalb ist die **Trennung zwischen Anwendung und Entwicklung** erforderlich. Dies setzt voraus, daß man die Anwendungsumgebung und die Programmentwicklungsumgebung eines Programmes voneinander trennen kann. Bei einigen Produkten ist dies möglich. Wenn man die neuen Gestaltungsspielräume dieser Programme nutzen will, ist es darüber hinaus erforderlich zu dokumentieren, welche Entwicklungswerkzeuge zu welchem Zweck und mit welchem Ergebnis eingesetzt werden.

Eine weitere wichtige datenschutzrechtliche Maßnahme ist die **Protokollierung der Systemnutzung,** um die nachträgliche Kontrolle einer datenschutzgerechten Verarbeitung zu ermöglichen. Durch die Protokollierung zu Datenschutzzwecken entstehen neue zusätzliche Sammlungen personenbezogener Daten (Benutzer- und evtl. Bürgerdaten). Deshalb müssen diese Daten einer engen Zweckbindung unterliegen und dürfen nur zur Datenschutzkontrolle verwendet werden. Zur Sicherstellung der Zweckbindung bieten sich folgende Maßnahmen an:

- die Auswertung der Protokolldaten im Beisein des Anwenders (Vier-Augen-Prinzip)
- eine sichere Aufbewahrung der Daten, z. B. die Speicherung in verschlüsselter Form
- festgelegte Löschungsfristen

Die Maßnahmen, die gegebenenfalls erforderlich sind, um den mit der Datenverarbeitung auf dem PC verbundenen Risiken zu begegnen, können hier nicht abschließend aufgeführt werden. Es ist zu beobachten, daß auch die Hersteller von Hard- und Software dazu übergehen, Datensicherheitskomponenten in ihre Produkte zu integrieren. Der Katalog der möglichen Maßnahmen ist daher vielfältig. Es bietet sich daher an, zugleich mit der Planung des PC-Einsatzes eine Bewertung der hiermit verbundenen Risiken vorzunehmen und hieran anschließend den Einsatz der geeigneten Sicherheitsmaßnahmen zu prüfen.

2.12.2 Richtlinien für den Datenschutz am Arbeitsplatz

Der Senat hat im August 1990 die Richtlinien für den Datenschutz am Arbeitsplatz erlassen (Brem.Abl., S. 221). Sie gelten für die Verarbeitung personenbezogener Daten beim dezentralen Einsatz von DV-Systemen (z. B. PC) und regeln die Freigabe von Programmen, die Nutzung privater und dienstlicher Hard- und Software, die organisatorischen und technischen Maßnahmen, die Datenträgerverwaltung und die Wartungsmaßnahmen. Die Richtlinien enthalten als Anlage das Muster einer Systemakte, in der die systemspezifischen und technischen Daten für einen ordnungsgemäßen Betrieb dokumentiert werden, sowie das Einsatzkonzept für ein Datenschutz- und Datensicherungs-System bei der Verarbeitung personenbezogener Daten auf isolierten Arbeitsplatzrechnern (PC). Welche Risiken der PC-Einsatz am Arbeitsplatz mit sich bringt und wie diesen begegnet werden kann, habe ich im vorgehenden Beitrag dargestellt.

Bei der Erarbeitung der Richtlinien konnte ich meine Anforderungen einbringen; es konnte jedoch nicht in allen Punkten Einigung erzielt werden. So habe ich prinzipiell gefordert, daß der Anwender keinen Zugang zu dem Betriebssystem hat, um den Anwendern jeweils nur die für ihre Aufgabenstellung erforderlichen Anwendungsprogramme und Daten zur Verfügung zu stellen. Dadurch würde eine darüber hinausgehende Verarbeitung verhindert, so könnte z. B. das Risiko der Eigenprogrammierung begrenzt oder ausgeschlossen werden.

Das Einsatzkonzept sieht dagegen vor, daß der Betriebssystemzugang nur in den Fällen gesperrt wird, in denen eine besondere Schutzwürdigkeit der Daten festgestellt wird. Dieses Stufenkonzept verlangt, über die Bewertung der Sensibilität der verarbeiteten Daten zu unterschiedlichen Anforderungen an deren Schutz zu kommen. Dem ist entgegenzuhalten, daß es grundsätzlich nicht möglich ist, einem einzelnen Datum seine Sensibilität anzusehen. Es ist kaum möglich, unterscheidbare Maßnahmenbündel für unterschiedliche Datenklassen zu definieren. Meine Kritik stütze ich auch auf die Feststellung des Bundesverfassungsgerichts in seinem Volkszählungsurteil, daß es unter den Bedingungen der automatisierten Datenverarbeitung kein „belangloses" Datum mehr gibt.

Weiter habe ich gefordert, zu Zwecken der Datenschutzkontrolle ein Protokollierungsverfahren einzusetzen. Da die Protokollierungsfunktion der eingesetzten Sicherungs-Software derzeit für die Datenschutzkontrolle wenig geeignet ist, wurde zunächst auf die Protokollierung verzichtet. Einzelheiten des Protokollverfahrens wie der Umfang, der Inhalt und die Nutzung der Protokolle sind noch zu erörtern.

Nach Inkrafttreten der Richtlinien sollte zunächst abgewartet werden, wie sie sich in der Praxis bewähren. Im Rahmen meiner Prüftätigkeit werde ich beobachten, ob der jetzt vorgeschriebene Maßnahmenkatalog ausreichend ist.

Für die Stadtverwaltung Bremerhaven liegen vergleichbare Richtlinien noch nicht vor.

2.12.3 Beratung bei der Erstellung einer neuen ADV-Beschaffungsliste

Im November 1990 wurde ich vom Rechenzentrum der bremischen Verwaltung um Stellungnahme zu den Vorschlägen für eine neue Beschaffungsliste ausgewählter ADV-Produkte gebeten. Die neue Beschaffungsliste umfaßt Hard- und Softwareprodukte und soll im Februar 1991 vom Senat beschlossen werden.

Unter den Produkten befand sich ein PC, der durch hardwareseitige Ausstattung über handelsübliche PC hinausgehende Datensicherungsfunktionen verfügt. Das RbV ging davon aus, daß die von dem PC gebotenen Sicherheitsfunktionen ausreichend seien, um genügend Schutz vor dem Zugriff Unberechtigter gem. dem Einsatzkonzept für ein Datenschutz- und Datensicherungssystem (Anlage 2 zu den Richtlinien für den Datenschutz am Arbeitsplatz vom 07. 08. 1990) zu bieten.

Nach einem Test des Geräts konnte ich erreichen, daß durch technische Umgestaltung der Schutz gegen äußere Eingriffe und Manipulationen wesentlich erhöht werden konnte. Gleichwohl erfüllen die getroffenen Sicherungsvorkehrungen nicht in vollem Umfang die Bedingungen des o. g. Einsatzkonzeptes.

Weiter habe ich zum generellen Einsatz eines in der Beschaffungsliste enthaltenen Softwareproduktes Bedenken geäußert. Die Bedienoberfläche des Produkts ermöglicht den Zugang zum Betriebssystem und kann den Wechsel des Benutzerbereiches nicht verhindern. Ich habe darauf hingewiesen, daß Softwareprodukte, die eine Trennung von Programmentwicklung und -anwendung nicht ermöglichen, hohe Datenschutzrisiken in sich bergen.

Die SKP hat die wesentlichen Punkte meiner Stellungnahme in die Senatsvorlage aufgenommen.

3. Datenschutz in Europa

Die Organe der Europäischen Gemeinschaft sind in den vergangenen Jahren von den Datenschutzbeauftragten kritisiert worden, weil befürchtet wurde, daß die Schaffung des europäischen Binnenmarktes bis zum 31.12.1992 ein enges Netzwerk grenzüberschreitender Datenflüsse zur Folge haben werde, ohne daß einheitliche Bestimmungen und Vorkehrungen zum Schutz der Persönlichkeitsrechte der EG-Bürger bei der Verarbeitung getroffen worden wären (vgl. 12. Jahresbericht, S. 54 und S. 82).

Inzwischen hat die Kommission der Europäischen Gemeinschaft am 13. 09. 1990 mitgeteilt, daß sie den anderen Gemeinschaftsorganen eine Reihe von Maßnahmen zum Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft vorgeschlagen habe. Neben einer speziellen Richtlinie zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen (ISDN-Richtlinie) handelt es sich dabei vor allem um den Vorschlag, daß der Rat eine allgemeine Richtlinie zur Harmonisierung des Datenschutzes in den Mitgliedsländern erlassen möge (Harmonisierungsrichtlinie, KOM (90) 314 endg. — SYN 187 vom 13.09.1990).

Die Kommission setzt sich das Ziel, ein gleichwertig hohes Schutzniveau in der gesamten Gemeinschaft sicherzustellen. Die Rechtsangleichung innerhalb der Gemeinschaft dürfe nicht zu einer Verringerung des in einzelnen Mitgliedsländern erreichten Schutzniveaus führen. Sie begründet dies damit, daß die einzelstaatlichen Datenschutzvorschriften das Ziel verfolgten, die Grundrechte, insbesondere das Recht auf Privatsphäre, zu garantieren, und damit, daß die EG selbst in Abs. 3 der Präambel zur Einheitlichen Europäischen Akte ihre Bindung an die Grundrechte zum Ausdruck gebracht habe. Weiter beruft sich die Kommission darauf, daß Art. 100 a des EWG-Vertrages sie verpflichte, Maßnahmen zu ergreifen, die als Mittel zur Verwirklichung des einheitlichen Binnenmarktes ein gleichwertiges Datenschutzniveau in den Mitgliedsländern garantierten. Die Kommission sieht somit nicht etwa Datenschutzregelungen an sich, sondern lediglich die Folgen als Handelshemmnis an, die daraus entstehen, daß in einzelnen Ländern der Gemeinschaft ein unzulängliches Datenschutzniveau fortbesteht.

Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrem Beschluß vom 29. 01. 1991 (Anlage 1) den Entwurf der Harmonisierungsrichtlinie und seine Zielsetzung grundsätzlich begrüßt und anerkannt, daß er in einer Reihe von Punkten über die Datenschutzkonvention des Europarates von 1980 hinausgehe und die technische und rechtliche Entwicklung des vergangenen Jahrzehnts berücksichtige. Zugleich haben sie eine Reihe von Vorschlägen für Verbesserungen unterbreitet, die sie für notwendig halten, um die Gleichwertigkeit des Schutzes auf dem Niveau zu gewährleisten, das die Mitgliedsländer mit bestehender Datenschutzgesetzgebung bereits erreicht haben. Die Datenschutzbeauftragten haben allerdings auch entscheidenden Wert darauf gelegt, daß die Mitgliedstaaten die Möglichkeit behalten, den Datenschutz in der nationalen Gesetzgebung weiterzuentwickeln.

Es kommt jetzt darauf an, daß die Organe der Europäischen Gemeinschaft, d. h. die Kommission, der Rat und das Parlament als Ergebnis ihres in Art. 149 des EWG-Vertrages geregelten Zusammenspiels die Richtlinie in einer Fassung verabschieden, die nicht durch Interventionen anderer abgeschwächt wird, sondern die das Datenschutzniveau des vorgelegten Entwurfs verbessert oder zumindest hält. Auch von deutscher Seite aus sollte die Initiative der Kommission gestützt werden.

Der Bundesrat hat mit seinem Beschluß vom 14. 12. 1990 zu der Harmonisierungsrichtlinie erkennen lassen, daß auch er sowohl für die Beibehaltung und Weiterentwicklung des erreichten nationalen Datenschutzniveaus als auch für eine Vereinheitlichung auf möglichst hohem Niveau innerhalb der Gemeinschaft eintritt. Ich habe den Senat gebeten, im Rahmen seiner Beteiligung über den Bundesrat nach Art. 2 des Gesetzes zur Einheitlichen Europäischen Akte die Initiative der Kommission zu unterstützen.

4. Nicht-öffentlicher Bereich

4.1 Internationaler Datenverkehr

Die EG-Kommission strebt mit dem von ihr vorgelegten Entwurf einer Datenschutz-Harmonisierungsrichtlinie (vgl. Nr. 3 dieses Berichts) an, daß personenbezogene Daten aus der Gemeinschaft nur dann in ein Drittland „exportiert" (übermittelt) werden dürfen, wenn dieses Land ein „angemessenes" Datenschutzniveau gewährleistet (Art. 24 des Entwurfs). Die Konferenz der Datenschutzbeauftragten hat es demgegenüber für notwendig erklärt, daß ein „gleichwertiges" Schutzniveau erforderlich ist (vgl. Beschluß vom 29. 01. 1991 in der Anlage 1).

Bereits vor Veröffentlichung der EG-Initiative waren Anstrengungen unternommen worden, durch vertragliche Regelungen sicherzustellen, daß die Daten betroffener Bürger trotz fehlender gesetzlicher Regelungen im Empfängerland einen unserem Recht gleichwertigen Datenschutz genießen. Angeregt durch die Konferenz der Obersten Aufsichtsbehörden für den Datenschutz (Düsseldorfer Kreis) sicherte die Kreditwirtschaft zu, daß die von ihr gegründeten Schufa-Gesellschaften, personenbezogene Informationen über Kunden deutscher Kreditinstitute nur dann an ausländische Vertragspartner übermitteln werden, wenn diese sich vertraglich verpflichten,

- die in der Datenschutzkonvention des Europarats niedergelegten Grundsätze einzuhalten,
- die Daten ausschließlich zu dem bei der Anfrage angegebenen Zweck zu nutzen, sie gegen eine Weitergabe an Dritte sowie eine unbefugte Nutzung abzusichern,
- Auskunfts-, ggf. auch Berichtigungs- und Löschungsverlangen der Schufa selbst sowie des betroffenen Kunden zu entsprechen und
- unter bestimmten Voraussetzungen die durch Vertragsverletzungen verursachten Schäden der Schufa oder des betroffenen Kunden zu ersetzen.

Dadurch — so wurde als Zielsetzung angegeben — werde ein Datenschutzniveau erreicht, das den deutschen Regeln vergleichbar sei und das den Grundsätzen der Datenschutzkonvention des Europarates entspreche. Es ist fraglich, ob die Einhaltung der vertraglichen Verpflichtungen tatsächlich durchgesetzt und kontrolliert werden kann. Dahingestellt sei, ob andere Wirtschaftszweige, etwa die Versicherungswirtschaft oder gar der Verband der Handelsauskunfteien, mit denen Gespräche darüber angestrebt werden, zu einem ähnlichen Vorgehen bereit sein werden. Zur Zeit wird erörtert, ob derartige „Vertragsmodelle" nach Wirksamwerden der EG-Harmonisierungsrichtlinie eine praktische Bedeutung behalten. Jedenfalls ist anzustreben, daß künftig als Maßstab das durch die EG-Richtlinie festgeschriebene Datenschutzniveau vereinbart wird.

4.2 Das neue Bundesdatenschutzgesetz

Das neue BDSG vom 20. 12. 1990 (BGBl. I, S. 2953) tritt am 01.06.1991 in Kraft. Das Gesetz nimmt gegenüber dem geltenden Recht für die nichtöffentliche Datenverarbeitung eine Reihe von Änderungen vor. Eine Vielzahl von Vorschlägen der Datenschutzbeauftragten und der Aufsichtsbehörden blieb unberücksichtigt (vgl. zuletzt meine Kritik im 11. Jahresbericht, S. 121). So trifft das Gesetz keine bereichsspezifischen Regelungen zum Arbeitnehmerdatenschutz, für Kreditinformationssysteme oder für Informationssysteme der Versicherungswirtschaft.

Abweichend vom bisherigen Gesetz ergeben sich für die nicht-öffentliche Datenverarbeitung Änderungen z. B. in folgenden Bereichen:

- Die Datennutzung und die Datenerhebung wird geregelt. Die Regelung der Erhebung fordert, daß die Daten nach Treu und Glauben und auf rechtmäßige Weise zu erheben sind.

- Der Dateibegriff ist geändert worden.Das Gesetz verlangt die Möglichkeit der automatisierten Auswertung, die Tatbestandsmerkmale des Ordnens oder Umordnens wurden fallengelassen.

- Bei automatisierten Abrufverfahren gilt nicht mehr die gesetzliche Fiktion, daß der gesamte Datenbestand als übermittelt gilt, wenn er zum Abruf bereitgehalten wird, sondern die Übermittlung liegt erst dann vor, wenn tatsächlich ein Abruf erfolgte.

- Die Möglichkeiten der listenmäßigen Übermittlung von bestimmten Daten (erweiterte Adreßdaten) sind erheblich erweitert worden. Bei der Übermittlung solcher listenmäßig erfaßten Daten, die sich auf Gesundheit, Straftaten, Ordnungswidrigkeiten, religiöse oder politische Anschauungen sowie auf arbeitsrechtliche Rechtsverhältnisse beziehen, statuiert das Gesetz die Vermutung, daß Betroffene ein schutzwürdiges Interesse daran haben, daß die Übermittlung unterbleibt (gesetzliche Vermutung).

- Bei der Übermittlung personenbezogener Daten für fremde Zwecke ist der Empfänger verpflichtet, Aufzeichnungen darüber vorzunehmen, daß ein berechtigtes Interesse an den abgerufenen Daten bestanden hat. Bisher mußte die glaubhafte Darlegung die übermittelnde Stelle aufzeichnen.

- Auskunfteien müssen in Fällen, in denen der Betroffene begründete Zweifel an der Richtigkeit der Daten geltend macht, auch Auskunft über Herkunft und Empfänger der Daten geben.

- Die Stellung des betrieblichen Datenschutzbeauftragten ist gestärkt worden.

- Die im alten Gesetz getroffene Trennung zwischen der Datenverarbeitung für eigene und für fremde Zwecke ist aufgegeben worden.

- Die Kontrollkompetenzen der Aufsichtsbehörden sind bei der Kontrolle der Datenverarbeitung für eigene Zwecke erweitert worden, nunmehr reicht es aus, wenn hinreichende Anhaltspunkte für einen Verstoß gegen Datenschutzbestimmungen vorliegen. Den Aufsichtsbehörden wird darüber hinaus die Befugnis gegeben, Maßnahmen zur Beseitigung von Mängeln bei der Datenverarbeitung anzuordnen. Dazu kann ein Zwangsgeld angedroht werden. Bei schwerwiegenden Mängeln kann der Einsatz des betroffenen DV-Verfahrens untersagt werden.

Derzeit führe ich mit einer Gruppe betrieblicher Datenschutzbeauftragter im Lande Bremen darüber Gespräche, welche praktischen Konsequenzen aus den im Gesetz getroffenen Änderungen zu ziehen sind. Da es zu den Aufgaben der betrieblichen Datenschutzbeauftragten gehört, die Ausführungen des neuen Datenschutzgesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen, geht es den betrieblichen Datenschutzbeauftragten darum, möglichst frühzeitig — spätestens aber bis zum Inkrafttreten des Gesetzes — die betriebliche Datenverarbeitung den neuen Regelungen anzupassen. Bei den Gesprächen hat sich gezeigt, daß die Aufgabe der Trennung zwischen 3. und 4. Abschnitt nicht mehr Klarheit gebracht hat, sondern wenigstens für die Übergangszeit für einige Verwirrung sorgt.

Gleichzeitig befinde ich mich in der Abstimmung mit den Obersten Aufsichtsbehörden für den Datenschutz der anderen Länder (Düsseldorfer Kreis) darüber, ob und in welchem Umfang es erforderlich ist, die Richtlinien zur Durchführung des BDSG (BremAbl. 1981, S. 183) zu ändern und zu ergänzen oder aber fallbezogene Durchführungshinweise zu erarbeiten. Dazu sollen auch Vertreter aus der Wirtschaft gehört werden (Münchener Runde).

4.3 Bonitätsprüfung im Versandhandel

Mir wurde im „Düsseldorfer Kreis" ein neues Verfahren zur Selektierung von Kunden unter Bonitätsgesichtspunkten vorgestellt. Dieses sogenannte Scoring-Verfahren (auch Aschenputtel-Verfahren genannt) basiert auf statistischen Auswertungen, die die Versandhäuser über das Kauf- und Zahlungsverhalten ihrer Kunden vornehmen. Zur Auswertung gelangen dabei nur Daten, die das Versandhaus dem Bestellschein des Kunden und der nachträglichen Abwicklung des Geschäftes entnimmt. Auf diese Art und Weise werden Merkmalscharakteristika zu Risikogruppen zusammengefaßt. Bei Eingang einer Bestellung wird der Kunde aufgrund seiner Angaben einer Kategorie zugeordnet. Erreicht der Kunde eine festgelegte Bonusgrenze, wird ein Kundenkonto ohne Prüfung eingerichtet. Über-

schreitet der Kunde hingegen eine Malusgrenze, wird er auf den Kauf per Nachnahme verwiesen. In dem breiten Zwischenbereich hängt die weitere Bonitätsprüfung von dem Ergebnis einer Schufa-Auskunft ab. Es gibt verschiedene Ausprägungen dieses Scoring-Verfahrens. Einzelne Versandhandelsunternehmen setzen das Scoring z. B. erst dann ein, wenn aufgrund der Schufa-Auskunft Bedenken auftreten, beispielsweise ob einem Ratenkauf zugestimmt werden kann. In diesen Fällen dient das Scoring-Verfahren der Selektion von Kunden, die man früher pauschal nicht bedient hat. Die Versandhandelsunternehmen sehen hierin eine Verbesserung der Leistungen für ihre Kunden.

Neben den bereits im letzten Jahresbericht (S. 60) geäußerten Bedenken gegen die generelle Schufa-Anfrage bei Nachnahmekunden habe ich auch datenschutzrechtliche Bedenken gegen dieses Verfahren. Um das Scoring-Verfahren zu entwickeln, müssen zunächst Kundenprofile angelegt werden. Das gesamte Verhalten des Kunden von der Bestellung bis zur Bezahlung — beim Ratenkauf also über mehrere Monate oder Jahre hinweg — wird festgehalten und selektiert. Bei neueingehenden Bestellungen läuft das Verfahren im Hintergrund ab. Ohne Wissen der Kunden werden deren Daten — wenn auch wie vom Versandhandel behauptet in anonymisierter Form — zu anderen Zwecken genutzt, die Bestelldaten der Kunden werden gerastert und faktisch in eine Bonus- oder Malus-Datei eingeordnet. Im Ergebnis findet eine Stigmatisierung bestimmter Gruppen statt, der einzelne Kunde kann sich gegen eine solche Einordnung nicht wehren. Er wird durch ein pauschales Verfahren klassifiziert. Ich habe deshalb erhebliche Bedenken, ob dieses Verfahren mit dem Recht auf informationelle Selbstbestimmung und dem von der Verfassung geprägten Menschenbild im Einklang steht. Die Überlegungen der Aufsichtsbehörden hierzu sind noch nicht abgeschlossen. Die Anregung, die Kunden wenigstens über das Verfahren und die Klassifizierung zu unterrichten, wurde von der Versandhandelswirtschaft mit zusätzlichem Verwaltungsaufwand und dem Argument abgelehnt, die Darstellung des Verfahrens sei so kompliziert, daß es die Betroffenen nur verwirren werde.

4.4 Versicherungswirtschaft

Verschiedene zentrale Warn- und Hinweissysteme der Versicherungswirtschaft habe ich bereits in früheren Berichten (zuletzt 11. Jahresbericht S. 110) dargestellt. Zwischen den Aufsichtsbehörden und der Versicherungswirtschaft hat es in folgenden Punkten keine Fortschritte gegeben: Im Bereich des Informationssystems der Sachversicherer (SAVIS) ist weiterhin streitig, ob und in welchem Umfang sogenannte Dritte, die nicht auf andere Art und Weise von der Aufnahme ihrer Daten in das Informationssystem Kenntnis erlangt haben, wie z. B. Zeugen, Verwandte des Versicherungsnehmers etc., über die Speicherung zu unterrichten sind.

Auch die Einordnung der Tätigkeit der Verbände bei Verwendung des sogenannten phonetischen Strukturcodes und die damit nach der Auffassung der Aufsichtsbehörden verbundene Meldung zum Register bleibt weiterhin streitig. Hintergrund dieses phonetischen Strukturcode-Verfahrens ist, daß anders als beim bisher verwendeten Match-Code-Verfahren nicht lediglich nur einige Buchstaben des Namens weggelassen werden, sondern ein nicht aus sich heraussprechender Strukturcode zu den einzelnen Versicherten gebildet wird. Nur derjenige, der über das technische Verschlüsselungsverfahren verfügt, kann eine Reidentifizierung vornehmen. Es werden somit personenbeziehbare Daten verarbeitet, das Bundesdatenschutzgesetz ist anzuwenden.

Die Aufsichtsbehörden neigen — anders als beim Match-Code-Verfahren — dazu, diese Tätigkeit des Verbandes nicht als Auskunfteibetrieb im Sinne von § 31 Abs. 1 Nr. 1 BDSG zu qualifizieren, sondern als eine Form der Auftragsdatenverarbeitung im Sinne von § 31 Abs. 1 Nr. 3 BDSG. Der Zentralverband der Versicherungswirtschaft hingegen vertritt die Auffassung, die Datenverarbeitung in den Warn- und Hinweisdateien unterliege dem 3. Abschnitt des BDSG, es bestünde daher auch keine Meldepflicht zum Register der zuständigen Aufsichtsbehörde.

4.5 Lohnpfändungskorrespondenz per Telefax

Mit dem zunehmenden Einsatz von Telefax-Geräten erhöht sich die Gefahr, daß Schriftstücke mit vertraulichem Inhalt Unbefugten zur Kenntnis gelangen. Nach

mir vorliegenden Eingaben wird auch die Korrespondenz in Lohnpfändungsangelegenheiten per Telefax abgewickelt. Telefax-Geräte befinden sich in der Regel in der allgemeinen Verwaltung der Betriebe und werden durch eine Vielzahl wechselnder Personen bedient. Auch wenn Telefaxe in Personalangelegenheiten an die zuständige Personalabteilung weitergeleitet werden, kann es sich im Betrieb sehr schnell herumsprechen, gegen welche Kollegen z. B. Lohnpfändungen angelaufen sind.

Da die Behandlung von Telefonaten weder beim Absender noch beim Empfänger eine dateimäßige Datenverarbeitung darstellt, unterliegt diese nicht den Regelungen des Bundesdatenschutzgesetzes. Gleichwohl darf dies nicht zur Folge haben, daß die Absender in derartigen Fällen das informationelle Selbstbestimmungsrecht der Betroffenen nicht beachten. Unabhängig davon, ob durch diese Versendungsart besondere Berufsgeheimnisse (z. B. Anwaltsgeheimnis, Arztgeheimnis) tangiert sein können, bedeutet dies, daß nicht in jedem Fall Schriftstücke per Telefax abgesandt werden dürfen. Das bedeutet, daß der Absender Vorkehrungen treffen muß, um die unbefugte Kenntnisnahme zu verhindern.

Darüberhinaus obliegen dem Arbeitgeber als Empfänger eines Faxes im Rahmen des Arbeitsverhältnisses mit dem Arbeitnehmer verschiedene Sorgfaltspflichten, u. a. ist das Persönlichkeitsrecht der Arbeitnehmer zu wahren. Daraus folgt die gesetzliche Verpflichtung, daß der Arbeitgeber den Telefax-Einsatz innerhalb seines Betriebes so zu gestalten hat, daß eingehende Post nicht Unbefugten zur Kenntnis gelangt. Er muß also darauf hinwirken, daß nur bestimmte Personen Zugang zum Telefax-Gerät erhalten sowie daß diese Personen zur Verschwiegenheit angehalten werden. Folgende Grundregeln sollten bei der Telefax-Korrespondenz beachtet werden:

- Telefax-Geräte sollten in Räumen untergebracht werden, die ausreichend gesichert sind und für die sichergestellt ist, daß eine Telefax-Sendung nicht unbeobachtet ankommt und nicht von Unbefugten entnommen oder eingesehen werden kann.

- Telefax-Übertragungen sind „abhörbar": Was am Telefon nicht gesagt werden darf, darf auch nicht gefaxt werden.

- In jedem Betrieb sollte eine Anweisung für die Nutzung des Telefax-Dienstes bestehen.

- Der Absender trägt die Verantwortung für die durch ihn übermittelten personenbezogenen Daten.

- Der Absender sollte sich vor einer Sendung vergewissern, ob der Adressat noch unter der bekannten Anschlußnummer erreichbar ist.

- Der Absender sollte alle der Sicherheit dienenden Einrichtungen des Gerätes nutzen, insbesondere die Anzeige des angewählten Gerätes überprüfen.

- Der Absender muß z. B. durch vorherige telefonische Ankündigung sicherstellen, daß das Telefax nur vom Berechtigten in Empfang genommen werden kann.

- Der Absender sollte während der Übertragung von Dokumenten mit personenbezogenen Daten — möglichst durch persönliche Anwesenheit am Gerät — gewährleisten, daß kein Unbefugter in diese Einsicht nehmen kann.

- Der Empfänger muß sicherstellen, daß nur bestimmte Personen Zugang zum Telefax-Gerät haben; dieser Personenkreis ist auf Verschwiegenheit zu verpflichten.

4.6 Austausch von Kundenprofilen im Rahmen eines Reisereservierungsverfahrens

Mir ist bekannt, daß in bundesdeutschen Reisebüros zunehmend Reservierungssysteme eingesetzt werden, in denen neben den Daten, die zur Abwicklung einer Reisevermittlung erforderlich sind, weitere personenbezogene Daten gespeichert werden, um sogenannte Kundenprofile zu erzeugen. Dies sind z. B. Daten über Hobbies, Positionen in der Firma, Vorlieben für bestimmte Speisen und Hotels und Angaben über den Ehepartner. Diese Kundenprofile werden zwischen den einzelnen Reisebüros ausgetauscht, wobei dieser Austausch auf direktem Wege oder über ein hierfür eingerichtetes Rechenzentrum erfolgt.

Für derartige zusätzliche Speicherungen und deren Übermittlungen kann sich das Reisebüro nicht auf die Zweckbestimmung eines Vertragsverhältnisses berufen. Schutzwürdige Belange der Betroffenen werden beeinträchtigt, da die genannten Daten im Zusammenhang mit den sonstigen Daten aufgrund der vielfältigen Verknüpfungsmöglichkeiten einen tiefen Einblick in die Persönlichkeit des Kunden gestatten. Der Kunde kann selbst dann in seinen schutzwürdigen Belangen beeinträchtigt sein, wenn er über die Tatsache, daß diese Daten gespeichert werden, unterrichtet wird und dieser Speicherung nicht widerspricht, da ihm die vielfältigen Verwendungs- und Verknüpfungsmöglichkeiten gar nicht bekannt werden. Allein die qualifizierte Einwilligung, d.h. die Einwilligung unter der Bedingung, daß der Kunde weiß, wer bei welcher Gelegenheit welche personenbezogenen Daten verarbeitet und zu welchem Zweck diese Verarbeitung erfolgen kann, führt zur Zulässigkeit der Datenverarbeitung. Entsprechend habe ich mich auch gegenüber den anderen Datenschutzaufsichtsbehörden geäußert.

4.7 Service-Rechenzentrum für Apotheken

Ich habe im Berichtsjahr die automatisierte Abrechnung von Rezepten bei einem Service-Rechenzentrum geprüft.

Zum Zwecke der Abrechnung übersenden die angeschlossenen Apotheken die bei ihnen eingereichten Rezepte an das Rechenzentrum, das diese maschinell aufbereitet und nach Krankenkassen sortiert und die Zahlungsbeträge pro Apotheke errechnet. Danach leitet das Rechenzentrum die Rezepte zusammen mit den Ergebnissen der maschinellen Aufbereitung an die einzelnen Krankenkassen weiter. Die errechneten Zahlungsbeträge werden daraufhin von den Krankenkassen an das Rechenzentrum überwiesen, das seinerseits wiederum die jeweiligen Beträge an die angeschlossenen Apotheken weiterleitet.

Bei der Prüfung habe ich festgestellt, daß das Rechenzentrum Datenverarbeitssubaufträge an Dritte vergibt. Weder die Vereinssatzung noch die Geschäftsordnung oder die Grundlagen der Rezeptabrechnung erhalten die Befugnis, solche Unteraufträge zu vergeben. Die Auftraggeber des Rechenzentrums haben diesem auch keine gesonderten Weisungen gem. § 37 BDSG erteilt. Ich habe die Vergabe von Subaufträgen ohne gesonderte Weisung der Auftraggeber für unzulässig erklärt, da ein Verstoß gegen § 37 BDSG vorliegt.

Weiterhin habe ich festgestellt, daß das Service-Rechenzentrum gegen § 31 Abs. 2 BDSG verstoßen hat, wonach es verpflichtet ist, den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technisch-organisatorischen Datenschutzmaßnahmen auszuwählen. Eine besondere Sorgfalt bei der Auswahl hätte insbesondere im Hinblick auf die Verarbeitung der sensiblen medizinischen Daten erfolgen müssen.

Ferner habe ich beanstandet, daß ohne Wissen der angeschlossenen Apotheken Rezepte für das Wissenschaftliche Institut der Ortskrankenkassen ausgewertet werden.

Ich habe das Rechenzentrum aufgefordert, in das Vertragswerk Regelungen über die Subauftragsvergabe sowie eine Auswertung der Rezepte für das Wissenschaftliche Institut der Ortskrankenkassen aufzunehmen. Es bleibt abzuwarten, inwieweit das Rechenzentrum dieser Aufforderung nachkommt.

4.8 Eingaben und Beschwerden

Im übrigen bin ich einer Vielzahl von Eingaben und Beschwerden von Bürgern aus dem Lande Bremen und der umliegenden Wirtschaftsregion nachgegangen. Diese bezogen sich u. a. auf die unsachgemäße Aufbewahrung und Verwendung von Personal-, Bewerbungs- und Privatschulunterlagen; viele Fragen bezogen sich auf die Telefondatenerfassung im Betrieb, auf die Datenverarbeitung durch Kreditinstitute, Maklerbüros, Ärzte und Versicherungen. Selbstverständlich betraf ein großer Anteil der Beschwerden das Tätigkeitsfeld von Auskunfteien. Die Mehrzahl der Eingaben konnte nur durch Feststellung des Sachverhalts vor Ort aufgeklärt werden.

5. Schluß

Mehrere Stellen beim Landesbeauftragten für den Datenschutz waren im letzten bzw. sind in diesem Jahr ganz oder teilweise nicht besetzt. Es bedurfte daher besonderer Anstrengungen, den Dienstbetrieb im vollen Umfang aufrecht zu erhalten. An dieser Stelle möchte ich daher allen Kolleginnen und Kollegen der Dienststelle danken, die zum Teil weit über das übliche Maß hinaus mich bei der Aufgabenerfüllung unterstützt haben.

Sven Holst
Vertreter des Landesbeauftragten für den Datenschutz

Bremerhaven, den 11. März 1991

Anlage 1

Vorschlag für eine EG-Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten

I.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in der Vergangenheit zu wiederholten Malen die Untätigkeit der Europäischen Gemeinschaft im Bereich des Datenschutzes kritisiert. Kernpunkt dieser Kritik war die Befürchtung, daß die Dynamik der wirtschaftlichen Entwicklung in Richtung auf den vollendeten Binnenmarkt zu einem „informationellen Großraum" mit einem engen Netzwerk grenzüberschreitender Datenflüsse führt, ohne daß gleichzeitig der Grundrechtsschutz in der Gemeinschaft bei der Verarbeitung und dem Austausch persönlicher Daten gewährleistet wird.

II.

Daher begrüßt die Konferenz, daß die EG-Kommission im Juli 1990 den „Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" vorgelegt hat. Der Kommissionsvorschlag geht in einer Reihe von Punkten über die Konvention des Europarats zum Datenschutz von 1980 hinaus und berücksichtigt insoweit die technische und rechtliche Entwicklung des vergangenen Jahrzehnts. Positiv bewertet die Konferenz vor allem die Intention des Entwurfs, den Datenschutz in der EG nicht auf dem kleinsten gemeinsamen Nenner, sondern auf einem möglichst hohen Niveau zu harmonisieren. Sie legt allerdings entscheidenden Wert darauf, daß die Mitgliedsstaaten die Möglichkeit behalten, den Datenschutz in der nationalen Gesetzgebung weiterzuentwickeln.

III.

Zahlreiche bewährte Vorschriften und Instrumente aus dem deutschen Datenschutzrecht sind in den Richtlinientext aufgenommen worden. Die Bewertung der einzelnen Bestimmungen des Richtlinienentwurfs kann jedoch nicht isoliert aus dem Blickwinkel des deutschen Datenschutzrechts erfolgen. Jeder nationale Gesetzgeber muß bei Rechtsharmonisierung auf europäischer Ebene bereit sein, einzelne seiner Regelungen auf dem Hintergrund der Erfahrungen und Vorstellungen anderer Mitgliedstaaten in Frage zu stellen. Zur Abstimmung der Auffassungen auf EG-Ebene besteht ein intensiver Meinungsaustausch zwischen der Konferenz und den Datenschutzinstitutionen der Partnerländer.

IV.

Die Konferenz hält, abgesehen von der Bereinigung von redaktionellen Unstimmigkeiten, einige Änderungen im Richtlinienvorschlag für notwendig, um die Gleichwertigkeit des Schutzes auf dem Niveau, das die Mitgliedsländer mit bestehender Datenschutzgesetzgebung bereits erreicht haben, sicherzustellen. Folgende Korrekturen sind dabei vorrangig:

1. Datenschutz muß, jedenfalls im Bereich der öffentlichen Verwaltung, für alle Unterlagen mit personenbezogenen Daten gelten. Die in der Richtlinie vorgesehene Beschränkung des Anwendungsbereichs auf die Verarbeitung personenbezogener Daten in „Dateien" ist ebenso technisch überholt wie Anlaß zu einer Fülle von Interpretationsproblemen.

2. Für die Verwendung und Weitergabe persönlicher Daten muß das Prinzip strikter Zweckbindung gelten und ausdrücklich statuiert werden. Wenn der Entwurf die bloße Vereinbarkeit der Zwecke von Erhebung, Speicherung und Übermittlung genügen läßt, werden inakzeptable Verarbeitungsfreiräume eröffnet; die Transparenz des Datenumgangs geht für den einzelnen verloren.

3. Der Anspruch auf Auskunft über die gespeicherten Daten ist das elementarste Individualrecht der Betroffenen. Nur gravierende Interessen der Allgemeinheit oder Dritter dürfen im Ausnahmefall diesen Auskunftsanspruch einschränken. Der im Entwurf vorgesehene Katalog von Fällen der Auskunftsverweigerung muß daher deutlich vermindert werden.

4. Der Forderung des Entwurfs, daß die Erhebung von Daten nur „nach Treu und Glauben" erfolgen darf, kann uneingeschränkt zugestimmt werden. Doch muß dieses Prinzip im Interesse des Einzelnen konkretisiert werden. Es gilt klarzustellen, daß persönliche Angaben vorrangig beim Betroffenen selbst zu erheben sind. Die Ausnahmefälle, in denen Informationen ohne Kenntnis des Betroffenen beschafft werden dürfen, sollten soweit wie möglich in der Richtlinie konkret benannt werden.

5. Der Datenschutz der EG-Bürger darf nicht an den Gemeinschaftsgrenzen haltmachen. Ziel der Richtlinie muß neben der EG-internen Harmonisierung auch sein, den Schutz des Betroffenen beim Datenexport in Drittländer zu gewährleisten. Dies setzt voraus, daß im Empfängerland ein dem EG-Standard gleichwertiges Datenschutzniveau besteht. Daß der Richtlinienentwurf sich mit einem „angemessenen" Schutz im Zielland zufriedengibt, genügt nicht. Notwendig ist schließlich, das Verfahren zur Feststellung des Datenschutzstandards in Drittländern übersichtlich und praktikabel auszugestalten.

6. Auf der EG-Ebene bedarf es einer unabhängigen Datenschutzinstanz, die alle EG-Organe in Datenschutzfragen berät und für die Überwachung der Einhaltung sowie die einheitliche Anwendung der Richtlinie sorgt. Die im Richtlinienvorschlag vorgesehene „Gruppe für den Schutz personenbezogener Daten" erfüllt — betrachtet man ihre Struktur, Aufgaben und Kompetenzen — diese Anforderungen nicht. Die Unabhängigkeit der Datenschutzkontrolle auf EG-Ebene wird in Zweifel gezogen, wenn den Vorsitz nicht ein gewähltes Mitglied dieser — aus den nationalen Datenschutzorganen zusammengesetzten — „Gruppe", sondern ein Vertreter der EG-Kommission führt. Klargestellt werden muß weiter, daß das Votum der „Gruppe" im vorhinein bei allen den Datenschutz betreffenden Initiativen und Entwürfen der Kommission einzuholen ist. Ansprechpartner der „Gruppe" darf nicht ausschließlich die EG-Kommission, sondern muß auch das Europäische Parlament sein.

7. Da die Kommission die entsprechende Anwendung der Richtlinie auf die personenbezogene Datenverarbeitung ihrer eigenen Dienststellen beschlossen hat, muß sie auch umgehend für eine unabhängige Kontrolle dieses Bereichs Sorge tragen.

V.

Die Konferenz weist darauf hin, daß die vorliegende Richtlinie durch Regelungen für besondere Anwendungsbereiche ergänzt werden muß. Sie sind insbesondere für den Arbeitnehmer- und Sozialdatenschutz vordringlich. Die Kommission sollte schon jetzt ihre Bereitschaft erklären, entsprechende Regelungen zu treffen, und möglichst bald erste Vorschläge vorlegen.

VI.

Die Konferenz begrüßt die Gesprächsbereitschaft der Kommission und geht davon aus, daß der bereits begonnene Dialog zu einer substantiellen Verbesserung des Richtlinienvorschlags führen wird. Die Konferenz wird diese Entschließung der EG-Kommission, dem Europäischen Parlament sowie der Bundesregierung zuleiten. Informiert werden ebenfalls die Datenschutzkontrollinstitutionen der Partnerländer in der Gemeinschaft.

Beschluß der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 29. Januar 1991

Bundesdatenschutzgesetz und Bundesverfassungsschutzgesetz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz (gegen die Stimme Bayerns) begrüßt die mit den am 13. März 1990 vorgelegten Vorschlägen der Koalitionsfraktionen verbundene Absicht, die längst fällige Novellierung des Bundesdatenschutzgesetzes und des Bundesverfassungsschutzgesetzes noch rechtzeitig vor dem Ende der Legislaturperiode zu verabschieden.

Die Vorschläge zum **Bundesdatenschutzgesetz** beseitigen eine Reihe von Schwächen des Regierungsentwurfes. Hervorzuheben ist insoweit

- daß nunmehr für den öffentlichen Bereich die Verarbeitung personenbezogenener Daten in Akten und die Datenerhebung durch öffentliche Stellen in den Geltungsbereich des Bundesdatenschutzgesetzes einbezogenen werden,
- daß künftig der Bundesbeauftragte für den Datenschutz durch das Parlament gewählt werden soll,
- daß der Betroffene bei Ablehnung der Auskunftserteilung darauf hingewiesen wird, daß er sich an den Bundesbeauftragten für den Datenschutz wenden kann.

Demgegenüber weisen auch die Vorschläge noch Schwächen und Defizite auf. Dazu gehören u. a.:

- Die unzureichende Kontrollbefugnis des Bundesbeauftragten für den Datenschutz bei der Datenverarbeitung in Akten,
- ein Widerspruchsvorbehalt für die Betroffenen gegen eine Kontrolle ihrer Daten durch den Bundesbeauftragten für den Datenschutz, der systematische Prüfungen gefährdet und deshalb entbehrlich ist, weil es für die Datenschutzbeauftragten schon immer selbstverständlich war, die Daten von Betroffenen nicht gegen deren erklärten Willen in Kontrollen einzubeziehen,
- die verfassungswidrige Erstreckung des Widerspruchsvorbehaltes in der Neufassung auf die Landesbeauftragten für den Datenschutz,
- das Fehlen eines gesonderten Gesetzesvorbehaltes für die Einrichtung von Direktzugriffsverfahren in besonders sensiblen Bereichen,
- der zu weite Katalog erlaubter Zweckänderungen und die unzureichende Unterrichtung des Betroffenen über die Zweckänderung.

Im Bereich der Datenverarbeitung durch nichtöffentliche Stellen verschlechtern einzelne vorgeschlagene Regelungen die Rechte der Betroffenen im Vergleich zum geltenden Gesetz, etwa bei der Übermittlung von Daten an den Adressenhandel. Sie bleiben im übrigen weit hinter den Vorschlägen für den öffentlichen Bereich zurück. Weder die Verarbeitung in Akten noch die Datenerhebung werden einbezogen. Auch die höchst unzureichenden Kontrollbefugnisse der Datenschutzaufsichtsbehörden sind nicht wesentlich verbessert worden.

Schließlich erinnern die Datenschutzbeauftragten an ihre früheren Forderungen nach bereichsspezifischen Regelungen für die Verarbeitung von Arbeitnehmerdaten sowie von Regelungen für den Kredit- und Versicherungsbereich.

Zu den Vorschlägen der Koalition für das **Bundesverfassungsschutzgesetz** stellen die Datenschutzbeauftragten des Bundes und der Länder fest:

Die Vorschläge bringen gegenüber dem Vorentwurf der Bundesregierung Verbesserungen. Dies gilt insbesondere für:

- Den Schutz des in Wohnungen nichtöffentlich gesprochenen Wortes vor heimlichem Mithören und Aufzeichnen,
- die Einschränkung der Speicherung von Daten über Minderjährige,
- die konkretisierenden und einschränkenden Regelungen für den Einsatz nachrichtendienstlicher Mittel,
- die präzise Definition der „Bestrebungen" gegen die freiheitlich-demokratische Grundordnung,
- die Anknüpfung der Sammlung und Verarbeitung von Daten an das Vorliegen tatsächlicher Voraussetzungen.

Hingegen sind u. a. folgende datenschutzrechtliche Anforderungen noch nicht erfüllt:

- Die Befugnisse zur Datenverarbeitung müssen differenziert den unterschiedlichen Aufgaben zugeordnet werden.
- Die Datenspeicherung ist nicht so präzise geregelt, daß der Bürger dem Gesetz entnehmen kann, unter welchen in seiner Person liegenden Voraussetzungen der Verfassungsschutz über ihn Daten speichern darf.
- Die Zweckbindung der Daten innerhalb des Verfassungsschutzes ist nicht gewährleistet.
- Das Auskunftsrecht des Bürgers auch gegenüber den Verfassungsschutzbehörden wird zwar nunmehr erstmals anerkannt.

  Die vorgeschlagene Regelung schränkt aber den Auskunftsanspruch zu sehr ein. So wird dem Bürger eine Pflicht zur Begründung seines Auskunftsersuchens auferlegt, während die Ablehnung der Auskunft unter keinen Umständen begründet werden muß.
- Die vorgesehenen Regelungen zur Sicherheitsüberprüfung ersetzen nicht eine bereichsspezifische, präzise Rechtsgrundlage in einem Geheimschutzgesetz für das Überprüfungsverfahren.

Die Datenschutzbeauftragten gehen davon aus und halten es für notwendig, daß die bestehenden Mängel der Gesetzentwürfe in den anstehenden Parlamentsberatungen behoben und ihre Anregungen aufgegriffen werden.

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. März 1990

Anlage 3

Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität

Die Konferenz der Datenschutzbeauftragten hat schwerwiegende datenschutzrechtliche Bedenken gegen die Ausweitung der polizeilichen Ermittlungsbefugnisse in der Strafprozeßordnung, wie sie mit dem vom Bundesrat vorgelegten Gesetzentwurf zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG) beabsichtigt ist.

Erstmals werden in die Strafprozeßordnung Regelungen zur Rasterfahndung, zum Einsatz verdeckter Ermittler sowie von Wanzen und Richtmikrofonen und heimlichen Film- und Fotoaufnahmen eingefügt. Die Konferenz der Datenschutzbeauftragten verkennt nicht, daß bestimmte Erscheinungsformen von Kriminalität im Interesse des Schutzes der Bürger besondere Ermittlungsmethoden erforderlich machen können. Der vorgelegte Entwurf regelt jedoch nicht nur neue Eingriffsbefugnisse zur Bekämpfung des illegalen Rauchgifthandels und sonstiger organisierter Kriminalität — die im übrigen nicht definiert wird —, sondern soll tief in die Privatsphäre der Bürger eingreifende Fahndungs- und Ermittlungsmethoden in das Strafverfahrensrecht allgemein einführen.

Gegen den vorliegenden Entwurf bestehen insbesondere folgende datenschutzrechtliche Bedenken:

- Die vorgesehenen Eingriffsbefugnisse der Strafverfolgungsbehörden werden an den konturenlosen Begriff „Straftaten von erheblicher Bedeutung" geknüpft. Damit dürfte nach der Begründung des Gesetzentwurfs in der Praxis allenfalls die Kleinkriminalität ausscheiden. So soll z. B. auch die **Rasterfahndung** für eine Vielzahl von Delikten außerhalb organisierter Kriminalität zugelassen werden. Dies erscheint besonders bedenklich, weil gerade diese Form der Fahndung unbescholtene Bürger in großer Zahl unvermeidlich mit einbezieht und sie in der Folge Ziel weiterer Ermittlungen werden können.
- Tief in die Privatsphäre eindringende Ermittlungsmethoden werden nicht hinreichend präzisiert und sind großenteils unverhältnismäßig: So dürfen ohne Wissen des Betroffenen zur Aufklärung **jeder Straftat** — sogar in Wohnungen hinein — „Lichtbilder und Bildaufzeichnungen" aufgenommen werden sowie „besondere Sichthilfen" eingesetzt werden.

- Maßnahmen, wie Einsatz von Peilsendern, Richtmikrofonen, Wanzen und sonstiger Überwachungstechniken, können sich auch gegen dritte **unverdächtige Personen** richten, wenn „aufgrund bestimmter Tatsachen" anzunehmen ist, „daß sie mit dem Täter in Verbindung stehen oder eine solche Verbindung hergestellt wird". Es bleibt völlig offen, wie das Tatbestandsmerkmal der „Verbindung" eingegrenzt werden soll. Foto- und Filmaufnahmen von Unbeteiligten sind bereits zulässig, wenn sie für Ermittlungen „geeignet" sind. Damit kann kein Bürger vorhersehen, ob und wann er hiervon betroffen sein kann. Ohne Kenntnis der gegen ihn gerichteten Eingriffe kann er im Regelfall nicht einmal Rechtsschutz erlangen.

- Die Möglichkeiten der Telefonüberwachung werden über das vertretbare Maß hinaus ausgeweitet.

- Bedenken richten sich ferner dagegen, bei besonderen Ermittlungsmaßnahmen auf die vorherige **richterliche Kontrolle** zu verzichten und durch Eilkompetenzen die Entscheidung der diese Maßnahmen selbst durchführenden Polizei zu übertragen. Nicht einmal die nachträgliche richterliche Kontrolle ist in jedem Fall zwingend vorgesehen.

Im Gegensatz zu den erweiterten Befugnissen der Strafverfolgungsbehörden sind Regelungen zum Schutz oder im Interesse der Betroffenen nur unzureichend vorgesehen. Die mit besonderen Ermittlungsmethoden für besondere Strafverfolgungszwecke erhobenen Daten dürfen für zu weitgehende andere Zwecke verwendet werden. So sind z. B. die Begriffe „Zwecke der staatsanwaltschaftlichen Vorgangsverwaltung" und „Zwecke der Rechtspflege" zu unbestimmt. Es fehlen weiterhin ausreichende Bestimmungen zum Auskunftsrecht des Betroffenen und zur Löschung.

Zusammenfassend ist festzustellen, daß dieser Entwurf selbst hinter den datenschutzrechtlichen Ansätzen, wie sie etwa noch im Entwurf des Strafverfahrensänderungsgesetzes 1989 enthalten waren, zurückbleibt.

Die Konferenz der Datenschutzbeauftragten fordert den Deutschen Bundestag auf, diese Vorschläge des Gesetzentwurfs abzulehnen und die unterbrochenen Arbeiten an der umfassenden datenschutzrechtlichen Novellierung der Strafprozeßordnung, die dringend geboten ist, wieder aufzunehmen. Hierzu haben die Datenschutzbeauftragten wiederholt konkrete Vorschläge vorgelegt.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juni 1990

Anlage 4

Neuregelung des Melderechtsrahmengesetzes

Der dem Deutschen Bundestag vorliegende Entwurf eines Ersten Gesetzes zur Änderung des Melderechtsrahmengesetzes hält weiter an der Hotel- und Krankenhausmeldepflicht fest. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz hat erhebliche Bedenken, ob dem Bund die Gesetzgebungskompetenz zur Regelung dieser Frage zusteht. In jedem Fall ist zu bedenken:

Zweck der allgemeinen Meldepflicht ist es, die Identität der Einwohner und deren Wohnungen festzustellen und diese Basisinformation für die Bewältigung einer Vielzahl von Verwaltungsaufgaben zur Verfügung zu stellen. Bei einem kurzfristigen Aufenthalt in einem Hotel oder Krankenhaus entfällt dieser Zweck. Lediglich die Polizei hat ein Interesse an der Feststellung dieser Tatsachen. Schon deshalb paßt die Hotel- und Krankenhausmeldepflicht nicht in die Systematik des Melderechts, es handelt sich vielmehr um materielles Polizeirecht.

Polizeiliche Datenverarbeitung setzt voraus, daß Gefahren abgewendet oder Straftaten verfolgt bzw. verhütet werden sollen. Hotelgäste und Krankenhauspatienten können jedoch nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen werden. Vielmehr ist zu berücksichtigen, daß es sich im Regelfall um Bürger handelt, die ein Recht darauf haben, von polizeilichen Ermittlungen unbehelligt zu bleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und die Datenschutzkommission Rheinland-Pfalz ist darüber hinaus der Auffassung, daß den Bürgern in allen Meldegesetzen ein Widerspruchsrecht gegen die Weitergabe ihrer Daten an politische Parteien und Wählergruppen zum Zwecke der Wahlwerbung eingeräumt werden muß.

Gegenstimme Bayern mit Ausnahme des letzten Absatzes.

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990

Anlage 5

Erarbeitung von Krebsregistergesetzen in Bund oder Ländern

1. Die Datenschutzbeauftragten haben schon in ihren Entschließungen vom 14. Dezember 1981 und 27. April 1982 zur Schaffung gesetzlicher Grundlagen für die Errichtung und Führung bevölkerungsbezogener epidemiologischer Krebsregister Stellung genommen. Wenn sich der Gesetzgeber zugunsten solcher Register, deren Nutzen auch unter Medizinern nicht unumstritten ist, entscheiden sollte, entspricht es dem gesetzlichen Auftrag der Datenschutzbeauftragten darauf zu achten, daß die Errichtung und Führung solcher Register in einer Weise geschieht, die auf das Persönlichkeitsrecht der Krebskranken in größtmöglichem Umfang Rücksicht nimmt.

2. Würde den Ärzten die Befugnis eingeräumt, ihre Krebskranken in jedem Fall ohne deren Einwilligung mit Namen an ein solches Register zu melden, würde dies einen äußerst schwerwiegenden Eingriff in deren durch Art. 1 i. V. m. Art. 2 Abs. 1 GG geschütztes Persönlichkeitsrecht darstellen, eine weitere Durchbrechung der ärztlichen Schweigepflicht zur Folge haben und damit das Arzt-/Patientenverhältnis erheblich belasten. Die Krebskranken würden ohne ihre Einwilligung zentral in einem Register gespeichert werden und zwar so, daß die registerführende Stelle feststellen kann, welche Personen an Krebs erkrankt und zum Register gemeldet worden sind.

   Die Datenschutzbeauftragten sind deshalb der Auffassung, daß die Einrichtung eines Krebsregisters auf einer solchen Grundlage (Melderechtsmodell) nicht in Betracht kommt.

   Sie sind nach wie vor der Meinung, daß das Krebsregister nur mit Einwilligung der Patienten oder auf anonymer Basis geführt werden könne. Für beides gibt es bereits Modelle (Einwilligungsmodell und dezentrales Verschlüsselungsmodell). Die Datenschutzbeauftragten sehen in diesen Modellen gangbare Wege zur Führung bevölkerungsbezogener Krebsregister, die auch noch fortentwickelt werden können.

   Sollten weitere Modelle, die das Persönlichkeitsrecht der Krebskranken in gleicher Weise wahren, weiterentwickelt werden, sind die Datenschutzbeauftragten selbstverständlich bereit, auch sie in Erwägung zu ziehen.

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990

Anlage 6

Datenschutz im deutsch-deutschen Verhältnis

1. Das Engagement der Bevölkerung in der DDR für den Schutz ihrer personenbezogenen Daten z. B. beim Staatssicherheitsdienst zeigt, wie elementar die Persönlichkeitsrechte von den Bürgern in der DDR verstanden werden und daß sie das Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Selbstbestimmungsrechts wahrnehmen.

   Die Konferenz der Datenschutzbeauftragten begrüßt Bemühungen, auch in der DDR angemessene Datenschutzregelungen zu schaffen.

2. Obwohl in der DDR keine hinreichenden Datenschutzregelungen bestehen, werden bereits jetzt mehr personenbezogene Daten als früher ausgetauscht. Dieser Datentransfer wird noch zunehmen. Aktuelle Anlässe, wie der Austausch von Daten bei Verkehrsunfällen sowie im Rahmen der Gefahrenabwehr und der Strafverfolgung haben in der Öffentlichkeit besondere Aufmerksamkeit gefunden.

   Der Prozeß der sozialen, wirtschaftlichen und politischen Einigung führt zu verstärktem grenzüberschreitenden Datenverkehr, z. B. im Sozialrecht, im Melderecht, im Versicherungs- und Kreditrecht. Dies wirft Fragen des Datenschutzes auf. Für die Bundesrepublik gelten das allgemeine Datenschutzrecht und besondere Gesetze wie z. B. das Gesetz über die innerdeutsche Rechts- und Amtshilfe in Strafsachen vom 2. Mai 1953 sowie Vereinbarungen.

   Bei der Verwirklichung technischer Maßnahmen insbesondere bei dem Ausbau der Telekommunikationsdienste und bei der automatisierten Datenverarbeitung muß der Datenschutz beachtet werden.

3. Die Datenschutzkonferenz hält es für geboten, daß der Austausch personenbezogener Daten zwischen Behörden und öffentlichen Stellen in der Bundesrepublik Deutschland und in der Deutschen Demokratischen Republik erst durchgeführt wird, wenn gewährleistet ist, daß nach folgenden Grundsätzen verfahren wird:

   - Die Grundsätze des Übereinkommens des Europarates über den Schutz des Menschen bei der Verarbeitung personenbezogener Daten vom 28. Januar 1981 sind zu beachten.

   - Die Übermittlung personenbezogener Informationen unterbleibt, soweit Grund zu der Annahme besteht, daß dadurch gegen den Zweck eines Gesetzes der Bundesrepublik Deutschland verstoßen würde oder schutzwürdige Belange bei den betroffenen Personen beeinträchtigt würden. Die Übermittlung personenbezogener Informationen unterbleibt insbesondere dann, wenn Grund zu der Annahme besteht, daß die Verwendung der übermittelten Informationen nicht in Einklang mit rechtsstaatlichen Grundsätzen steht oder dem Betroffenen aus der Verwendung der Informationen erhebliche Nachteile erwachsen, die im Widerspruch zu rechtsstaatlichen Grundsätzen stehen.

   - Der Empfänger darf personenbezogene Informationen nur zu dem durch die übermittelnde Stelle angegebenen Zweck und unter den von ihr vorgeschriebenen Bedingungen nutzen.

   - Personenbezogene Informationen dürfen ausschließlich an die in den Abkommen oder Absprachen genannten Behörden übermittelt werden. Eine Übermittlung an andere Stellen darf nur mit vorheriger Zustimmung der übermittelnden Stelle erfolgen.

   - Der Empfänger unterrichtet die übermittelnde Stelle und den zuständigen Datenschutzbeauftragten auf Ersuchen über die Verwendung der übermittelten Informationen und über die dadurch erzielten Ergebnisse.

   - Die übermittelnde Stelle ist verpflichtet, auf die Richtigkeit der zu übermittelnden Informationen zu achten. Erweist sich, daß unrichtige oder zu vernichtende personenbezogene Informationen übermittelt worden sind, so ist dies dem Empfänger unverzüglich mitzuteilen. Dieser ist verpflichtet, die Berichtigung oder Vernichtung vorzunehmen.

   - Dem Betroffenen ist auf Antrag über die zu seiner Person vorhandenen Informationen sowie über den vorgesehenen Verwendungszweck Auskunft zu erteilen. Eine Verpflichtung zur Auskunftserteilung besteht nicht, soweit eine Abwägung ergibt, daß eine Auskunft den Verwendungszweck oder schutzwürdige Interessen Dritter gefährden würde.

   - Die Übermittlung und der Empfang personenbezogener Informationen sind aktenkundig zu machen.

   - Zur Gewährleistung dieser Grundsätze sind die verfahrensmäßigen Sicherungen vorzusehen. Dazu kann es gehören, besondere Stellen mit der Datenübermittlung zu beauftragen. Die Kontrolle der Datenübermittlung durch unabhängige Datenschutzbeauftragte muß gewährleistet sein.

4. Die Verarbeitung personenbezogener Daten bei den Sicherheitsbehörden der Bundesrepublik Deutschland muß im Hinblick auf die politischen Veränderungen in der DDR und im übrigen Mittel- und Osteuropa über die bereits getroffenen Maßnahmen hinaus überprüft werden. Diese Notwendigkeit besteht u. a. bei:

   — dem Verfahren der Sicherheitsüberprüfung,

   — der Datenerhebung und Datenübermittlung des Bundesgrenzschutzes anläßlich von Grenzkontrollen an die Nachrichtendienste,

   — der Bereinigung der Datensammlungen der Verfassungsschutzbehörden.

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 22./23. März 1990

Anlage 7

Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nicht-öffentlich gesprochenen Wortes

Wegen der dynamischen technischen Entwicklung auf dem Gebiet der Telekommunikation ist es dringlich, das Grundrecht auf freie Entfaltung der Persönlichkeit gegen neue Gefährdungen zu schützen. Den Risiken für das Recht auf unbeobachtete Kommunikation muß rechtzeitig begegnet werden:

— Die Einführung von ISDN macht es möglich, daß auch nach Beendigung von Telefongesprächen über einen bestimmten Zeitraum gespeichert wird, wer wann mit wem wie lange telefoniert hat.

— Der zunehmende Einsatz von Funkdiensten im Telekommunikationsverkehr (z. B. mobile Telefone, Satellitenkommunikation) ist mit der Speicherung von noch mehr Daten über die Telefonverbindung verbunden und erleichtert die Möglichkeit des Abhörens und Aufzeichnens der Gesprächsinhalte.

— Zunehmend stehen Abhöranlagen zur Verfügung, mit denen aus der Masse der geführten Telefongespräche bestimmte Telefonate gezielt herausgegriffen, aufgezeichnet und nach bestimmten Gesichtspunkten ausgewertet und gespeichert werden können.

Das Grundgesetz läßt Einschränkungen des Fernmeldegeheimnisses unter gewissen Voraussetzungen auf gesetzlicher Grundlage zu. In den vergangenen Jahren hat der Gesetzgeber diese Eingriffsmöglichkeiten mehrmals erweitert und hierbei alle Telekommunikationsdienste (wie z. B. Telefax und BTX) einbezogen. Zudem hat die Rechtsprechung den Anwendungsbereich extensiv ausgelegt. Vor diesem Hintergrund ist es erforderlich:

— Die gesetzlichen Regelungen präziser und enger zu fassen,

— bei Entwicklung, Auswahl und Einsatz von Telekommunikationstechniken darauf zu achten, daß bei deren Betrieb die Speicherung personenbezogener Daten nach Dauer und Umfang auf das wirklich Notwendige beschränkt wird,

— erlaubte Eingriffe in das Grundrecht nach Art. 10 auf das unerläßliche Maß zu beschränken und eine strenge Zweckbindung der dabei gewonnenen Daten sicherzustellen,

— eine wirksame Kontrolle solcher Eingriffe durch geeignete technisch-organisatorische Maßnahmen zu gewährleisten.

Neben die Ausweitung der Möglichkeit der Überwachung der Telekommunikation treten zunehmend weitere Techniken der heimlichen Datenerhebung (z. B. durch Videoaufnahmen, Abhörgeräte, Richtmikrofone), durch die das Recht auf ungestörte Kommunikation auch außerhalb des Fernmeldebereiches gefährdet ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, daß der Gesetzgeber diesen Gefährdungen des Rechts auf informationelle Selbstbestimmung seine Aufmerksamkeit zuwendet. Sie unterstützt in diesem Zusammenhang die Einwände der Bundesregierung in deren Stellungnahme zum Gesetz-

entwurf des Bundesrates zur Bekämpfung der organisierten Kriminalität. Die Datenschutzbeauftragten sehen in der Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes einen Schwerpunkt ihrer weiteren Arbeit.

Enthaltung: Bayern

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990

Anlage 8

Telekommunikation und Datenschutz

I.

Die Telekommunikation hat außerordentlich stark an Bedeutung gewonnen und ersetzt häufig den Brief oder auch das persönliche Gespräch: Über die dreißig Millionen deutschen Telefone werden monatlich rund drei Millionen Gespräche geführt. Für die Privatsphäre des Bürgers in einer freiheitlichen Gesellschaft ist es unverzichtbar, daß Telefongespräche unkontrolliert und unbeobachtet geführt werden können. Von existentieller Bedeutung wird dies, wenn der Bürger in Notlagen gerät, aus denen er sich nur mit vertraulicher Beratung und Hilfe befreien kann. Daher unterstützen sowohl die Kirchen als auch Hilfs- und Beratungsorganisationen die Forderung, das „Grundrecht auf unbeobachtete Kommunikation" zu sichern.

Dieser Forderung muß die technische Ausgestaltung der Telekommunikationsnetze und -dienste folgen, und die rechtlichen Regelungen müssen diesen sich aus der Verfassung ergebenden Auftrag erfüllen. Der Gesetzgeber hat in dem am 01. 07. 1989 in Kraft getretenen Poststrukturgesetz die Bundesregierung aufgefordert, „Rechtsverordnungen zum Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten" zu erlassen. Der Ausschuß für Post und Telekommunikation und der und der Innenausschuß des Deutschen Bundestages haben mehrfach den Schutz des Fernmeldegeheimnisses angemahnt.

Die vom Bundesminister für Post und Telekommunikation vorgelegten Entwürfe von Verordnungen über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (TDSV) und über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (UDSV), widersprechen in wesentlichen Punkten dem Grundrecht auf unbeobachtete Kommunikation. Dabei ist besonders unverständlich, daß der Bundesminister von bereits früher gemachten Zusagen an den Deutschen Bundestag wieder abgerückt ist.

Die Entwürfe bleiben in wichtigen Punkten unter dem Datenschutzniveau, das von der EG-Kommission in ihrem Richtlinienentwurf zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen für den europäischen Binnenmarkt angestrebt wird.

II.

Ein wesentlicher Mangel besteht in der beabsichtigten Vollerfassung aller Verbindlichkeiten von Telefongesprächen: Für jedes Telefonat soll bis zur Versendung der Entgeltrechnung bei der Deutschen Bundespost TELEKOM festgehalten werden dürfen, wer wann wie lange und mit wem telefoniert hat, nach Wahl des Kunden achtzig Tage darüber hinaus. Eine monatliche Auflistung dieser dem Fernmeldegeheimnis unterliegenden Informationen (Einzelentgeltnachweis) soll jeder Kunde — auch jeder Arbeitgeber — auf Wunsch erhalten können. Außerdem können nach § 12 Fernmeldeanlagengesetz (FAG) auch Gerichte und Staatsanwaltschaften bei strafrechtlichen Ermittlungen jeder Art, also auch bei Bagatelldelikten, ohne besondere Voraussetzungen auf diese Daten zugreifen.

Abzulehnen ist auch die vorgesehene Beschränkung des Kunden auf die Alternative, daß von einem Anschluß die Telefonnummer des Anrufers immer oder nie beim Angerufenen angezeigt wird. Dem Recht auf informationelle Selbstbestimmung entspricht es, daß der Anrufer in jedem Einzelfall entscheiden kann, ob seine Rufnummer beim Angerufenen angezeigt wird. Umgekehrt hat jeder Angerufene selbstverständlich das Recht, nur Gespräche entgegenzunehmen, bei denen die Nummer des Anrufers angezeigt wird.

III.

Die Datenschutzbeauftragten fordern:

1. Alle — durch die computergesteuerte Vermittlungstechnik entstehenden — Verbindungsdaten sind nach dem Ende der Verbindung mit folgender Maßgabe unverzüglich zu löschen:

   In die Entgeltdatenverarbeitung dürfen nur diejenigen Daten eingehen, die zur Berechnung der Entgelte in Summenform unerläßlich sind . Auf beerechtigten Antrag des Kunden darf zur Prüfung der Richtigkeit des zu Recht gestellten Entgelts oder zur Erstellung des Einzelentgeltnachweises die Rufnummer des Angerufenen nur in einer zumindest um die letzten vier Ziffern verkürzten Form gespeichert werden. Die Daten sind spätestens achtzig Tage nach dem Absenden der Entgeltrechnung zu löschen.

   Die Entscheidung des Kunden über die Form muß auch bei der Abrechnung zwischen verschiedenen Netzbetreibern respektiert werden.

2. Die Erstellung von „Kommnikationsprofilen", die Aussagen über das persönliche Telefonierverhalten des Bürgers und die Nutzung anderer Telekommunikationsdienste enthalten, muß ausgeschlossen sein.

3. Bei der Anzeige der Rufnummer des Anrufers beim Angerufenen müssen beide die Wahlmöglichkeit haben, diese Anzeige entweder auf Dauer oder im Einzelfall „auf Knopfdruck" zu unterdrücken.

4. Ausnahmen von diesen Grundsätzen — zum Beispiel zur Aufklärung telefonischer Bedrohungen oder in Notfällen — müssen begründet, ausdrücklich geregelt und für den Betroffenen transparent sein.

5. Die Konferenz bekräftigte ihre Forderung (Beschluß vom 4./5. 10. 1990), Eingriffe in das grundgesetzlich geschützte Fernmeldegeheimnis (Art. 10 GG) auf das unerläßliche Maß zu beschränken und insbesondere nicht schon im Bereich der Bagatellkriminalität zuzulassen. Die Regelung des § 12 FAG hat im Zuge der technischen Entwicklung eine verfassungsrechtlich bedenkliche neue Qualität erhalten, da sie nunmehr auch die bei Einsatz neuer Kommunikationstechniken anfallenden Abrechnungs-, Verbindungs-, Nutzungs- und Inhaltsdaten umfaßt. Statt im FAG sollten die Eingriffsmöglichkeiten in das Fernmeldegeheimnis im Rahmen der Strafverfolgung — schon aus Gründen der Normenklarheit — in der Strafprozeßordnung unter engen Voraussetzungen und Beschränkungen abschließend geregelt werden.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 7./8. März 1991

Druck: Anker-Druck Bremen