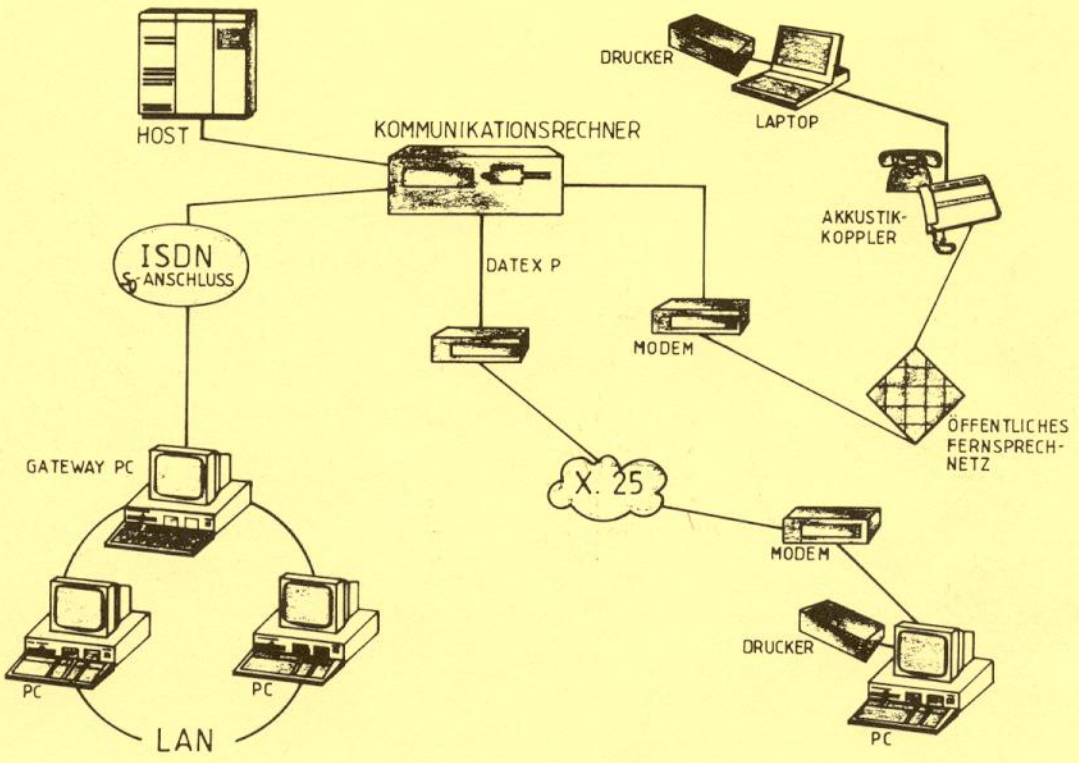
Freie Hansestadt Bremen

Landesbeauftragter für den Datenschutz

14. Jahresbericht



Beispiel für schnelle und weitverzweigte Datenkommunikation
— eine Herausforderung für den Datenschutz —

Vorgelegt zum 31. März 1992

60 Seiten

BREMISCHE BÜRGERSCHAFT
Landtag
13. Wahlperiode

Drucksache 13/97
31.03.92

Vierzehnter Jahresbericht des Landesbeauftragten für den Datenschutz

Hiermit erstattet der Landesbeauftragte für den Datenschutz der Bürgerschaft (Landtag), dem Präsidenten des Senats den 14. Bericht über das Ergebnis seiner Tätigkeit im Jahre 1991 zum 31. März 1992 (§ 33 Abs. 1 Bremisches Datenschutzgesetz).

Sven Holst, Vertreter des Landesabeauftragten für den Datenschutz

Inhaltsübersicht Seite

„Im Jahre 2000 würde ich es bestimmt vorziehen, eingefroren zu werden, aber im Jahr 3000 würde ich vermutlich lieber einem Computer überspielt werden."

F. Schwenkel

1. Überblick über das Berichtsjahr

1.1 Verantwortbarkeit des Machbaren

Dem Datenschutz wird immer wieder nachgesagt, er sei technologiefeindlich, er verhindere oder behindere doch wenigstens den gesellschaftlichen Fortschritt.

Der Volksmund sagt: Jede Medaille hat zwei Seiten. Wer so über den Datenschutz denkt, vernachlässigt grundlegende Fragen des menschlichen Zusammenlebens, die auch in der Verfassung ihren Ausdruck gefunden haben, kurz, er reduziert den Fortschritt auf das Machbare, ohne nach der Verantwortbarkeit des Machbaren zu fragen. In meinem letzten Jahresbericht habe ich geschrieben, daß der Datenschutz für einen wichtigen Teil unserer freiheitlichen Ordnung steht und die Datenschutzkontrolle dazu beitragen soll, das Grundrecht auf freie Entfaltung der Persönlichkeit zu schützen. Damit ist auch ein Teil des vor Einführung neuer Techniken erforderlichen Reflexionsprozesses angesprochen, der in jedem Fall zu führen wäre, der aber in der notwendigen Intensität keinerlei institutionelle Absicherung hat oder sonst gesellschaftlich organisiert ist. Zu fragen wäre, was diese Technik für den einzelnen Menschen und die Gesellschaft bedeutet, was verändern wir durch die Einführung neuer Techniken, was wird dadurch dem Menschen entzogen von dem, was er selbst ausüben konnte und von ihm selbst sinnlich wahrgenommen werden konnte.

Eine große Gefahr sehe ich in der Ahnungslosigkeit, mit der unsere Gesellschaft in eine Informationsgesellschaft hineinschlittert, ganz davon abgesehen, daß es an der Fähigkeit fehlt, die Grenzen der Technik und des verantwortbaren Einsatzes zu erkennen. Was wir in diesem Zusammenhang brauchen, ist sowohl eine stärker entwickelte Benutzer-Verbraucherethik als auch eine verstärkte Forscherethik. Das allein ist aber nicht ausreichend, vielmehr muß unsere immer stärker auf Partizipation und Mitwirkung angelegte Gesellschaft eine breite öffentliche Diskussion über den Weg in die Informationsgesellschaft entfachen. Denn die Bewertung gesellschaftlicher Fragen hängt auch immer von der Einbettung in die gesellschaftliche Situation ab. Seit geraumer Zeit ist Informationstechnik in Mode, wer Probleme mit dem Einsatz von Informations- und Kommunikationstechnik löst, liegt im Trend. Deshalb werden gesellschaftliche Probleme in technische Probleme verwandelt, die dann auch technisch gelöst werden. Die gesellschaftliche Situation, die zu den Problemen geführt hat, wird damit aber nicht aufgegriffen und kritisiert. D. h., nicht die Technik ist isoliert zu problematisieren, sondern die gesellschaftliche Situation, denn die Gesellschaft bestimmt die Technik.

Vor dieser Aufgabe steht partiell auch der Datenschutz, der zwar den einzelnen Bürger schützt, gleichzeitig aber durch seine ins Generelle zielenden Verfahrensfragen oder bei der Gesetzgebungsberatung versucht eine offene Gesellschaft zu erhalten. So paradox es klingen mag, aber der Datenschutz erzeugt keine geheimen, nach innen gekehrten Menschen, sondern er gibt Sicherheit mit seinen Garantien und der Forderung nach Transparenz der Datenverarbeitung und ermöglicht einen offenen Umgang unter den Bürgern, nicht nur in seinen vier Wänden, sondern auch in der Gesellschaft.

1.2 Datenschutz und Verfassung

Datenschutz ist somit ein Schutzteil demokratischer Gesellschaft. Vor dem Hintergrund der auf Landes- und Bundesebene geführten Diskussion einer Verfassungsreform steht damit auch die Frage an, Kernelemente des Datenschutzes mit Verfassungsrang auszustatten. Drei Bereiche sind in der öffentlichen Diskussion bisher angesprochen:

- Grundrecht auf informationelle Selbstbestimmung, hier haben bisher drei der alten Länder eine Regelung in ihre Verfassung aufgenommen,
- Grundrecht auf freien Informationszugang gegenüber der Exekutive und
- Verfassungsrechtliche Absicherung der Unabhängigkeit der Datenschutzbeauftragten im Sinne einer „institutionellen Verfassungsgarantie".

1.3 Novellierung des Bremischen Datenschutzgesetzes

Nach den Wahlen zur Bremischen Bürgerschaft 1991 haben sich die Koalitionsparteien darauf geeinigt, das Bremische Datenschutzgesetz, soweit erforderlich, den Bestimmungen des neuen Bundesdatenschutzgesetzes anzugleichen, dabei soll insbesondere die Möglichkeit der Einführung eines Schadensersatzanspruchs

im Bremischen Datenschutzgesetz geprüft werden. Außerdem soll dem Landesbeauftragten für den Datenschutz ein Rederecht in der Bürgerschaft zur Erläuterung des Jahresberichts und seiner Gutachten eingeräumt werden. Begleitet werden soll die Weiterentwicklung des Datenschutzrechts, wie auch dessen praktische Durchsetzung, von der Pflege des Datenschutzbewußtseins aller Verantwortlichen.

Ohne den Beratungen vorgreifen zu wollen, möchte ich an dieser Stelle darauf hinweisen, daß im Rückblick gesehen die Entwicklung des Datenschutzes ein gutes Beispiel abgibt für die Bedeutung und Leistungskraft eines konsequent praktizierten Föderalismus. Schließlich waren es Landesgesetzgeber, die weit vor dem Bund mit gesetzlichen Regelungen zur automatisierten Verarbeitung personenbezogener Daten reagierten. Sie waren es auch — und Bremen mit an vorderster Stelle —, die seither immer wieder die Initiative ergriffen haben, um bestehende Regelungen zu verbessern und auszubauen. Der Kollege Spiros Simitis kommt denn auch zu dem Schluß, dem Bundesdatenschutzgesetz stehe eine „Leitfunktion" nicht zu, auch könne von ihm nicht erwartet werden, Lösungen für alle Datenschutzprobleme anzubieten, dem Grundgesetz sei eine Verpflichtung zur Konformität nicht zu entnehmen. Ich meine, in diesem Sinne sollte das Land Bremen weiterhin die Chance wahrnehmen, die vom Grundgesetz zugestandenen Gestaltungsspielräume in vollem Umfange zu nutzen.

Weiterhin hat es in der Bürgerschaft eine Initiative gegeben, die die Stellung und Bedeutung des Landesbeauftragten für den Datenschutz betrafen. Die Fraktionen der Grünen und der FDP hatten 1990 Anträge zur Änderung des Bremischen Datenschutzgesetzes in die Bürgerschaft eingebracht (Bürgerschaftsdrs. 12/931 und 12/969). Die Gesetzentwürfe sahen vor, den Landesbeauftragten für den Datenschutz von der Bürgerschaft (Landtag) mit der Mehrheit von zwei Dritteln ihrer Mitglieder zu wählen. Die Bürgerschaft lehnte nach Aussprache beide Vorlagen mit Mehrheit ab. Am 24. 01. 1991 haben 40 Mitglieder der Bürgerschaft, die den Fraktionen der CDU, der Grünen und der FDP angehörten, den Staatsgerichtshof angerufen. Der Staatsgerichtshof hat in seiner am 18. 11. 1991 verkündeten Entscheidung (St 1/91) festgestellt: „Nach Art. 90 der Landesverfassung ist die einfache Stimmenmehrheit der in der Versammlung Anwesenden auch für Wahlen maßgebend; eingeschlossen sind Wahlen, die aufgrund von einfachen Landesgesetzen durchzuführen sind."

1.4 Datenschutzrechtlich bedeutsame Gesetzgebung, Initiativen und Verordnungen

Auch im letzten Jahr sind sowohl vom Landes- als auch vom Bundesgesetzgeber neue Datenschutzregelungen verabschiedet worden. In Bremen hat die Bremische Bürgerschaft (Landtag) das Archivgesetz (vgl. Pkt. 2.4 dieses Berichtes) und das Energiegesetz (vgl. Pkt. 2.8.3 des Berichts) verabschiedet.

Auf Bundesebene ist am 01. 06. 1991 das neue Bundesdatenschutzgesetz in Kraft getreten. Vorrangiges Ziel war es, das aus dem Jahre 1977 stammende Bundesdatenschutzgesetz den Anforderungen aus dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 anzupassen. Das neue Datenschutzgesetz hat die Akte im öffentlichen Bereich in den Schutzbereich des Gesetzes einbezogen, neu ist auch die Einführung des verschuldensunabhängigen Schadensersatzanspruchs gegen öffentliche Stellen sowie die Verstärkung der Zweckbindung bei der Verarbeitung oder Nutzung personenbezogener Daten. Die von den Datenschutzbeauftragten seit langem geforderten Regelungen des Datenschutzes für Arbeitnehmer (vgl. hierzu auch den Beschluß der Datenschutzkonferenz, Anlage des Berichts), sind von dem Gesetz nicht umgesetzt worden, hingegen enthält das Gesetz bereichsspezifische Regelungen für die Datenverarbeitung in Wissenschaft und Forschung sowie bei Rundfunkanstalten des Bundes. Die in § 24 Abs. 2 BDSG getroffene Regelung, die dem Bürger ein Widerspruchsrecht gegen die Einbeziehung seiner Daten in die Datenschutzkontrolle vorsieht, muß als verfehlt angesehen werden. Auf einige rechtliche Aspekte der vom neuen BDSG getroffenen Regelungen für den nicht-öffentlichen Bereich gehe ich unter Pkt. 3.1 dieses Berichtes ein.

Für Klarstellung hat auch die Entscheidung des Bundesverfassungsgerichts (Beschluß vom 11. 06. 1991 — 1 BvR 239/90) in der Debatte gesorgt, ob denn das mit dem Volkszählungsurteil bestätigte Recht auf informationelle Selbstbestimmung auch im Privatbereich Wirkung entfalten könne. Nach dieser Entscheidung umfaßt das allgemeine Persönlichkeitsrecht die Befugnis des einzelnen über die Preisgabe und Verwendung seiner persönlichen Daten, zu denen auch Akten

gehören, selbst zu bestimmen. In seiner Entscheidung hat das Bundesverfassungsgericht ausgeführt: „Geschützt ist das so gewährleistete, allgemeine Persönlichkeitsrecht nicht nur vor direkten staatlichen Eingriffen. Es entfaltet als objektive Norm einen Rechtsgehalt auch im Privatrecht und strahlt in dieser Eigenschaft auf die Auslegung und Anwendung privatrechtlicher Vorschriften aus."

Weiter ist auf den Entwurf zur Gewerbeordnung (vgl. Pkt. 2.8.2 des Berichts) und auf einen weiteren Entwurf eines Gesetzes über Mitteilungen der Justiz vom Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz) hinzuweisen. Der jetzt vorgelegte Entwurf enthält weiterhin einige datenschutzrechtliche Defizite. Die Empfehlungen der Datenschutzbeauftragten wurden nur in geringem Maße oder gar nicht berücksichtigt. Schließlich haben die auch nach Inkrafttreten der Telekommunikationsdatenschutzverordnungen TDSV und UDSV (vgl. Pkt. 1.6.1 dieses Berichts) weiterhin bestehenden datenschutzrechtlichen Fragestellungen im Bereich der Telekommunikation bei meinen Beratungen, insbesondere von Nutzern und Betroffenen, eine wesentliche Rolle gespielt.

1.5 Aufbewahrungs- und Löschungsfristen

In fast allen Bereichen der Verwaltung kommt es immer wieder zu Auseinandersetzungen darüber, wie lange Akten und Datenträger aufbewahrt werden dürfen und wann sie zu vernichten bzw. zu löschen sind. Diese Frage zieht sich über Jahre wie ein roter Faden durch die Jahresberichte: Wann sind Gesundheitsakten beim Hauptgesundheitsamt zu löschen, wann Beratungsakten, wann Akten beim Verfassungsschutz oder der Polizei, wann sind Ordnungswidrigkeiten zu vernichten usw.?

In den meisten Fällen fehlen präzise gesetzliche Löschungsvorschriften. In anderen Fällen wird darum gestritten, ob z. B. gesetzliche Tilgungsfristen oder Verwertungsverbote konsequent eine Löschung der Akte nach sich ziehen oder ob die Verwaltungsbehörde die Vorgänge trotzdem länger aufbewahren darf, z. B. weil die Akte irgendwann einmal später der Rechnungsprüfung unterliegen könnte. Sicherlich ist es auch möglich, einen Vorgang zu früh zu vernichten. Die bisher an mich gerichteten Eingaben beklagten sich aber allesamt über die Weigerung der Verwaltungsbehörden, Akten zu vernichten oder Daten zu löschen.

§ 20 Abs. 3 Nr. 2 BrDSG sagt wie selbstverständlich: Personenbezogene Daten sind zu löschen, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Wann aber dieser Zeitpunkt eingetreten ist, darüber läßt sich vortrefflich streiten. Der Gesetzgeber regelt in vielen bereichsspezifischen Regelungen wer was wann und wozu erheben und verarbeiten darf, eine Regelung, wann zu löschen oder zu vernichten ist, wird in den seltensten Fällen getroffen.

Deshalb ist es dringend erforderlich, Löschungs- und Vernichtungsbestimmungen für alle Verwaltungsbereiche zu schaffen. Damit wäre dann auch die Lücke zwischen aktiver Bearbeitung und Archivierung (vgl. Landesarchivgesetz Pkt. 2.4 des Berichts) geschlossen.

1.6 Datenschutzprobleme rund um das Telefon

Die ISDN-Telefontechnik und andere von der Deutschen Bundespost — TELEKOM angebotenen Dienste haben nicht zuletzt wegen der vielen Bürgeranfragen zu einem Beratungsschwerpunkt geführt. Die Verbindungen der bisher selbständigen Kommunikationsmöglichkeiten (wie Sprache, Schrift und Bild) werden durch die technischen Entwicklungen integriert und zu komplexen Kommunikationssystemen umgestaltet. Die daraus entstehenden Nutzungsmöglichkeiten führen in verschiedenen Bereichen zu neuen Datenschutzproblemen. Einige davon sollen im Folgenden näher ausgeführt werden.

1.6.1 Unzureichender Datenschutz beim Telefonieren

Am 1.Juli 1991 ist die Telekommunikations-Datenschutzverordung — TDSV — für die Deutsche Bundespost — TELEKOM — in Kraft getreten. Die TDSV regelt die Datenverarbeitung und deren Schutz beim Fernmeldeverkehr, soweit er von der Deutschen Bundespost betrieben wird. Für den nicht-öffentlichen Bereich gilt die Telekommunikations-Unternehmens-Datenschutzverordnung — UDSV —. Beide Verordnungen gestatten Eingriffe in das informationelle Selbstbestimmungsrecht der Fernsprechbenutzer, die im Gesetz selbst hätten geregelt werden müssen.

Bei der Gestaltung der Technik, wie auch der Abfassung der Verordnungen standen wirtschaftliche Interessen im Vordergrund, während das Recht und die Befugnisse des Einzelnen auf ungestörte und unbeobachtete Kommunikation nicht hinreichend berücksichtigt wurden. Die Anregungen der Datenschutzbeauftragten und die Wünsche der Vertreter gesellschaftlicher Gruppen und Organisationen, wie z. B. Kirchen, Gewerkschaften, Ärzteverbände und Sozialverbände sind offensichtlich nicht ausreichend berücksichtigt worden. Bei einer frühzeitigen Beteiligung dieser Gruppen und einer rechtzeitigen Offenlegung der Absichten der Post hätte eine Vielzahl von datenschutzrechtlichen Problemen vermieden werden können.

Mit der Einführung der ISDN-Technik wird sich vieles ändern. Während bisher bei allen Fernsprechteilnehmern nur die Summen der Fernsprechgebühren (ähnlich einem Stromzähler) gezählt wurden, darf die DBP-TELEKOM seit dem 01. 07. 1991 — und nach Erlaß der UDSV sind auch die privaten Diensteanbieter dazu berechtigt — die Verbindungsdaten der Fernsprechteilnehmer speichern. Aus den Verbindungsdaten ist zu erkennen, wer mit wem, wann, wie lange, von welchem, zu welchem Ort und mit welcher Technik Kommunikation betrieben hat. Diese sensiblen Verbindungsdaten werden bei den Anbietern (TELEKOM oder private Netzbetreiber) bis zu achtzig Tage nach Versand der Entgeltabrechnung gespeichert. Zwar werden keine Gesprächsinhalte gespeichert, jedoch ist die Kenntnis der Verbindungsdaten in vielen Fällen ausreichend, um sich ein klares Bild von den Planungen, Aufenthalten, Vorhaben oder Problemen des Fernsprechteilnehmers zu machen.

Es ist erforderlich, daß die Bürger verantwortlich für sich als Fernsprechteilnehmer oder als Mitbenutzer entscheiden, ob sie einen Einzelentgeltnachweis wünschen oder aus Gründen des Schutzes ihrer Daten darauf verzichten und eine vollständige oder eine teilweise (Verkürzung um die letzten drei Rufnummern) Löschung der Verbindungsdaten beantragen. Diese Antragsrechte haben auch juristische Personen (Firmen, Vereine, Stiftungen u. a. m.) für ihren Fernmeldeverkehr.

Auch gibt es Probleme beim Schutz der Vertraulichkeit der Anrufe bei den Beratungsstellen, wie Telefonseelsorge, Drogenberatung, Erziehungsberatung etc., durch die Aufzeichnung im Einzelgebührennachweis. Ich habe diese Stellen darüber informiert, daß die Deutsche Bundespost — TELEKOM verpflichtet ist, die Aufzeichnung derartiger Anrufe zu unterdrücken.

Bisher fehlen ausreichende technische Schutzvorkehrungen, für die Nutzer ist nicht zu erkennen, ob für einen Anschluß beim Telefonieren ein Einzelgebührennachweis erstellt wird oder nicht.

Ein Datenschutzproblem bildet weiterhin die Rufnummernanzeige des Anrufenden beim Angerufenen. Die DBP-TELEKOM bietet nach wie vor nur die Möglichkeit der generellen Anzeige oder der Nichtanzeige an. Eine Wahlmöglichkeit für jedes Einzelgespräch wird erst ab 01. 01. 1994 bei Einführung von Euro-ISDN eröffnet. Allerdings wird dieses dann nur mit neuen ISDN-Geräten möglich sein, die bis dahin eingesetzten ISDN-Geräte können nach Herstellerangaben nicht umgestellt werden.

Die in den Verordnungen vorgesehene Ausnahme der Rufnummernanzeige im Display des Angerufenen — die nur auf Antrag erfolgt — beschränkt sich nur auf einen kleinen Teil der Beratungsstellen, außerdem fehlt die Einbeziehung von Ärzten, Seelsorgern, Rechtsanwälten, Journalisten u. a.. Auch scheint der Verordnungsgeber das Problem der zugesicherten Vertraulichkeit bei Anrufen bei der Polizei überhaupt nicht gesehen zu haben. Ein anonymer Anruf bei der Polizei ist beim Einsatz von ISDN-Technik nicht mehr sichergestellt.

Vielmehr läßt die neue Technik zu, daß selbst bei Abwesenheit des Angerufenen alle Rufnummern der Anrufer auf einem Drucker oder einem anderen Medium gespeichert und evtl. sogar für andere Zwecke genutzt werden. Ebenso können die Bewegungsdaten im Mobilfunkdienst (Autotelefon, Satellitenfunk, Cityfunk u. a.) für Zwecke der Verhaltenskontrolle und -überwachung verwendet werden. Da die technische Entwicklung erst am Anfang steht, können zukünftige Gefahren für das informationelle Selbstbestimmungsrecht nur erahnt werden.

Im Moment hat der Nutzer wenige Möglichkeiten, auf den Datenschutz beim Telefonieren selbst Einfluß zu nehmen. Gleichwohl sollte jeder Fernmeldeteilnehmer für sich und seine Partner sorgfältig prüfen, wie er die Gefahren für das informationelle Selbstbestimmungsrecht so gering wie möglich halten kann.

1.6.2 Das gesamte Telefonbuch der Bundesrepublik Deutschland auf CD-ROM

Jeder kennt die CD (Compact Disc) wie sie heute perfekte Ton — insbesondere Musiküberspielung ermöglicht. In den letzten Jahren werden diese CD auch als Massendatenspeicher verwendet und unter der Bezeichnung CD-ROM (ROM = Read only memory) geführt. So ist es möglich, den Inhalt umfangreicher Lexika und Gesetzes- oder Urteilssammlungen auf einer einzigen CD-ROM zu speichern, wogegen keine datenschutzrechtlichen Bedenken bestehen. Diese Datenträger werden aber auch als sogenannte elektronische Telefonbücher eingesetzt und vertrieben. Für die gesamte Bundesrepublik Deutschland würden fünf CD-ROM ausreichen, um den Inhalt aller derzeitigen Telefonbücher zu speichern. Die Fähigkeit auf der CD-ROM Daten zu suchen, abzurufen und auszuwerten hängt ausschließlich von der eingesetzten Software ab.

Die Vorteile eines solchen Verzeichnisses liegen auf der Hand. Zu bedenken ist aber auch, daß durch die Erstellung des elektronischen Telefonbuchs auf diesem Wege ein riesiges Adressenverzeichnis — eine Art Ersatz-Melderegister — entstehen würde, während die Rechtsordnung z.B. die Zusammenfassung aller Meldedaten eines Landes oder gar für die Bundesrepublik Deutschland nicht zuläßt. Aber damit sind noch nicht alle Probleme beschrieben, denn diese CD-ROM lassen nicht nur eine gezielte Suche nach Name und Vorname zu, um Telefonnummer und evtl. Adresse zu erhalten. Nein, auch nach Anschrift, z. B. wer wohnt in der Stadt Y in der A-Str. von Nr. 1 — 50 kann selektiert werden oder nach der Rufnummer, z. B. wer verbirgt sich hinter der Rufnummer XXXXX — oder nach den Berufsangaben — soweit angegeben — kann gesucht werden. Mit entsprechender Software läßt sich eine Vielzahl von Auswertungen erstellen, wie z. B. nach sozialen Kriterien nach Formen des Zusammenlebens wie Single, getrenntlebende Eheleute insbesondere, wenn sie vorher einen gemeinsamen Anschluß hatten oder nach Wanderungsbewegungen (Umzüge wohin oder woher). Aus diesen wenigen Daten können Marketing-Strategien für Werbefeldzüge entwickelt werden, auch für die sog. Direktwerbung (Telefonwerbung) bietet das elektronische Telefonbuch erfolgversprechende Ansätze, dies war auch einer Information der Handelskammer Bremerhaven zu entnehmen. Diese Darstellung erhebt keinen Anspruch auf Vollständigkeit, denn der Ideenvielfalt ist ein breiter Raum gegeben, wenn beispielsweise die Versicherungen, Banken, Versandhäuser, Reisebüros u. a. ihre eigenen Datenbestände gegen diesen Datenbestand laufen lassen würden.

Die Deutsche Bundespost TELEKOM hat die Datenschutzregelungen für das elektronische Telefonbuch so gestaltet, daß nur wenn der Teilnehmer auf die Aufnahme in das örtliche Telefonbuch verzichtet, er auch nicht im elektronischen Telefonbuch aufgenommen wird. Der Teilnehmer hat also keinen eigenen Spielraum zu entscheiden, ob er nur in das örtliche (amtliche) Telefonbuch aber nicht in das elektronische Telefonbuch aufgenommen werden will oder umgekehrt. Es ist durchaus denkbar, daß der Teilnehmer keine Einwände gegen die Aufnahme in das örtliche Telefonbuch hat, aber erhebliche Bedenken gegen eine bundesweite Offenbarung. Die Deutsche Bundespost — TELEKOM — bleibt aufgefordert, die Rechtsvorschriften so zu fassen, daß der Teilnehmer im einzelnen entscheiden kann, ob seine Daten nur für das örtliche Telefonbuch, für das elektronische Telefonbuch oder auch für andere Zwecke (Postreklame) genutzt werden dürfen.

Alle Anschlußinhaber sollten daher sehr genau überlegen, ob und welche Daten sie für die Eintragung in dem Telefonbuch freigeben.

1.6.3 Probleme bei dem Einsatz von Telefax-Geräten

Im letzten Jahresbericht (S. 19 und 55) hatte ich auf Probleme des Datenschutzes und des Fernmeldegeheimnisses bei der Verwendung von Telefax-Geräten hingewiesen. Dies hat im Berichtsjahr zu einer Vielzahl von Nachfragen und Erlebnisschilderungen von Bürgern geführt, die meine Befürchtungen bestätigen, daß die Funktionsweise und die Risiken der Telefax-Technik nicht hinreichend bekannt sind. Aufgrund dieser Feststellungen und meiner Erfahrungen wurde von mir ein Kriterienkatalog für Schutzmaßnahmen entworfen und weiterentwickelt.

Dieser Kriterienkatalog wird die Grundlage einer Handreichung oder Richtlinie bilden, die ich zur Zeit mit dem für die Telekommunikation in der bremischen Verwaltung zuständigen Fernmeldetechnischen Amt der Stadt Bremen erarbeite, um datenschutzrechtlichen Gefahren bei dem Einsatz von Telefax-Geräten durch Aufklärung und Anregung von geeigneten technischen und organisatorischen Maßnahmen zu begegnen.

1.6.4 Leistungsmerkmale von Telefonanlagen

Der Senat der Freien Hansestadt Bremen und der Gesamtpersonalrat haben am 3. Mai 1991 die Dienstvereinbarung über den Betrieb und die Nutzung von Telekommunikationsanlagen (Fernsprechanlagen) abgeschlossen.

Diese Dienstvereinbarung enthält im wesentlichen Datenschutzregelungen für die Betreiber und Nutzer von Telefonanlagen in der bremischen Verwaltung. Diese Regelungen sollen aber nicht nur die informationellen Rechte der Mitarbeiter der Verwaltung schützen sondern auch die der anrufenden oder angerufenen Bürger, denn die Information wer, wann, mit wem, wie lange und von welchem Ort Telekommunikation betreibt, fällt unter das Fernmeldegeheimnis, und ist deshalb besonders schutzwürdig.

So regelt die Dienstvereinbarung z.B. präzise, wer (nur Zentralen) und unter welchen Bedingungen (begleitender Ton), sich jemand in bestehende Ferngespräche aufschalten darf. Weiter beschreibt die Dienstvereinbarung den Umfang der sog.Leistungsmerkmale von Telefonanlagen die installiert werden dürfen, wie auch einzelne Leistungsmerkmale, die nur installiert werden dürfen, wenn eine besondere Vereinbarung zwischen Dienststellenleiter und Personalrat getroffen wird. Schließlich legt sie Leistungsmerkmale fest, die nicht installiert werden dürfen.

Für folgende Leistungsmerkmale sieht die Dienstvereinbarung eine generelle Freigabe vor:

- Wahlwiederholung
- Anrufumleitung (wobei beide Stellen an der Aktivierung beteiligt sein müssen)
- Kurzwahl, individuell
- Makeln
- elektronisches Sperrschloß
- automatischer Rückruf im Besetztfall.

Folgende Leistungsmerkmale bedürfen zu ihrer Freigabe einer entsprechenden Vereinbarung zwischen Dienststellenleiter und örtlichem Personalrat:

- Kurzwahl, zentral
- Sammelanschluß
- Anrufübernahme
- integrierte Vorzimmerfunktion
- feste Anrufumleitung
- selbständige Rufweiterleitung

Bei Gesprächen mit industriellen Anbietern stellte ich fest, daß diese Leistungsmerkmale z. T. sowohl begrifflich als auch inhaltlich nicht einheitlich sind und unterschiedlich interpretiert werden. Die Telefonnebenstellenanlagen sind mit vielfältigen Leistungsmerkmalen ausgestattet, die sie zu „Alleskönnern" machen, allerdings sind einfache Datenschutzvorkehrungen zum Teil nicht enthalten oder diese erst nachträglich installiert werden müssen. Die Einschränkung des Umfangs der Leistungsmerkmale durch die Dienstvereinbarung sowie das besondere Freigabeverfahren für bestimmte Leistungsmerkmale stellt einen Schutz vor dem technisch Machbaren dar. Aus datenschutzrechtlicher Sicht ist dazu folgendes anzumerken:

- Wahlwiederholung

  Dieses Merkmal kann durch einen Dritten ausgelöst werden und dieser kann dann feststellen (insbesondere bei Displaytelefonen), wer angerufen wurde, ohne Rücksicht, ob das Gespräch zustande gekommen war oder nicht. Die Nutzer sollten darüber unterrichtet werden, wie der Wahlwiederholungsspeicher gelöscht werden kann.

- Anrufumleitung

  Die Gestaltung dieses Leistungsmerkmals — wenn auch die geforderte technische Umsetzung noch nicht von der Industrie angeboten wird — sollte so erfolgen, daß dem Anrufer deutlich durch Signalton und/oder Anzeige auf dem Display signalisiert wird, daß der Anruf umgeleitet wird. So wäre sichergestellt, daß der Anrufer die Möglichkeit hat, vor der Herstellung der Verbindung durch Anrufumleitung den Vorgang abzurechen oder sich auf einen anderen Gesprächspartner einzustellen.

Auch sollte technisch sichergestellt werden, daß nur auf bestimmte Nummernkreise umgeleitet werden kann, um zu verhindern, daß Gespräche über eine behördliche Einheit hinaus umgeleitet werden.

— Kurzwahl, individuell

Die persönlichen Benutzer-Kurzwahlziele sollten im Telefonapparat gespeichert werden. Die Speicherung dieser Nummern im Zentralspeicher der Nebenstellenanlage birgt die Gefahr des Auslesens des Speicherinhalts und deren unzulässige Nutzung in sich.

— Elektronisches Sperrschloß

Der Code dieses Sperrschlosses sollte mindestens vierstellig sein, um eine hohe Sicherheit zu bieten. Durch die Sperrwirkung dieses Schlosses muß sowohl die unerlaubte Fremdnutzung als auch die Nutzung oder Veränderung der Leistungsmerkmale verhindert werden.

— Rufnummernanzeige

Datenschutzrechtlich ist zu begrüßen, daß die Dienstvereinbarung regelt, daß bei der Anzeige der rufenden Nummer im Display des Angerufenen, dieses nicht ohne Zustimmung des Anrufenden erfolgen darf. So lange die Industrie entsprechende Technik nicht zur Verfügung stellt, ist eine Anzeige nicht zugelassen.

— Gebührendatenverarbeitung

Bei der Gebührendatenverarbeitung von Privatgesprächen sollte eine Reduzierung des Speicherumfangs geprüft werden, wenn die Telefonanlagen und Telefonapparate manipulationssicher und gegen Fremdbenutzung geschützt sind, z. B. durch ein elektronisches Schloß. In diesem Falle wäre die Anzeige und Speicherung der Gebühreneinheiten ausreichend.

Unabhängig davon habe ich festgestellt, daß die Industrie Telefonnebenstellenanlagen anbietet, die mit weiteren Leistungsmerkmalen ausgestattet sind, die z. T. besondere datenschutzrechtliche Probleme aufwerfen. Hier möchte ich nur einige anführen:

— Automatischer Rückruf im Freifall

In diesem Fall werden die Anrufe, die bei Abwesenheit des Teilnehmers ankommen gespeichert und durch z. B. ein später geführtes Telefonat wird der Rückruf automatisch ausgelöst. Hier ist aus datenschutzrechtlicher Sicht zu fordern, daß dieses Leistungsmerkmal nur durch ein aktives und bewußtes Handeln des Angerufenen (= Rückrufenden) ausgelöst wird.

— Freisprechen

Durch dieses Leistungsmerkmal ist es möglich, ohne daß der Hörer abgenommen wird, mit einem anderen Teilnehmer zu telefonieren. Dabei werden anstelle des Hörers im Telefonapparat installierte Lautsprecher und Mikrophone aktiviert. Die Leistung von Lautsprecher und Mikrophon wird durch Technik verstärkt, so daß sowohl Raumgespräche an einen Einzelnen übertragen werden können als auch mehrere Personen mithören können, was zwischen zwei Teilnehmern gesprochen wird. Dadurch kann die „Privatheit" eines Telefongesprächs verloren gehen. Auch könnte die Freisprecheinrichtung als Abhöranlage mißbraucht werden, wenn z. B. ein Teilnehmer den Telefonapparat auf „freisprechen" stellt und einen anderen Teilnehmer anruft, ohne daß die im Raum anwesenden Gesprächsteilnehmer davon Kenntnis haben.

— Baby-call

Datenschutzrechtlich wenigstens ebenso problematisch ist die Möglichkeit einer Raumüberwachung mit Hilfe der Funktion „Baby-call". Dieses Leistungsmerkmal bieten viele moderne Telefonapparate. Von einem beliebigen Telefon aus kann diese Funktion aktiviert werden; ohne die Kenntnis der im Raum befindlichen Personen schaltet sich im Telefon ein Mikrophon ein und gestattet dem Anrufer das Abhören der im Raum geführten Gespräche.

Ich empfehle allen, angesichts der beschriebenen technischen Möglichkeiten, sich vor Installation von Telefonnebenstellenanlagen und Endgeräten über die Leistungsmerkmale einen genauen Überblick zu verschaffen, die Risiken — gegebenenfalls mit meiner Hilfestellung — auszuloten und eine präzise Entscheidung zu treffen. Dann ist festzulegen, welche der Leistungmerkmale installiert werden sollen und wie diese genutzt werden dürfen.

2. Öffentlicher Bereich

2.1. Personalwesen

2.1.1 Datenschutz im Recht des öffentlichen Dienstes

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 26./27. September 1991 in einer Entschließung zum „Datenschutz im Recht des öffentlichen Dienstes" bekräftigt, daß jede Verarbeitung von Daten der Beamten, Angestellten und Arbeiter eine Einschränkung des informationellen Selbstbestimmungsrechts dieser Personen bedeutet und einer verfassungsgemäßen Rechtsgrundlage bedarf (Anlage).

Bremen hat mit der Novellierung des Bremischen Datenschutzgesetzes im Jahre 1987 Datenschutzregelungen bei Dienst- und Arbeitsverhältnissen erlassen und ist mit diesen Regelungen führend im Vergleich zu Bund und Ländern. Die im Beschluß aufgeführten Forderungen gehen jedoch auch über diese Regelungen weit hinaus und geben eine Vielzahl von konkreten Anregungen.

2.1.2 Auskunft aus Personalakten an Dritte

Die Senatskommission für das Personalwesen (SKP) wird vielfach von privaten Stellen aufgefordert, Auskünfte über Beschäftigte zu erteilen mit dem Hinweis, diese hätten darin eingewilligt. Ich habe sie darauf hingewiesen, daß Schweigepflichtentbindungsklauseln (z. B. in Versicherungsverträgen), die von „Behörden" bzw. „Stellen" allgemein sprechen, nicht genügend bestimmt sind, um wirksam zu sein. Den datenschutzrechtlichen Anforderungen an eine Einwilligungserklärung entsprechen sie nicht. Die personalaktenführenden Stellen haben im Rahmen der verwaltungsrechtlichen Ermessensausübung zu beurteilen, ob die Einwilligungserklärung hinreichend bestimmt und detailliert ist. Im Zweifel sollten Übermittlungen unterbleiben. In solchen Fällen ist es angemessen, die fraglichen Informationen den Bediensteten zuzuleiten und anheim zu stellen, sie selbst an Dritte zu übermitteln. Die SKP teilt meine Rechtsauffassung und hat die Personalstellen der bremischen Verwaltung gebeten, entsprechend zu verfahren.

2.1.3 Versendung der Lohnsteuerkarten

Immer wieder haben sich Beschäftigte an mich gewandt und moniert, daß die Lohnsteuerkarten von der zentralen Gehaltsstelle der Senatskommission für das Personalwesen (SKP) für die einzelnen Beschäftigungsdienststellen gebündelt weitergeleitet und von den jeweiligen Personalstellen, den Schulsekretariaten u. a. am Ende eines jeden Jahres offen an die Betroffenen zurückgegeben wurden. In Beschwerden wurde gerügt, der Hausmeister habe die mit dem Jahreseinkommen und den Abzügen versehene Lohnsteuerkarte ohne Umschlag ausgehändigt, Beschäftigte fänden ihre Karte offen in ihrem Fach oder auf dem Schreibtisch oder es sei zu Verwechslungen bei der Verteilung gekommen.

Nach nunmehr zehn Jahren ist es gelungen, bei der SKP ein datenschutzgerechtes Verfahren durchzusetzen. Danach werden sämtliche Lohnsteuerkarten von der zentralen Gehaltsstelle einzeln in verschlossenen Umschlägen über die Dienststellen an die Betroffenen gesandt.

2.1.4 Übermittlung von Beschäftigtendaten an Rechtsanwälte

Aufgrund einer Beschwerde habe ich festgestellt, daß die Senatskommission für das Personalwesen (SKP) Auskunftsersuchen von Rechtsanwälten zur Vorbereitung eines Antrags auf vorläufiges Zahlungsverbot bzw. Pfändungs- und Überweisungsbeschluß beantwortet. Als Rechtsgrundlage hat die senatorische Behörde § 845 Zivilprozeßordnung (ZPO) angegeben.

Die Vorschrift besagt jedoch lediglich, daß der Gläubiger vor der Pfändung aufgrund eines vollstreckbaren Schuldtitels durch den Gerichtsvollzieher dem Drittschuldner die Benachrichtigung, daß die Pfändung bevorstehe, zustellen lassen kann. Daraus ergibt sich für die SKP keine Berechtigung, derartige Auskünfte an Rechtsanwälte zu erteilen. Die SKP will künftig daher Auskünfte nur noch erteilen, wenn der Betroffene vorher schriftlich eingewilligt hat.

2.1.5 Dienstvereinbarung „Sucht"

Das Personalamt hat mir seinen Entwurf für eine Dienstvereinbarung zwischen dem Magistrat der Stadt Bremerhaven und dem Gesamtpersonalrat beim Magistrat über den Umgang mit Suchtkranken oder suchtgefährdeten Mitarbeitern/innen

zur Stellungnahme vorgelegt. Der Entwurf baut auf der entsprechenden Dienstvereinbarung auf, die in 1989 die Senatskommission für das Personalwesen und der Gesamtpersonalrat für das Land und die Stadtgemeinde Bremen abgeschlossen haben. Mir war seinerzeit nicht Gelegenheit gegeben worden, hierzu Stellung zu nehmen. Der datenschutzrechtliche Aspekt derartiger Vereinbarungen liegt darin, daß gesundheitliche Probleme heikelster Art der betroffenen Beschäftigten zum Gegenstand von Vorgängen gemacht werden, an denen die personalführende Stelle, Kollegen, Suchtberater und Personalräte beteiligt sind. Dabei sind diese Vorgänge vom vertraulichen ersten Gespräch der personalführenden Stelle mit dem Betroffenen bis zu dienstrechtlichen Konsequenzen gestuft. Die Rechtsgrundlagen dafür finden sich im Beamtengesetz, in der Disziplinarordnung und in Tarifverträgen. Zudem ist zu berücksichtigen, daß es von der Sache her unumgänglich sein kann, Suchtkranke offen mit den Folgen ihres Verhaltens zu konfrontieren, notfalls Konsequenzen anzudrohen und dann auch zu handeln.

Falls erforderlich, soll die personalführende Stelle den Betroffenen in einem zweiten Gespräch auf dienst- und versicherungsrechtliche Konsequenzen hinweisen und ihn auffordern, sich von der betrieblichen oder von einer anderen Suchtkrankenhilfe beraten zu lassen. Ich begrüße es, daß der Entwurf des Personalamts der Stadt Bremerhaven es der Entscheidung des Betroffenen überlassen will, ob die betriebliche Suchtkrankenhilfe schon zu diesem Gespräch hinzugezogen wird. Allerdings habe ich empfohlen, die Beteiligung des Personalrats gleichfalls von der Entscheidung des Betroffenen abhängig zu machen und es ihm überdies zu ermöglichen, ein bestimmtes Mitglied des Personalrats zu benennen.

Die Senatskommission für das Personalwesen und der Gesamtpersonalrat des Landes und der Stadtgemeinde Bremen sollten die von ihnen abgeschlossene Dienstvereinbarung noch einmal in diesem Sinne überdenken.

2.1.6 Fehlerhafte Telefondatenspeicherung und -abrechnung beim FTA

Mitarbeiter der Freien Hansestadt Bremen dürfen nach den Fernsprechrichtlinien private Ferngespräche führen, wenn sie damit einverstanden sind, daß diese Gespräche ihnen in Rechnung gestellt werden. Für die Abrechnung speichert das Fernmeldetechnische Amt (FTA) neben dem Datum, der Uhrzeit und der Anzahl der aufgelaufenen Gebühreneinheiten auch die Zielrufnummer. Um das Fernmeldegeheimnis zu schützen, sollen die beiden letzten Ziffern der Rufnummer nicht erfaßt werden.

Aufgrund einer Eingabe erhielt ich davon Kenntnis, daß dieses System nicht sicher ist. Ein betroffener Beschäftigter stellte fest, daß auf seiner Gebührenabrechnung stets auch „Phantomgespräche" aufgeführt und abgerechnet sind, die tatsächlich nicht stattgefunden haben und nach der gespeicherten Länge des Gesprächs falsche Gebühreneinheiten ergaben. Zu diesen „Phantomgesprächen" kam noch ein weiteres Phänomen dergestalt hinzu, daß die vollständige Rufnummer des vorher tatsächlich geführten Gesprächs angezeigt wurde. Die Zielnummern der Privatgespräche waren damit nicht nur für das FTA, sondern auch für die Beschäftigungsdienststelle erkennbar. Ein klarer Verstoß gegen § 8 der Dienstvereinbarung über den Betrieb und die Nutzung von Telekommunikationsanlagen (Fernsprechanlagen) vom 03. 05. 1991 (BrAbl. Nr. 43).

Es ist nicht auszuschließen, daß auch bei anderen vergleichbare Fehler aufgetreten sind, ohne daß es die Mitarbeiter bemerkt haben.

Da die Beschwerden des Betroffenen sowohl bei seiner Beschäftigungsbehörde als auch beim FTA keinen Erfolg zeigten, wandte er sich an mich. Auf meine Aufforderung ist das FTA in eine umfangreiche technische und organisatorische Prüfung eingetreten, die noch nicht abgeschlossen ist.

2.2 Inneres

2.2.1 Verfassungsschutz

2.2.1.1 Erneute Behinderung der Datenschutzkontrolle

Aufgrund von Hinweisen vermutete ich, daß das Landesamt für Verfassungschutz (LfV) eine ihm vorliegende Liste mit personenbezogenen Informationen einer anderen öffentlichen Stelle übermittelt hatte. Ein Telefonanruf beim Leiter des LfV ergab keine Klärung der Frage. Deshalb wandte ich mich schriftlich an das LfV und bat um Mitteilung zu dem Vorgang, insbesondere auch um Bekanntgabe der Personen, die durch das Verfahren betroffen waren. Daraufhin teilte mir das LfV

u. a. mit: „Aus Gründen des nachrichtendienstlichen Quellenschutzes und der notwendigen Geheimhaltung ist es mir leider nicht möglich, Ihnen im einzelnen Namen zu nennen."

Mein Hinweis auf § 27 Abs. 3 BrDSG, wonach nur der Senator für Inneres selbst darüber entscheiden kann, ob die Staatswohlklausel zum Zuge komme, blieb unbeachtet. Ich bat deshalb den Senator für Inneres um Klärung. In einer Besprechung wurden die Rechtsauffassungen dargelegt. Der Senator für Inneres erklärte in dem Zusammenhang, das LfV habe mir angeboten, die Personenakten der betreffenden Personen einzusehen, eine grundsätzliche Weigerung des LfV zur Einsichtnahme in die Daten liege deshalb nicht vor.

Ich unternahm deshalb erneut den Versuch, an die Daten der Betroffenen zu gelangen. Zum angemeldeten Termin wurde mir zwar eine Anzahl von Akten vorgelegt, mir wurde aber untersagt, Aufzeichnungen zu fertigen. Dies sei ausdrückliche Anweisung des Amtsleiters, der zum Prüfungszeitpunkt nicht im Hause war. Ich prüfte zwar eine kleine Auswahl von Akten, gleichwohl machte ich deutlich, daß ich die Behinderung meiner Prüfung nicht hinnehmen werde. Bei meiner nächsten Prüfung beim LfV, bei der auch der Amtsleiter anwesend war, habe ich meine Rechtsauffassung noch einmal deutlich gemacht. Erst jetzt sah sich der Amtsleiter in der Lage, mir eine Liste mit den Namen der Betroffenen auszuhändigen, die mich nunmehr in die Lage versetzte, weitere Prüfungen vorzunehmen. Nur am Rande sei bemerkt, daß die Auflistung mit dem niedrigsten Geheimhaltungsgrad „VS-NfD" versehen war.

Ich habe den Fall zum Anlaß genommen, den Senator für Inneres darauf hinzuweisen, daß in der Art und Weise, wie ich an der Wahrnehmung meiner gesetzlichen Aufgaben behindert worden bin, ein Verstoß gegen die Vorschriften des Datenschutzes im Sinne von § 29 BrDSG liegt. Ich habe den Senator für Inneres um Stellungnahme gebeten, wie in Zukunft das mir vom Gesetzgeber eingeräumte Prüfrecht auch beim Verfassungsschutz sichergestellt werden kann.

2.2.1.2 Datenschutzkontrolle in NADIS

Bereits im 13. Jahresbericht (S. 12 ff.) hatte ich berichtet, daß mir der Zugang zu den Datensätzen verweigert wurde, die von anderen Verfassungsschutzämtern zu bremischen Datensätzen in NADIS gespeichert sind. Wie mir der Senator für Inneres zwischenzeitlich mitteilte, wurde die Problematik auf Initiative Bremens bei einer Tagung der Leiter der Verfassungsschutzbehörden erörtert. Der Kreis hat die Auffassung des LfV Bremen im Ergebnis nicht gestützt, denn man hat sich im Interesse des auskunftssuchenden oder beschwerdeführenden Bürgers darauf verständigt, den Datenschutzbeauftragten auf Anfrage mitzuteilen, ob solche Datensätze anderer NADIS-Teilnehmer vorliegen, und die jeweilige speichernde Stelle zu benennen.

2.2.1.3 Einsatz eines PC-Netzes beim Landesamt für Verfassungsschutz

Das Landesamt für Verfassungsschutz (LfV) plant, die vorhandenen NADIS-Terminals durch ein PC-Netz mit Verbindung an das NADIS-System zu ersetzen und hierin weitere Datenverarbeitungsfunktionen aufzunehmen. So ist geplant, die eigene Textverarbeitung und Tabellenkalkulation sowie ein Mail-Box-Verfahren zur Versendung von Dokumenten an die NADIS-Teilnehmer zu integrieren.

In meiner Stellungnahme zu dem ADV-Antrag habe ich zunächst darauf hingewiesen, daß die Anzahl der geplanten Rechner faktisch eine Aufstockung gegenüber der derzeitigen Rechnerausstattung darstellt. Hierzu wurde mir erklärt, daß durch die Integration der Textverarbeitung mehr PC-Arbeiten als bisher auszuführen seien. Daraufhin habe ich vorgeschlagen, nur für einen Teil der Rechner NADIS-Anschlüsse vorzusehen. Dieser Vorschlag ist aufgrund fehlender technischer Möglichkeiten nicht weiter verfolgt worden.

Hinsichtlich der Textverarbeitung und der Tabellenkalkulation ist mir versichert worden, daß diese nur zum Schreibdienst und zur eigenen Berichterstattung genutzt würden. Um eine darüberhinausgehende Datenverarbeitung zu verhindern und die erforderlichen technischen und organisatorischen Maßnahmen festzulegen, habe ich verlangt, vor dem Einsatz Regelungen zu den einzelnen Verarbeitungsvorgängen in einem Datenschutzkonzept zu treffen.

Bei der Umstellung eines Terminalverfahrens auf ein PC-Netz ist zu berücksichtigen, daß ein PC Möglichkeiten bietet, die die bisher eingesetzten „dummen

Terminals" nicht ermöglichen. Technisch ist es möglich, Daten aus dem Großrechner, der die NADIS-Daten zentral beim Bundesamt vorhält, auf die PC zu übertragen und weiter zu verarbeiten Diese Funktion würde eine nicht mehr kontrollierbare Datenverzweigung und -verkettung ermöglichen. Es sind daher Maßnahmen zu treffen, die diesen Transfer ausschließen. Die mir vom LfV dargelegten Maßnahmen lassen Zweifel an ihrer tatsächlichen technischen Eignung zu. Ich habe daher verlangt, vor Inbetriebnahme des Systems zu überprüfen, ob diese Maßnahmen tatsächlich greifen.

Eine besondere Problematik stellt der Einsatz des Mail-Box-Verfahrens dar. Dieses ELKOM (Elektronische Kommunikation) genannte System ist in das NADIS-Verfahren integriert. Die NADIS-Teilnehmer haben die Möglichkeit, hierüber Dokumente zu versenden, diese weiterzuleiten, aufzubewahren und auszuwerten. ELKOM ist bereits im September 1990 in Betrieb genommen worden. Erst anläßlich der Beantragung des PC-Netzes erhielt ich hiervon Kenntnis. Seiner Unterrichtungspflicht nach § 27 Abs. 4 BrDSG ist das LfV nicht nachgekommen. Die Verfassungsschutzbehörden messen diesem System keine datenschutzrechtliche Bedeutung zu, da sie davon ausgehen, daß die über ELKOM versandten Dokumente nicht den Dateibegriff erfüllen. Ich habe das LfV darauf hingewiesen, daß es nach § 2 Abs. 2 BrDSG nicht auf eine dateimäßige Datenverarbeitung ankommt, denn unstreitig werden mit ELKOM personenbezogene Daten verarbeitet. Die Frage, ob mit derartigen Mail-Box-Verfahren wie ELKOM Dateien im Sinne anderer datenschutzrechtlicher Bestimmungen erzeugt und verarbeitet werden, kann nach Bremer Rechtslage dahinstehen. Die Bestimmungen des Bremischen Datenschutzgesetzes waren anzuwenden. Eine abschließende Bewertung von ELKOM konnte ich noch nicht vornehmen. So ist z. B. noch nicht geklärt, wie § 5 Abs. 2 BrDSG Rechnung getragen werden kann.

Bereits in meinem 12. Jahresbericht hatte ich im Zusammenhang mit der Einführung des Polizeisystems ISA-Dezentral auf die Unterrichtungspflicht gemäß § 27 Abs. 4 hingewiesen. Der Datenschutzausschuß der Bremischen Bürgerschaft hat in seinem Bericht und Antrag zum 12. Jahresbericht festgestellt, daß er vom Senat erwarte, daß der Datenschutzbeauftragte bei Planungen zum Aufbau automatisierter Informationssysteme in gesetzeskonformer Weise beteiligt wird; eine Unterrichtung lediglich im ADV-Ausschuß sei in diesem Zusammenhang nicht ausreichend. Ich habe gegenüber dem Senator für Inneres festgestellt, daß diese erneute Nichtbeachtung des § 27 Abs. 4 BrDSG einen Verstoß gegen Datenschutzbestimmungen im Sinne von § 29 Abs. 1 BrDSG darstellt.

Der Ausschuß für ADV hat der beantragten Beschaffung zugestimmt unter der Bedingung, daß vor dem Einsatz noch offene Fragen mit mir geklärt werden und die Wirksamkeit der getroffenen technischen Maßnahmen überprüft wird.

2.2.1.4 Unvollständige Aufzeichnungen der Übermittlungen vom und an den Verfassungsschutz

Gemäß § 6 Abs. 3 Bremisches Verfassungsschutzgesetz (BremVerfSchG) ist das Landesamt für Verfassungsschutz (LfV) verpflichtet, bei allen Übermittlungen personenbezogener Informationen vom und an das LfV den Namen und die Anschrift des Betroffenen sowie den Hinweis auf den Anlaß der Übermittlung aufzuzeichnen. Diese Aufzeichnungen sind gesondert aufzubewahren, durch geeignete Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Aufzeichnung folgt, zu vernichten. Auf der Basis dieser Regelung habe ich eine Querschnittsüberprüfung beim LfV vornehmen wollen.

Die Aufzeichnungen werden beim LfV in nach Jahrgängen getrennten Ordnern aufbewahrt. Die übermittelnde bzw. empfangende sachbearbeitende Stelle füllt hierzu entsprechende Formulare aus, die in Ordnern in chronologischer Reihenfolge abgeheftet werden. Der Pflicht der gesonderten Aufbewahrung und zur besonderen Sicherung wird hinreichend genügt.

Zur Prüfung habe ich aus verschiedenen Ordnern die dort dokumentierten Übermittlungsfälle durchgesehen und nach unterschiedlichen Kriterien und Fragestellungen geprüft.

Dabei habe ich festgestellt, daß die vorgesehenen Formulare in vielen Fällen unvollständig ausgefüllt worden sind. Das hat zur Folge, daß in diesen Fällen meistens nicht mehr nachzuvollziehen war, aufgrund welchen Anlasses welche Übermittlungen erfolgten. Zu dieser Feststellung wäre es nötig gewesen, entweder über das Aktenzeichen oder, soweit für den Vorgang kein Aktenzeichen vorhanden war, über ein anderes Zuordnungskennzeichen eine direkte Verbindung zu

dem der Übermittlung zugrunde liegenden Vorgang herzustellen oder sonst in geeigneter Weise den Anlaß der Übermittlung zu dokumentieren. Dieser Eintrag fehlte aber in der Mehrzahl der Fälle. Darüber hinaus ist festzustellen, daß bei ca. 50 % der durchgesehenen Aufzeichnungsformulare fehlte, aufgrund welcher Aufgabenstellung nach § 3 BremVerfSchG die Übermittlung erfolgte, obwohl diese Rubrik im Formular vorgesehen ist.

Problemlos war die Zuordnung zu einem Vorgang nur in den Fällen, in denen für die betroffene Person ein NADIS-Eintrag vorlag. Dieses war allerdings nur bei etwa 15 % der zur Prüfung herangezogenen Fälle der Fall. Häufig war hier weder aus der Aufzeichnung noch aus der Aktenlage eindeutig feststellbar, aus welchem Anlaß die aufgezeichnete Übermittlung erfolgte. In den meisten Fällen traten vage Erklärungsversuche oder Hinweise auf routinemäßige Abfragen, die nicht aktenkundig werden, an die Stelle einer konkreten Benennung des Anlasses. Andererseits waren in den herangezogenen Akten auch Übermittlungsvorgänge eingetragen, die sich wiederum in den Aufzeichnungen nach § 6 Abs. 3 BremVerfSchG nicht wiederfanden.

Aufgrund dieser festgestellten Mängel war eine strukturelle Prüfung der vorgenommenen Übermittlungen nicht mehr in dem gewünschten Umfang möglich.

Als Fazit meiner Prüfung kann ich feststellen, daß die Dokumentationspflicht nach § 6 Abs. 3 BremVerfSchG vom LfV nicht hinreichend beachtet worden ist. Wenn ihr vollständig und nachvollziehbar nachgekommen wird, können die Aufzeichnungen wertvolle Unterstützung für eine Datenschutzprüfung und für datenschutzrechtliche Beratungen sein. Ich habe das Prüfergebnis dem Senator für Inneres mitgeteilt und gefordert, daß die Bestimmungen des § 6 BremVerfSchG eingehalten und die Dokumentationsunterlagen vollständig ausgefüllt werden.

Darüber hinaus hat die inhaltliche Prüfung der dokumentierten Fälle ergeben, daß in einigen Personenakten eine unzulässige Datenverarbeitung durch das LfV stattgefunden hat. Soweit diese Vorgänge nicht auf meine Anregung hin gelöscht wurden, habe ich dies gegenüber dem Senator für Inneres bemängelt.

2.2.1.5 Extremisten im öffentlichen Dienst

Das LfV Bremen meldet seit langem regelmäßig einmal im Jahr die nach seiner Einschätzung im öffentlichen Dienst beschäftigten Rechts- und Linksextremisten namentlich an das BfV. Die vom Senat in den Richtlinien über das Verfahren bei der Feststellung der Verfassungstreue im öffentlichen Dienst (BrAbl. 1977 Nr. 19 und BrAbl. 1983 Nr. 15) festgelegten Bewertungskriterien wurden dabei nicht berücksichtigt.

Um korrekte Daten zu übermitteln, wurde vorher zu jeder Person jährlich bei der Senatskommission für das Personalwesen (SKP) angefragt, bei welcher Dienststelle die Person zur Zeit beschäftigt ist und ob es zwischenzeitlich eine Beförderung gab. Die SKP lieferte prompt jeweils zu den Personen die neuesten Beschäftigtendaten an das LfV. In der von dem LfV an das BfV gelieferten Liste ist eine große Bandbreite des öffentlichen Dienstes vertreten: z. B. Krankenhauspersonal, Sozialarbeiter, Hochschullehrer.

Um mir einen Eindruck zu verschaffen, auf Grundlage welcher Erkenntnisse die Meldungen des LfV erfolgen, habe ich mir die Vorgänge betroffener Hochschullehrer zeigen lassen.

Während nach der Richtlinie des Senats zum „Verfahren bei Feststellung des Erfordernisses der Verfassungstreue von Bewerbern für den öffentlichen Dienst" Tatsachen, die in die Studienzeit fallen, oder die mehr als drei Jahre zurückliegen, grundsätzlich nicht berücksichtigt werden dürfen, fand hier alles Eingang, was über Jahre hin an Informationen angefallen war. Es störte das LfV auch nicht, wenn die letzte Eintragung mehr als fünf Jahre zurücklag. Während akribisch nachverfolgt wurde, ob sich etwa der Wohnsitz oder die Besoldungsgruppe geändert hatte, wurde scheinbar nicht geprüft, ob nicht die gesamte Personenakte zu löschen war.

Auch wenn die Personen nicht Mitglieder oder Funktionäre einer beobachteten Partei waren, sondern in nach Auffassung des Verfassungsschutzes von diesen beeinflussten Organisationen eine Funktion ausübten, reichte dies für den Verfassungsschutz aus, in der Person einen Extremisten im öffentlichen Dienst zu erkennen. Auch per se nicht gegen die freiheitlich demokratische Grundordnung

gerichtete Meinungsäußerungen dieser Personen wurden gesammelt und in den Akten zu den Personen abgelegt. Hier finden sich Erklärungen gegen das Pinochet-Regime in Chile wieder, Manifeste gegen die Neutronenbombe oder Aufrufe für das Russeltribunal, um einige Beispiele zu nennen.

Ohne behaupten zu wollen, daß es sich bei der Stichprobe um einen repräsentativen Querschnitt handelt, konnte ich immerhin erreichen, daß über die Hälfte der geprüften Personenakten vernichtet wurde — wohlgemerkt Akten, die nach meiner Auffassung bereits seit längerer Zeit hätten gelöscht werden müssen. Das LfV selbst erklärte mir, daß man noch für 1991 die Meldefälle radikal reduzieren wolle.

Das Bremische Verfassungsschutzgesetz trifft keine Regelungen zu Online-Verfahren und regelmäßigen Datenübermittlungen, so daß § 14 BrDSG Anwendung findet. Das Verfahren sieht vor, daß regelmäßig einmal im Jahr eine Meldung zu erfolgen hat. Eine regelmäßige Datenübermittlung im Sinne von § 14 Abs. 7 BrDSG liegt somit vor. Nach § 14 BrDSG sind regelmäßige Datenübermittlungen aber nur zulässig, soweit dies durch Bundes- oder Landesrecht bestimmt ist. Nach § 14 Abs. 2 BrDSG sind nur die Senatoren ermächtigt, für die Behörden und Einrichtungen ihres Geschäftsbereichs ein solches Verfahren durch Rechtsverordnung einzuführen. Eine Rechtsverordnung liegt nicht vor. Weiter hätte ein solches Verfahren nur eingerichtet werden dürfen, soweit dies unter Berücksichtigung des informationellen Selbstbestimmungsrechts des betroffenen Personenkreises und der Aufgaben der beteiligten Stellen angemessen ist. Meine stichprobenartigen Prüfungen derartiger Übermittlungen haben ergeben, daß auch diese Voraussetzungen nicht erfüllt sind. Schließlich hätte gem. § 14 Abs. 2 der Landesbeauftragte für den Datenschutz vorher beteiligt werden müssen. Auch dies ist zu keinem Zeitpunkt erfolgt. Auch die Beachtung von § 5 Abs. 2 BremVerfSchG steht in Frage. Die Übermittlung einer anonymisierten Statistik wurde scheinbar nicht in Erwägung gezogen.

Ich habe den Senator für Inneres aufgefordert, wegen der oben dargelegten Rechtslage das LfV anzuweisen, vorläufig keine weiteren personenbezogenen Meldungen an das BfV vorzunehmen. Darüber hinaus habe ich ihn aufgefordert, vor der Regelung eines Übermittlungsverfahrens zunächst zu prüfen, ob nicht mit den eingangs erwähnten Verfahrensrichtlinien des Senats eine ausreichende Grundlage geschaffen ist, Extremisten im öffentlichen Dienst zu begegnen.

2.2.2 Polizei

2.2.2.1 ISA-Dezentral

In den letzten Jahren hatte ich über die geplante Einführung des Verfahrens Informations-System-Anzeigen-Dezentral (ISA-D) bei der Polizei berichtet. Das Vorhaben, dieses Verfahren im Berichtsjahr in einigen ausgewählten Organisationseinheiten (z. B. Reviere) probeweise einzuführen, konnte bisher nicht realisiert werden.

Trotz meiner bereits in meinem 11. Jahresbericht (S. 54 ff.) dargestellten Bedenken gegen die Rechtmäßigkeit des Verfahrens habe ich die beim Senator für Inneres gebildete Projektgruppe bei der Ausgestaltung des Datenschutzkonzeptes beraten. Dabei konnte ich u. a. erreichen, daß

- die Aktivitäten des Systembetreuers dokumentiert werden;
- für den Fall des Systemausfalls besondere Vorkehrungen getroffen werden;
- Regularien zur Benutzerkontrolle präzise gefasst werden;
- die Berechtigungen zum Zugriff auf das Betriebssystem, den Rechner und die Netze präzisiert werden.

Zur Ausgestaltung der Zugriffs- und Benutzerkontrolle ist mir ein Magnetkartenverfahren vorgestellt worden, auf dem die einzugebende persönliche Identifikationsnummer (PIN) nicht gespeichert wird. Die Zuordnung von Karten-Nummer und PIN erfolgt auf dem Rechner. Somit ist bei Verlust der Karte gewährleistet, daß ohne Kenntnis der PIN diese für einen Dritten wertlos ist, da die PIN auch nicht mit technischen Mitteln ausforschbar ist. Ich habe diese Lösung unter der Voraussetzung akzeptiert, daß die von mir geforderten organisatorischen Maßnahmen getroffen werden.

Breiten Raum nahm die Frage ein, in welchem Umfang Zugriffe auf die integrierten Systeme — die Polizeiinformationssysteme des Bundes (INPOL) und Bremens (ISA), das Bremer Einwohnermelderegister, die Kfz.-Zulassungsdateien des Bundes

(ZEVIS) und der Stadt Bremen (FAZID) — zu protokollieren sind. Ich habe gefordert, eine einheitliche Protokolloberfläche für alle im ISA-D eingebundenen Systeme bereitzuhalten, damit ich in die Lage versetzt werde, zu kontrollieren, ob ISA-D den gesetzlichen Normen entsprechend genutzt wird. Hinsichtlich des Zugriffs auf die landesseitigen Informationssysteme wurden das Protokoll und die für Datenschutzzwecke auswertbaren Datenfelder festgelegt. Diese Protokolldaten werden für die Dauer eines Jahres im Rechenzentrum der bremischen Verwaltung (RbV) gespeichert und sind Mitarbeitern der Polizei nicht zugänglich. Sie werden ausschließlich zu Zwecken der Datenschutzkontrolle gespeichert und dürfen nicht für andere Zwecke verarbeitet werden. Innerhalb des RbV werden diese Daten durch die hauseigene Sicherheits-Software besonders geschützt.

Auch hinsichtlich des Anschlusses an die Bundessysteme ist eine entsprechende Protokollierung gem. § 6 BrDSG vorzusehen. Die Nutzung durch bremische Polizeidienststellen unterliegt den Bestimmungen des BrDSG und damit meiner Kontrolle. Als wirksames Kontrollinstrument kann dabei nur eine zusätzliche landesseitige Protokollierung angesehen werden, da ansonsten das Zusammenwirken von Anfragen aus Bundes- und Landessystemen nicht mehr nachvollziehbar ist. Nur eine gleichgeartete Protokollierung in allen Systemen, verbunden mit der Möglichkeit der technischen Verknüpfung aller Abfragen zu einer bestimmten Person, ermöglicht überhaupt erst eine wirkungsvolle Datenschutzkontrolle. Einer mühsamen Auswertung irgendwelcher Protokollausdrucke — etwa des Bundeskriminalamtes — und die Zusammenführung mit anderen Protokollen kann bei der Neukonzeption eines modernen und komfortablen Informationssystemes, wie es ISA-D einmal sein soll, nicht mehr vertreten werden. Von Seiten des Senators für Inneres wurde anerkannt, daß ein derartiges Verfahren für meine Kontrolltätigkeit sinnvoll ist; offen ist aber noch die Frage, wie dieses technisch zu realisieren ist.

Hingegen konnte bisher mit dem Senator für Inneres kein Konsens erzielt werden, ob auch der Grund, der zu dem Datenabruf aus dem Informationssystem führt, protokolliert werden muß.

Ich habe dem Senator für Inneres mehrfach dargelegt, daß die Protokollierung auch des Abfragegrundes unabdingbar für die Erfüllung meiner Aufgaben ist, die einzelnen Verarbeitungs- und Nutzungsvorgänge in einem derart komplexen System zu kontrollieren. Die Rechtmäßigkeit eines Datenabrufes kann nur dann geprüft werden, wenn bekannt ist, zu welchem Zweck die Daten verwendet werden sollen.

Prüferfahrungen, die ich in anderen Bereichen gewonnen habe, haben gezeigt, daß ohne hinreichende Protokollierung des Abfragegrundes Anlaß und Zweck des Abrufes häufig nicht mehr nachzuvollziehen sind, da diese weder aus der Aktenlage noch aus der Erinnerung des Abrufenden hervorgehen. Gerade bei der Nutzung von ISA-D gehe ich davon aus, daß eine Vielzahl von Abfragen sich nicht in Akten niederschlägt oder sonst dienstlich dokumentiert wird. In allen solchen Fällen ist deshalb der Abfragegrund festzustellen und festzuhalten.

Aufgrund von Eingaben, denen ich bisher nicht nachgehen konnte, weil die Vorwürfe der Bürger mangels Protokollierung nicht verifiziert werden konnten, kann nicht ausgeschlossen werden, daß — so jedenfalls die Bürger — von Polizeibeamten Abfragen aus den Informationssystemen für private Zwecke vorgenommen wurden. Wie auch in anderen Bereichen ist das Dunkelfeld mit den mir über die Jahre vorliegenden Eingaben nicht ausgeleuchtet. Aber es geht nicht nur um die Verhinderung mißbräuchlicher Datenverarbeitung sondern auch um die Kontrolle der rechtmäßigen Datenverarbeitung. Um diese Aufgabe wirksam wahrnehmen zu können, sind Revisionsinstrumente wie die Protokollierung des Abfragegrundes notwendig.

Der Senator für Inneres hält dem entgegen, die Angabe des Abfragegrundes sei deshalb nicht erfolgversprechend, weil diese Information zur Aufdeckung eines Mißbrauches ungeeignet sei, und daß jemand, der unzulässigerweise abrufen wolle, die Möglichkeit habe, einen entsprechenden Abfragegrund zu erfinden.

Diese Argumentation übersieht aber, daß dann, wenn der Abfragegrund vorliegt, eine Recherche über die Zulässigkeit der Abfrage wesentlich erleichtert wird, da durch zusätzliche Informationsquellen — wie z. B. Akten, Vorgangsregister, Wachbücher etc. insbesondere aber auch Angaben des Betroffenen — die tatsächlichen Verhältnisse, wenigstens aber die Plausibilität des Abfragegrundes überprüfbar sind. So läßt sich z. B. feststellen, ob ein Eintrag „Verkehrsüberprüfung"

richtig ist, weil recherchierbar ist, ob zu dem Zeitpunkt der Anfrage überhaupt Verkehrskontrollen durch den Abrufenden oder den Veranlasser durchgeführt worden sind und ob die Person, zu der Daten abgefragt worden sind, von einer solchen Überprüfung überhaupt betroffen sein konnte. Die Notwendigkeit einer Protokollierung des Abfragegrundes wird auch vom Gesetzgeber gesehen. So ist bei einem Übermittlungsersuchen die abfragende Stelle gem. § 30 Abs. 3 BremMeldG verpflichtet, den Anlaß der Übermittlung aufzuzeichnen.

Um meine Vorschläge in der Praxis zu überprüfen, habe ich mir zunächst in den zentralen Datenstationen des Polizeipräsidiums ein Bild darüber verschafft, aus welchen Gründen dort angefragt wird. Als Ergebnis ist festzustellen, daß — bezogen auf das jeweilige System — bestimmte gleichgeartete Abfragegründe überdurchschnittlich häufig auftreten (teilweise bis zu 90 % der Anfragen). Ich habe daher einen Vorschlag entwickelt, der Standardabfragen vorsieht, für die dann der entsprechende Abfragegrund systemseitig zugeordnet wird, sowie Regelabfragen, die per Katalog vorgegeben und vom Anwender angesteuert werden können. Damit verbleibt ein Eingabeaufwand nur noch in den wenigen Fällen, die vom Standard abweichen und für die kein Katalogeintrag vorgesehen ist. Nachdem ich diesen Vorschlag dem Senator für Inneres zugesandt habe, hat dieser sich bereit erklärt, in einem Gespräch eine praktikable Lösung herbeizuführen.

Bereits im 13. Jahresbericht (S. 21) habe ich dargestellt, daß die Datenbestände in ISA (alt) bereinigt und aktualisiert werden müssen. Ich habe vorgeschlagen, den Altbestand von ISA mit ADV-technischer Unterstützung nach Datenschutzschwerpunkten qualifiziert zu bereinigen. Es reicht nicht aus, wenn die Polizei hierzu auf ein „Löschfristenverfahren" hinweist. Dieses Verfahren hat in den meisten Fällen nicht automatisch die Löschung der Daten zur Folge, vielmehr muß zunächst der Vorgang manuell geprüft und ggf. durch zusätzliche Eingaben die Löschung bestätigt werden. Prüferfahrungen zeigen, daß dies in der Vergangenheit häufig unterblieben ist. Es ist aber sicherzustellen, daß ein derart breitgefächertes Verfahren, wie es ISA-D darstellt, mit der Zugriffsmöglichkeit für fast jeden Polizeibeamten, nur Daten enthält, deren Speicherung rechtmäßig und aktuell erforderlich ist.

2.2.2.2 Erkennungsdienst

Aufgrund meiner Prüfungen der Dateien des Erkennungsdienstes (ED) (vgl. 13. Jahresbericht S. 18 ff.) ist der Datenbestand in der ED-Hauptdatei von 106.000 auf 30.000 reduziert worden. Bei einer kursorischen Prüfung in der ED-Stelle im Berichtsjahr habe ich festgestellt, daß weiterhin Fälle gespeichert waren, deren Löschung mir bereits 1990 zugesichert worden war. Mittlerweile hat mir der Senator für Inneres bestätigt, daß nunmehr alle beanstandeten Fälle gelöscht worden seien. Ebenfalls bestätigt wurde mir, daß gleichzeitig mit den Löschungen aus der ED-Datei auch die Negative der Lichtbilder vernichtet worden seien.

Das von der ED-Stelle verwendete Formular zur Einordnung in die Lichtbildvorzeigekartei, das eine unzulässige Kategorisierung der Betroffenen vorsah, ist geändert worden. Nach mehreren Gesprächen konnte erreicht werden, daß die Einteilung nun nicht mehr von bestimmten Merkmalen des Täters (Homosexualität, Prostitution, etc.) abhängig gemacht wird, sondern die Tat und ihre Umstände zur Einordnung herangezogen werden. Das Formular wurde durch ein Hinweisblatt ergänzt, das dem Sachbearbeiter Hilfestellungen bei der korrekten Zuordnung bietet. Gleichzeitig soll auch die ED-Karteikarte entsprechend umgearbeitet werden. Außerdem sind für die Entnahme und Vernichtung von Lichtbildern neue präzisere Anweisungen getroffen worden.

Die ebenfalls von mir verlangte Feststellungsanordnung zu den in der ED-Stelle geführten Dateien liegt im Entwurf vor, konnte aber aufgrund personeller Veränderungen im Polizeipräsidium bisher noch nicht abschließend erörtert werden.

Trotz aller festzustellenden Verbesserungen gegenüber der Situation, die ich 1989/90 vorfand, ist eine strukturelle Neuordnung des Verfahrens der Einordnung in und besonders der Aussonderung aus den ED-Dateien von großer Bedeutung, da — auch nach Angabe der in der ED-Stelle Beschäftigten — ansonsten nicht auszuschließen ist, daß sich immer wieder Fälle in den ED-Dateien befinden, die entweder von vornherein nicht oder nicht mehr hier gespeichert sein dürften. Ich habe gegenüber dem Senator für Inneres und gegenüber der Deputation für Inneres entsprechendes gefordert und erwarte, daß spätestens mit Einführung der Technik im Zusammenhang mit ISA-D diese Forderung erfüllt wird.

2.2.2.3 Datenverarbeitung beim Staatsschutz in APIS/ISA

Um meiner Forderung gerecht zu werden, das für schwere Staatsschutzdelikte und terroristische Gewalttaten eingerichtete bundesweite Informationssystem APIS nicht mehr als Aktennachweissystem für alle Staatsschutzvorgänge zu nutzen, ist für die Staatsschutzabteilung des Polizeipräsidiums Bremen der Einsatz eines PC mit Zugriffsmöglichkeiten auf ISA beantragt worden.

Dabei sollen die Staatsschutzfälle gegenüber den übrigen ISA-Fällen abgeschottet werden. Meinen Datenschutzanforderungen soll Rechnung getragen werden. Hinsichtlich der technischen Ausstattung des PC hatte ich zunächst Bedenken wegen der umfangreich zur Verfügung gestellten Software-Leistungen. Nachdem mir aber das Rechenzentrum der bremischen Verwaltung dargelegt hat, daß aufgrund einer entsprechenden Installation die Mehrfunktionalität für den Anwender nicht nutzbar ist, habe ich diese zurückgestellt. Der PC wurde leider noch immer nicht beschafft und installiert. Mittlerweile liegen auch für Bremerhaven Pläne vor, das Staatsschutzkommissariat an diesem Verfahren partizipieren zu lassen.

2.2.2.4 Hooligan-Datei

Die gewalttätigen Ausschreitungen im Zusammenhang mit Fußball — und sonstigen Sportveranstaltungen haben die Polizei veranlaßt, darüber nachzudenken, welche präventiven und strafverfolgenden Maßnahmen geeignet sind, um dieser Entwicklung entgegenzuwirken. Die Innenministerkonferenz hat im Mai 1991 beschlossen, eine „Datei Gewalttäter Sport" einzuführen. Nach den bisherigen Planungen soll sie als automatisierte Verbunddatei zentral beim Bundeskriminalamt (BKA) geführt werden. Die Planung sieht vor, Personen, gegen die ein Ermittlungsverfahren im Zusammenhang mit Ausschreitungen bei Sportveranstaltungen eingeleitet wurde, gegen die ein Stadionverbot verhängt wurde, die mit Waffen oder ähnlichen Gegenständen angetroffen wurden oder die im Zusammenhang mit Sportveranstaltungen in Gewahrsam genommen wurden, zu speichern. Es sind folgende Datenfelder vorgesehen: Personalien, erkennungsdienstliche Behandlung oder Hinweis auf Bildaufzeichnungen, Zugehörigkeit zu bestimmten Störergruppen, Anlässe und Umstände, die zur Aufnahme in die Datei führten, Informationen über Reisewege, Antrefforte und Umstände der Überprüfungen im Zusammenhang mit Sportveranstaltungen.

Obwohl die Innenministerkonferenz bereits im Dezember 1990 vorgesehen hatte, die Datenschutzbeauftragten des Bundes und der Länder schon bei der Frage zu beteiligen, ob die Datei eingerichtet werden soll, wurde ich erst im April 1991 auf meine Nachfrage vom Senator für Inneres über die Beschlußlage der Innenministerkonferenz unterrichtet.

Ich verkenne nicht, daß die Gewalttätigkeiten im Zusammenhang mit Sportveranstaltungen stark eskalieren und z. T. eine erhebliche Gefährdung der öffentlichen Sicherheit darstellen. Es kann daher nicht Anliegen des Datenschutzes sein, Maßnahmen im rechtlich vorgegebenen Rahmen zu verhindern, die geeignet sind, die Sicherheit bei Sportveranstaltungen zu erhöhen.

In meiner vorläufigen Stellungnahme gegenüber dem Senator für Inneres habe ich auf folgendes hingewiesen:

- Zunächst ist die Rolle des BKA beim Aufbau der Datei zu klären, insbesondere ob und wie angesichts der geltenden Rechtslage BKA und BGS im Rahmen eines Online-Verfahrens auf die Datei Zugriff nehmen dürfen.

- Es bedarf einer Klärung, ob und unter welchen Voraussetzungen die beabsichtigten Datenübermittlungen an Veranstalter und Betreiber von Sportstätten in Betracht kommen. § 33 Abs. 2 BremPolG läßt die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen nur zur Abwehr einer (konkreten) Gefahr zu.

- Auch die Eignung der Datei „Gewalttäter Sport" für die angestrebten Zwecke ist für mich nicht nachvollziehbar. Bisher ist nicht dargelegt worden, daß die Datei auch Informationen liefert, die in den konkreten Situationen die Abwehr von Gefahren oder die Verfolgung von Straftaten ermöglichen. Die Polizei weist vielmehr selbst darauf hin, daß relevante Personen oft nicht mehr durch ihr Erscheinungsbild erkennbar sind und sich dadurch weitgehend polizeilicher Kontrolle entziehen können. Berücksichtigt man die vielen Möglichkeiten zu Sportveranstaltungen zu gelangen (Bus, Bahn, Pkw etc.), erscheint es auch schwierig, Personalienfeststellungen im weiteren Vorfeld von Sportveranstal-

tungen zu organisieren. Über die Leibesvisitation z. B. an den Stadiontoren hinausgehende Maßnahmen der Personalienfeststellung und der Abgleich aller Besucher der Sportveranstaltungen in der Datei „Gewalttäter Sport" erscheinen gerade bei Großveranstaltungen schwer durchführbar. In diesem Zusammenhang ist auch zu berücksichtigen, daß Personen- und Identitätsfeststellungen nur im Rahmen von § 11 BremPolG zulässig sind.

- Gegen Personen, die als Gewalttäter gespeichert sind, können keine anderen Maßnahmen ergriffen werden als gegen andere Personen. Wird aufgrund bestimmter Tatsachen das Vorliegen einer konkreten Gefahr angenommen, können seitens der Polizei Maßnahmen gegen den Störer ergriffen werden, unabhängig davon, ob er in der Datei gespeichert ist oder nicht.

- Schließlich ist § 14 Abs. 1 BrDSG zu berücksichtigen. Danach ist die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, nur zulässig, soweit dies durch Bundes- oder Landesrecht bestimmt ist.

Zwischenzeitlich hat sich im Zuge der Prüfung der Realisierung des Projekts auf seiten der Polizei gezeigt, daß es derzeit keine INPOL-Anwendung gibt, die den fachlichen Anforderungen der vorgesehenen Datei „Gewalttäter Sport" entspricht. Angesichts der vielen offenen Fragen im Zusammenhang mit dieser Datei hat auch die Konferenz der Datenschutzbeauftragten von einer Beschlußfassung abgesehen. Die Datenschutzbeauftragten des Bundes und der Länder werden sich im Detail zu dem geplanten Projekt äußern, soweit es zu einem Entwurf einer Errichtungsanordnung für die Datei kommen sollte.

2.2.2.5 Bremer Palästinenser auch lange nach dem Golfkrieg im Computer des Staatsschutzes gespeichert

Am 22. 01. 1991 erschienen in der lokalen Presse Berichte, u. a. mit der Überschrift „Vorladung beim Staatsschutz — Palästinenser empört und verunsichert". Darin wurde berichtet, daß rund 30 Palästinenser mit dem Formblatt zur Zeugenvernehmung „zu ihrer Vernehmung als Zeuge zu einem Gespräch wegen des Golfkrieges und der hierdurch zu erwartenden Terroranschläge in der BRD durch ‚Palästinensergruppen'" von der Abteilung Staatsschutz der Kriminalpolizei vorgeladen worden waren. Bei den Betroffenen handelt es sich z. B. um Geschäftsleute oder Arbeitnehmer, die z. T. bereits 10 Jahre und länger in der BRD leben.

Meine Nachforschungen beim Staatsschutz haben seinerzeit folgendes ergeben: Vor dem Hintergrund des Krieges am Golf und der sich immer deutlicher abzeichnenden Gefahr von Anschlägen terroristischer Gruppierungen aus dem Nahen Osten gegen Einrichtungen der Allianzkräfte auf dem Gebiet Deutschlands wurden bundesweit gezielt Personen der Volkszugehörigkeit „Palästinenser" überprüft und angesprochen. Ziel war es, deren mögliche Kooperation mit solchen Gruppierungen auszuschließen. Mir wurde erläutert, daß der Staatsschutz zur Vermeidung von Anschlägen aus präventiven Gesichtspunkten eine Gruppe von Palästinensern eingeladen habe, um sie — falls geplant — von solchen Vorhaben abzubringen.

Die in den Presseberichten geäußerte Mutmaßung, die Kripo habe sich die Daten aller in Bremen lebenden Palästinenser aus den Dateien der Ausländerbehörde abgerufen, fand ich nicht bestätigt.

Sowohl das Polizeipräsidium als auch der Senator für Inneres erklärten seinerzeit, daß in Bremen lebende Palästinenser aus Anlaß des Golfkrieges nicht in Dateien des Staatsschutzes gespeichert würden. Im übrigen hielt der Staatsschutz dieses aus polizeilicher Sicht auch nicht für erforderlich.

Eine Prüfung beim Staatsschutz konnte erst sehr spät durchgeführt werden, weil mir erst nach zähem Ringen die für die Prüfung erforderlichen Unterlagen zur Verfügung gestellt wurden. Bei meiner Prüfung mußte ich feststellen, daß aus Anlaß des Golfkrieges Bremer Palästinenser im Informationssystem des Staatsschutzes „APIS" gespeichert sind.

Der Bremer Staatsschutz macht andere für die Speicherung verantwortlich. Ich habe deshalb den Senator für Inneres aufgefordert, den Sachverhalt aufzuklären und sich für eine Löschung der Bremer Datensätze einzusetzen.

2.2.2.6 Datenübermittlung der Kriminalpolizei an das LfV

Die Kriminalpolizei Bremen — Abteilung Staatsschutz — übermittelte dem Landesamt für Verfassungsschutz (LfV) eine Liste mit Personen, die im Zusammenhang mit einer gewalttätigen Demonstration aufgefallen waren. Zu den Personen wurde vorher eine ISA-Anfrage gemacht und das Ergebnis zu jeder Person in der Liste vermerkt. Auf diese Weise erhielt das LfV Informationen über den Verdacht früherer Kfz-Diebstähle, Ladendiebstähle, Beförderungserschleichung und die Einstellung des Verfahrens als Bagatellsache u. a.. Einige Tatvorwürfe waren älter als fünf Jahre und hätten wegen der geringen Bedeutung bereits in USA gelöscht werden müssen.

Gemäß § 6 Abs. 1 Satz 2 BremVerfSchG darf der Staatsschutz von sich aus an den Verfassungsschutz alle ihm im Rahmen seiner Aufgaben vorliegenden Informationen über Bestrebungen übermitteln, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen im Sinne des § 3 Abs. 1 BremVerfSchG verfolgt werden.

In einigen Fällen ist zweifelhaft, ob die Personendaten überhaupt an das LfV übermittelt werden durften, denn es ist fraglich, ob die Voraussetzungen von § 3 Abs. 1 BremVerfSchG vorlagen. So lautete der Vorwurf gegenüber einer Person „Störer/Delikt zur Zeit noch nicht bekannt", weitere polizeiliche Erkenntnisse lagen nicht vor.

In jedem Fall waren die Ergebnisse der polizeilichen ISA-Anfrage zu den Personen dem LfV nicht mitzuteilen. Hierbei handelt es sich zwar um Informationen, die „der Polizei vorliegen". Bei den Taten in völlig anderem Sachzusammenhang handelt es sich aber nicht um Informationen über Bestrebungen im Sinne des § 3 Abs. 1 BremVerfSchG. Auch aus dem allgemeinen verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit ergibt sich, daß dem LfV nur die Informationen zuteil werden dürfen, die für die Aufgabenerfüllung des LfV erforderlich und geeignet sind. Hierzu zählen isolierte polizeiliche Erkenntnisse wie „Beförderungserschleichung" nicht. Bei der Übermittlung an das LfV wurden das informationelle Selbstbestimmungsrecht der Betroffenen und das Trennungsgebot zwischen Polizei und Verfassungsschutz nicht beachtet.

Ich habe den Senator für Inneres darauf hingewiesen, daß hierin ein Verstoß gegen § 6 Abs. 1 BremVerfSchG im Sinne von § 29 BrDSG liegt und ihn zur Stellungnahme aufgefordert.

2.2.3 Meldewesen

2.2.3.1 Meldedatenübermittlungsverordnung des Landes

Im Berichtsjahr wurde die Meldedatenübermittlungsverordnung des Landes erneut geändert. Bei dieser Änderung wurde der Katalog der Behörden, die Meldedaten im automatisierten Verfahren abrufen dürfen, wiederum ausgeweitet. Neu hinzugekommen sind die Führerscheinstelle Bremen, die Ausländerbehörden in Bremen und Bremerhaven, die Personalausweisbehörde Bremen und die Paßbehörde Bremen. Außerdem wurden einige Befristungen gestrichen mit der Folge, daß bisher nur befristet zugelassene regelmäßige Datenübermittlungen nunmehr auf Dauer zugelassen sind.

Ich hatte zu den Verordnungsentwürfen Stellung genommen und hatte Gelegenheit, meine kritischen Einwände in der Deputation für Inneres zu erläutern. Leider haben auch dieses Mal wieder die Vorstellungen und Wünsche der Verwaltung die Bedenken des Datenschutzes beiseite gedrängt. Das auf der Meldepflicht des Einwohners beruhende, in Bremen und Bremerhaven voll automatisierte Melderegister entwickelt sich zunehmend zu einem allgemeinen Informations- und Abgleichsregister für die gesamte Verwaltung, ohne daß der Gesetzgeber dies in den meldegesetzlichen Grundlagen explizit zugelassen hätte. In meinem 12. Jahresbericht hatte ich bereits auf diesen Sachverhalt hingewiesen, leider ohne Erfolg.

2.2.3.2 EDAS-/DEMOS-Verfahren in Bremen

Die Ablösung des technisch veralteten und nicht dem geltenden Melderecht entsprechenden EDAS-Verfahrens durch das neue DEMOS-Verfahren (Dezentrales Einwohner-Melde-Online-System) ist immer noch nicht erfolgt. Zur bisherigen Verzögerung von 3 Jahren ist ein weiteres Jahr hinzugekommen. Ich habe dieses Thema in früheren Tätigkeitsberichten ausführlich dargestellt; Senat und Bürgerschaft kennen die datenschutzrechtliche Problematik und haben sich mehrfach damit und mit der schleppenden Realisierung des Projektes befaßt.

Im Berichtsjahr habe ich mehrere Gespräche mit dem Innenressort und der DEMOS-Projektgruppe geführt. Ich habe in diesen Gesprächen deutlich gemacht, daß es mir darauf ankommt, die datenschutzrechtlichen Mängel des alten EDAS-Verfahrens schnellstmöglich zu beseitigen, sei es durch Nachbesserung am alten EDAS-Verfahren (insbesondere durch Stillegung rechtswidriger Online-Anschlüsse), sei es durch Einführung von Teilen oder des gesamten neuen DEMOS-Verfahrens. Da die gravierendsten Mängel des alten DV-Verfahrens im Bereich der Online-Übermittlungen liegen (Verstöße gegen § 5 der Bremischen Meldedatenübermittlungsverordnung), konzentrierten sich die Bemühungen der Verwaltung auf diesen Bereich. Im Berichtsjahr schlug das Innenressort vor, den DEMOS-Verfahrensteil Fremdnutzer früher als geplant zu realisieren und zusammen mit dem Teilverfahren Paß-/Ausweiswesen als erste DEMOS-Realisierungsstufe in den Meldestellen einzuführen. Als Zeitraum wurde die erste Hälfte 1992 genannt. Die Entwicklungsarbeiten an dieser DEMOS-Teillösung wurden im Berichtsjahr aufgenommen.

Ende März 1992 soll in einer Meldestelle (Pilotmeldestelle) das neue Paß-/Ausweisverfahren zusammen mit der EDAS-/DEMOS-Fremdnutzer-Schnittstelle eingeführt und von diesem Zeitpunkt an auch die ersten Online-Fremdnutzer-Anschlüsse umgestellt werden. Im Laufe des Jahres 1992 sollen nacheinander dann die weiteren Meldestellen an dieses Teilverfahren angeschlossen werden, so daß Ende 1992 alle Meldestellen in der Stadt Bremen einbezogen und alle Online-Anschlüsse an das bremische Melderegister umgestellt, d. h. der geltenden Melderechtslage angepaßt sein sollen. Weitere Verzögerungen sind allerdings zu befürchten, wenn der beabsichtigte Rechneraustausch beim Rechenzentrum der bremischen Verwaltung sich verschiebt (Asbestproblem, vgl. Ziffer 2.12.1).

2.2.3.3 Datenübermittlungen an politische Parteien

Im Vorfeld der Wahlen zur Bremischen Bürgerschaft, zur Stadtverordnetenversammlung Bremerhaven und zu den Beiräten in der Stadtgemeinde Bremen Ende September 1991 (Bürgerschaftswahl 1991) häuften sich bei mir Anfragen und Beschwerden von Wahlberechtigten, die direkt adressierte Zuschriften politischer Parteien erhalten hatten. Die Überprüfung des Sachverhalts bei den Meldebehörden ergab, daß sowohl die Meldebehörde Bremen als auch die Meldebehörde Bremerhaven Adreßdaten aus dem Melderegister an politische Parteien auf deren Anforderung hin übermittelt hatten und dies jeweils mit der Erlaubnisbestimmung im Bremischen Meldegesetz (§ 33 Abs. 1) begründeten.

Die **Meldebehörde Bremerhaven** übermittelte in Form von Adreßaufklebern die Angaben Familienname, Namensbestandteile, Rufname, Vorname, Straße und Hausnummer mit evtl. Zusatz

- an die CDU, Kreisverband Bremerhaven, Erstwähleradressen der Jahrgänge 1969 bis 1973,
- an die DVU, München, die Adressen der männlichen Erst- und Jungwähler, Jahrgänge 1966 bis 1973 sowie die Adressen älterer männlicher Wähler, Jahrgänge 1911 bis 1931,
- an die SPD, Unterbezirk Bremerhaven, Erstwähleradressen der Jahrgänge 1969 bis 1973 sowie in siebenfacher Ausfertigung sortiert nach Wahlbezirken und nach Straßen die Adressen aller Wahlberechtigten der Wahlbezirke zweier Ortsteile (Leherheide-West und Grünhöfe).

Die Adreßaufkleber wurden von Beauftragten der jeweiligen Parteien bei der Meldebehörde Bremerhaven innerhalb der zugelassenen Sechs-Monats-Frist abgeholt. In dem Begleitschreiben an die Parteien wurde ausdrücklich auf die Zweckbindungsbestimmung des Bremischen Meldegesetzes (§ 32 Abs. 4) hingewiesen, d. h. auf die Verpflichtung, die übermittelten Meldedaten nur für Zwecke der Bürgerschaftswahl 1991 zu verwenden.

Die **Meldebehörde Bremen** übermittelte in Form von Adreßaufklebern

- an die DVU, München, Erst- und Jungwähleradressen der Jahrgänge 1966 bis 1973 sowie die Adressen sogenannter Altwähler (60 Jahre und älter),
- an die SPD-Bürgerschaftsfraktion drei Sätze Erstwähleradressen der Jahrgänge 1969 bis 1973. Die SPD-Bürgerschaftsfraktion forderte die Adressen „im Auftrag der SPD-Landesorganisation Bremen" schriftlich an.

Die Adreßaufkleber wurden auch in Bremen von Beauftragten abgeholt. Ein Begleitschreiben mit Hinweis auf die Zweckbindungsbestimmungen des Bremischen Meldegesetzes wurde nicht übergeben.

Nach § 33 Abs. 1 Bremisches Meldegesetz darf die Meldebehörde Parteien und Wählergruppen im Zusammenhang mit allgemeinen Wahlen zu parlamentarischen und kommunalen Vertretungskörperschaften in den sechs der Wahl vorangehenden Monaten Auskunft aus dem Melderegister über Vor- und Familiennamen, akademische Grade und Anschriften von Wahlberechtigten erteilen, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist. Die Geburtstage selbst oder weitere Angaben dürfen dabei nicht übermittelt werden. Die übermittelten Adreßdaten dürfen nur für Wahlzwecke verwendet werden. Andere Zwecke, z. B. Mitgliederwerbung, Aktualisierung einer Mitglieder- oder Interessentenkartei, Werbung für Zeitschriften oder andere Produkte, Übermittlung an Parteimitglieder oder Dritte für deren Zwecke sind nicht zugelassen. Die Betroffenen können der Datenweitergabe widersprechen, wobei auf dieses Recht bei der Anmeldung und acht Monate vor der Wahl öffentlich hinzuweisen ist.

Die Art der Datenträger, auf denen die Adreßdaten übermittelt werden dürfen, ist nicht vorgeschrieben. Praktiziert wurde in diesem Fall wie bisher stets üblich die Erstellung und Weitergabe von Adreßaufklebern. Die Kontrolle der Einhaltung der Zweckbindungsbestimmung ist schwierig, vor allem dann, wenn die Daten an von einer Partei bezeichnete Stellen außerhalb Bremens übermittelt werden. Das ihnen zustehende Widerspruchsrecht ist den wenigsten Einwohnern bewußt. Jung- und Erstwähler rutschen, ohne ihr Recht wahrzunehmen, automatisch in diese Gruppe hinein und werden bei entsprechender Anforderung an die politischen Parteien und Wählergruppen übermittelt. Aus diesem Bereich kamen im übrigen die meisten Anfragen und Beschwerden. Die gesetzliche Regelung ist eine Erlaubnisbestimmung, d. h., die Meldebehörden sind nicht verpflichtet, an die politischen Parteien und Wählergruppen zu übermitteln. Sie müssen ihren Ermessensspielraum jedoch ermessensfehlerfrei und unter Beachtung des Gebots der Gleichbehandlung ausüben.

Die geprüften Übermittlungsvorgänge gaben zu folgender Kritik Anlaß:

- Die Praxis der Meldebehörden im Lande Bremen ist nicht einheitlich.
- Die Meldebehörde Bremerhaven übermittelte an die DVU Adreßdaten männlicher Wahlberechtigter und an die SPD in siebenfacher Ausfertigung die Adreßdaten aller Wahlberechtigten zweier ausgewählter Ortsteile, sortiert nach Wahlbezirken und innerhalb der Wahlbezirke nach Straßen. In beiden Fällen wurden wegen der speziellen Auswahl und Sortierung mehr Daten übermittelt, als nach dem Gesetzeswortlaut zulässig war. Beide Fälle verstießen gegen § 33 Abs. 1 Bremisches Meldegesetz.
- Die Meldebehörde Bremen akzeptierte ohne Nachfrage die Anschriftenanforderung der SPD-Bürgerschaftsfraktion im Auftrag der SPD-Landesorganisation. Nach dem Meldegesetz können nur Parteien und Wählergruppen, die an einer Wahl oder Abstimmung teilnehmen, derartiges Adreßmaterial erhalten, nicht Fraktionen. Deshalb wäre es erforderlich gewesen, daß die SPD-Landesorganisation bei der Meldebehörde die Erstwähleradressen anfordert. Anderenfalls wäre es Aufgabe der Meldebehörde Bremen gewesen zu überprüfen, ob die Voraussetzungen einer Auftragsdatenverarbeitung erfüllt waren.
- Keine der beiden Meldebehörden hat bei den Übermittlungsersuchen der Parteien bedacht, daß ein Zwang zur Übermittlung nicht besteht, weil § 33 Abs. 1 lediglich eine Erlaubnisregelung darstellt, die in das pflichtgemäße Ermessen der Meldebehörden gestellt ist. Das Einwohnermeldeamt der Stadt Aachen hat z. B. unter Berufung auf die zunehmenden Risiken für die schutzwürdigen Interessen der Betroffenen und ihr informationelles Selbstbestimmungsrecht es abgelehnt, an politische Parteien und Wählergruppen Adreßdaten überhaupt zu übermitteln. Das OVG Münster hat diese Entscheidung bestätigt: Die Verwaltung ist nicht gehindert, sich bei Ausübung ihres Ermessensspielraumes von Gesichtspunkten des Datenschutzes leiten zu lassen; der Gleichbehandlungsgrundsatz wird nicht verletzt, wenn der Entschluß für alle Parteien und Wählergruppen gleichermaßen gilt (Az.: 18 B 1630/89).

Den Parteien kommt eine besondere Stellung in unserer Demokratie zu. Wenn sich aber immer wieder eine große Zahl von Bürgern über die Adreßweitergabe für Wahlwerbung beschwert, ist zu prüfen, ob dem Anliegen dieser Bürger besser entsprochen werden kann. Insgesamt ergeben sich folgende Empfehlungen:

- Im Hinblick auf die zunehmenden Risiken für die schutzwürdigen Belange der Einwohner und ihr informationelles Selbstbestimmungsrecht sollte überprüft werden, ob die Regelungen des § 33 Abs. 1 Bremisches Meldegesetz noch sachgerecht sind. Wenigstens ist zu prüfen, ob die Widerspruchslösung in eine Zustimmungslösung umgewandelt werden sollte. Nur Daten derjenigen Wahlberechtigten dürften dann an Parteien und Wählergruppen übermittelt werden, die der Übermittlung ausdrücklich zugestimmt haben. Eine solche Regelung entspräche dem informationellen Selbstbestimmungsrecht der Einwohner mehr und könnte den vielen Beschwerden gegen die derzeitige Praxis Rechnung tragen.
- Die Frist für den Hinweis auf die Widerspruchsmöglichkeit bzw. künftig evtl. die Möglichkeit einer Zustimmungserklärung sollte verkürzt werden. Die Frist für die Datenübermittlung sollte ebenfalls reduziert werden. Die Fristensystematik insgesamt sollte an diejenige des Bremischen Wahlgesetzes bzw. des Bundeswahlgesetzes angeglichen werden. Die Übermittlung sollte nur an Parteien und Wählergruppen zugelassen werden, die tatsächlich an der Wahl oder Abstimmung teilnehmen.
- Wegen der besonderen Gefahren, die mit der Herausgabe elektronischer Datenträger verbunden sind, sollten nur Adreßaufkleber zugelassen werden. Dem Datenempfänger sollte neben der Zweckbindungsverpflichtung auch eine Datenlöschungsverpflichtung auferlegt werden (Löschung bzw. Vernichtung der übermittelten Daten bzw. Datenträger spätestens eine Woche nach dem Wahltermin). Verstöße gegen die Löschungsverpflichtung sollten in die Regelung über die Ordnungswidrigkeiten des Meldegesetzes einbezogen werden.
- Zur einheitlichen Durchführung dieser, evtl. auch anderer Übermittlungsbestimmungen sollte der Senator für Inneres Durchführungsbestimmungen erlassen. Darin sollten auch Kriterien für die Ausübung der in § 33 Abs. 1 BremMeldG vorgesehenen Ermessensentscheidung festgelegt werden.

2.2.3.4 Auskünfte aus dem Einwohnermelderegister

Im Zusammenhang mit der Bearbeitung einer Eingabe erfuhr ich von der Meldebehörde Bremen, daß die dortigen Mitarbeiter aufgrund einer vom Senator für Inneres erteilten Dienstanweisung gehalten seien, auch ohne nähere Angaben wie z. B. das Geburtsdatum oder die früher gemeldete Anschrift Auskünfte aus dem Einwohnermelderegister an Dritte zu erteilen, wenn der Name der Person, zu der um Auskunft gebeten wird, nur einmal im Einwohnermelderegister gespeichert ist. In verschiedenen Fällen ist es deshalb vorgekommen, daß über eine Person Auskunft erteilt wurde, zu der gar nicht angefragt wurde.

Der Senator für Inneres will an seiner aus dem Jahre 1989 stammenden Dienstanweisung aber festhalten, weil über den Namen hinausgehende Merkmale von Auskunftsuchenden vielfach nicht beigebracht werden können und bei der Melderegisterauskunft nach § 32 Abs. 1 BremMeldG nur wenige Grunddaten (Vor- und Familienname, akademische Grade, Anschriften) übermittelt werden.

Dem habe ich widersprochen. Gemäß § 32 Abs. 1 BremMeldG dürfen Daten nur übermittelt werden, wenn die Person, zu der um Auskunft gebeten wird, vom Auskunftsuchenden vor der Übermittlung bestimmt worden ist. Die Person, zu der angefragt wird, muß dermaßen konkret bestimmt sein, daß für die Meldebehörde Verwechslungen und darauf zurückzuführende Falschübermittlungen ausgeschlossen sind. Die beschriebene Praxis verstößt auch gegen § 7 BremMeldG, weil nicht ausgeschlossen werden kann, daß durch sie schutzwürdige Belange unbeteiligter Dritter beeinträchtigt werden.

2.2.4 Straßenverkehrsangelegenheiten

2.2.4.1 Aufbewahrungsfristen von Verkehrsordnungswidrigkeiten

Bereits in meinen letzten beiden Jahresberichten (S. 21 bzw. 23) hatte ich darüber berichtet, daß die Bußgeldakten in Straßenverkehrsangelegenheiten viel zu lange aufbewahrt werden. Inzwischen hat der Senator für Inneres erneut den Entwurf eines Erlasses über die Aufbewahrungsfristen vorgelegt. Auch dieser Entwurf enthält Aufbewahrungszeiten, die insbesondere über die gesetzlich festgelegten Tilgungsfristen im Straßenverkehrszentralregister hinausgehen. Insbesondere ist vorgesehen, Bußgeldentscheidungen einschließlich der damit zusammenhängenden Vollstreckungsunterlagen fünf Jahre aufzubewahren. Nachdem jahrelang argumentiert wurde, dies werde auch in anderen Ländern so gemacht, im übrigen

handele es sich um einen zu hohen Verwaltungsaufwand, habe ich mich bei Datenschutzbeauftragten anderer Länder nach der dort geübten Praxis erkundigt. Viele unterstützen meine Rechtsauffassung und erklärten mir, in ihrem Land würden die Tilgungsfristen als Löschfristen eingehalten.

Damit konfrontiert verlagerte die Straßenverkehrsbehörde die Argumentation und erklärte, die über die Tilgungsfristen hinausgehende Aufbewahrung der Vorgänge verlange der Rechnungshof zur Gewährleistung seiner Rechnungsprüfungskompetenz. Außerdem ergebe sich aus den Verwaltungsvorschriften zu § 71 Landeshaushaltsordnung (VV-LHO) eine Aufbewahrungsfrist von fünf Jahren für rechnungsbegründende Unterlagen, zu denen nach Auffassung des Rechnungshofes auch die kompletten Bußgeldakten gehörten. Der Senator für Inneres sehe sich daher außerstande, ohne Beachtung der Vorgaben des Rechnungshofs kürzere und insbesondere den gesetzlichen Tilgungsfristen entsprechende Aufbewahrungsfristen für die Bußgeldakten festzulegen. Meine Überlegungen hierzu habe ich unter Pkt. 2.11.1 des Berichts dargestellt.

2.2.4.2 Fehlen von Datenschutzregelungen im Fahrlehrergesetz

Nach der Verwaltungsvorschrift zum Fahrlehrergesetz hat die Erlaubnisbehörde die Inhaber der Fahrlehrerlaubnis unter laufender Nummer in ein Fahrlehrerverzeichnis einzutragen, sowie das Ruhen oder Erlöschen, die Rücknahme oder den Widerruf der Fahrerlaubnis im Fahrlehrerverzeichnis zu vermerken. Darüber hinaus hat die zuständige Verwaltungsbehörde der Erlaubnisbehörde die Entziehung der Fahrerlaubnis und Fahrverbote mitzuteilen. Außerdem sieht diese Verwaltungsvorschrift vor, daß sich die für allgemeine Fahrerlaubnisse zuständige Behörde und die für Fahrlehrerlaubnisse zuständige Behörde gegenseitig die Rücknahme oder den Widerruf der jeweiligen Fahrerlaubnis mitteilen, wenn der Betroffene eine allgemeine Fahrerlaubnis und eine Fahrlehrerlaubnis besitzt.

Ich habe gegenüber dem Senator für Inneres dargelegt, daß die Verarbeitung personenbezogener Daten der Fahrlehrer und Inhaber von Fahrschulen nur auf gesetzlicher Grundlage erlaubt ist; Verwaltungsvorschriften reichen hierzu nicht aus. Daher habe ich die senatorische Dienststelle gebeten, sich auf Bundesebene dafür einzusetzen, das Fahrlehrergesetz mit bereichsspezifischen Datenverarbeitungsregelungen zu ergänzen. Der Senator für Inneres teilt meine Auffassung und wird die Problematik im Bund-Länder-Fachausschuß „Fahrlehrerrecht" erörtern.

2.2.4.3 Aufbewahrung von Führerscheinakten

Bürger haben sich dagegen gewandt, daß die Führerscheinstellen die Führerscheinakten (Fahrerlaubnisse und Fahrerlaubnisse zur Fahrgastbeförderung) fünf bzw. zehn Jahre aufbewahren, obwohl die ausgehändigten Führerscheine nach Abschluß des Verwaltungsverfahrens zur Erteilung einer Fahrerlaubnis nach § 10 Abs. 2 Straßenverkehrszulassungsordnung (StVZO) in die Führerscheinkartei eingetragen werden.

Der Senator für Inneres will die Führerscheinstellen in Bremen und Bremerhaven anweisen, nach Erteilung der Fahrerlaubnisse und Eintragung in die Führerscheinkartei die Führerscheinakten zu vernichten. Lediglich in den Verfahren, in denen Anträge auf Erteilung einer Fahrerlaubnis insbesondere wegen Eintragungen in das Straßenverkehrszentralregister abgelehnt worden sind, sollen die Akten bis zur Tilgung dieser Eintragungen aus dem Verkehrszentralregister aufbewahrt werden.

2.2.4.4 Mitteilung eines Fahrverbotes an die örtliche Polizei

Auf Anfrage hat mir der Senator für Inneres mitgeteilt, daß die Bußgeldstelle in Bremerhaven die örtliche Polizei über angeordnete Fahrverbote unterrichtet; Rechtsgrundlagen hierfür bestehen nicht. Eine Mitteilung über ein verhängtes Fahrverbot an die örtliche Polizei durch die Führerscheinstelle wird nur in Bremerhaven vorgenommen. Eine solche Mitteilung in Bremerhaven hält der Senator für Inneres für die Durchsetzung des Fahrverbotes für notwendig. Durch Verwahrung des Führerscheins nach § 25 Abs. 2 StVG könne nicht sichergestellt werden, daß das Fahrverbot tatsächlich beachtet wird. Der Betroffene könne nach der Ablieferung des Führerscheins zum Zwecke der Verwahrung auf Antrag einen Ersatzführerschein erhalten, wenn die Fahrerlaubnisbehörde von dem Fahrverbot keine Kenntnis erlangt. Diese Mitteilung sei im Gegensatz zu Bremen

lediglich in Bremerhaven wegen der örtlichen Überschaubarkeit geeignet, die eventuelle Begehung einer Straftat (Fahren entgegen einem Fahrverbot) zu verhindern.

Ich habe dem Senator für Inneres dargelegt, daß dieses Ziel diese Maßnahme nicht rechtfertigt, da es sich dabei ausschließlich um eine Präventivmaßnahme handelt, für die nach den allgemeinen Grundsätzen der Gefahrenabwehr keine Rechtsgrundlage besteht. Im übrigen müssen die Täter bei der Begehung weiterer Straftaten bzw. Ordnungswidrigkeiten damit rechnen, aufgrund der dann erfolgenden Mitteilungen aus dem Verkehrszentralregister beim „Erschleichen" eines Ersatzführerscheins entdeckt zu werden. Dieser Fall ist jedoch so gut wie ausgeschlossen, weil auch anläßlich eines Antrages auf Erteilen eines Ersatzführerscheins eine Auskunft aus dem Verkehrszentralregister eingeholt wird.

Der Senator für Inneres will an der Praxis in Bremerhaven festhalten.

2.2.4.5 Verwertungsverbot bei Ermittlungen über die Eignung zum Führen von Kraftfahrzeugen

Die Führerscheinstelle Bremerhaven hat in mehreren Fällen im Rahmen der Prüfung, ob eine Fahrerlaubnis nach erfolgter Entziehung neu zu erteilen ist, in den Akten enthaltene zum Teil bis zu 30 Jahre zurückliegende Vorgänge herangezogen, obwohl diese Vorgänge schon lange aus dem Verkehrszentralregister getilgt worden sind. Begründet wurde die Verwertung mit § 52 Abs. 2 Bundeszentralregistergesetz (BZRG), wonach eine frühere Tat in einem Verfahren zur Erteilung oder Entziehung einer Fahrerlaubnis auch dann berücksichtigt werden darf, wenn die Verurteilung wegen dieser Tat bereits im Verkehrszentralregister getilgt worden ist.

Diese Rechtsvorschrift ist unter Berücksichtigung des Volkszählungsurteils des Bundesverfassungsgerichts als nicht mehr verhältnismäßig anzusehen. Aus diesem Grunde hat der Bundesminister der Justiz einen Referentenentwurf zur Änderung des Bundeszentralregistergesetzes erarbeitet. Danach ist beabsichtigt, diese Vorschrift dahingehend zu fassen, daß eine frühere Tat in einem Verfahren zur Erteilung oder Entziehung einer Fahrerlaubnis berücksichtigt werden darf, solange die Verurteilung wegen dieser Tat im Verkehrszentralregister eingetragen ist. Begründet wird diese Änderung damit, daß die derzeit geltende Regelung eine zeitlich unbegrenzte Berücksichtigung einer solchen Tat ermöglicht, obwohl eine solche unbegrenzte Verwertbarkeit nicht zwingend geboten ist. Die eingangs beschriebene Praxis verstößt nach meiner Auffassung auch gegen den Rehabilitationsgedanken.

Inzwischen hat mir der Senator für Inneres zugesagt, daß er bei der Auslegung des § 52 Abs. 2 BZRG das informationelle Selbstbestimmungsrecht und die neuere Rechtsentwicklung berücksichtigen will.

2.2.5 Ausländerangelegenheiten

2.2.5.1 Direktanschluß an das Ausländerzentralregister

Mit diesem Thema habe ich mich bereits in den letzten Jahren befaßt (siehe jeweils S. 27 des 12. und 13. Jahresberichts). Der Senat hat meiner Rechtsauffassung, daß es zum Anschluß des Ausländeramtes an das Ausländerzentralregister (AZR) beim Bundesverwaltungsamt einer entsprechenden Rechtsvorschrift bedarf, in seiner Stellungnahme vom 2. Juli 1991 zu meinem 13. Jahresbericht ausdrücklich zugestimmt und die Inbetriebnahme eines automatisierten Auskunftsverfahrens zum Ausländerzentralregister von der erforderlichen Rechtsgrundlage im Ausländerzentralregistergesetz abhängig gemacht.

Entgegen dieser Aussage hat der Senat am 6. August 1991 beschlossen, das Ausländeramt unverzüglich an das AZR anzuschließen und die erforderlichen Haushaltsmittel zur Verfügung zu stellen. Von diesem Senatsbeschluß erhielt ich erst wenige Tage vor der Einrichtung des Anschlusses im September 1991 Kenntnis.

Die erforderlichen Rechtsnormen fehlen nach wie vor. Das gesamte online-Abrufverfahren ist rechtswidrig.

2.2.5.2 Verwaltungsvorschriften zum neuen Ausländergesetz

Seit neun Monaten liegt mir der Entwurf von Verwaltungsvorschriften zu dem vor einem Jahr in Kraft getretenen Ausländergesetz (sog. Anwendungshinweise) vor.

In diesem Entwurf hat der Bundesminister des Inneren meine Anregungen und kritischen Anmerkungen zum Ausländergesetz in vielfältiger Form aufgenommen. So hat er u.a. konkretisiert, welche öffentlichen Stellen übermittlungspflichtig sind, welche Daten im einzelnen übermittelt werden dürfen und welche Daten die Ausländerbehörden verwerten dürfen. Wenn auch nicht alle meine Vorstellungen — wie z. B. die Datenübermittlungen von der Polizei und den Sozialbehörden an die Ausländerbehörden — realisiert werden konnten, so stellt dieser Entwurf eine deutliche datenschutzrechtliche Verbesserung dar. Ich habe jedoch Bedenken, ob die Verwaltungsvorschriften praktikabel sein werden, denn allein die Vorschriften zu den §§ 75 und 76 Ausländergesetz, die die Datenverarbeitung betreffen, umfassen zur Zeit 40 Schreibmaschinenseiten.

2.2.5.3 Erkennungsdienstliche Behandlung von Ausländern

Die Innenministerkonferenz hat im Mai 1991 die Einführung eines automatisierten Fingerabdruckidentifizierungssystems — AFIS — beschlossen. Es soll die Auswertung der Fingerabdrücke automatisieren und wesentlich vereinfachen. Begründet wurde die Notwendigkeit des AFIS neben der Einbeziehung der fünf neuen Bundesländer in das Auswertungsverfahren des Bundeskriminalamtes u. a. mit der Erfassung des erkennungsdienstlichen Materials aller Asylantragsteller. Durch diesen Beschluß erhielt ich erstmals von dem Erfassungsverfahren Kenntnis, das nunmehr durch das neue System fortgeführt und technisch verfeinert werden soll.

Nach meinen Feststellungen wurden entgegen den Vorschriften des Ausländergesetzes und des Asylverfahrensgesetzes alle Asylantragsteller ohne Ausnahme (sogar Kinder) erkennungsdienstlich behandelt, indem von allen zehn Fingern Abdrücke genommen werden und diese Daten — wie die von Straftätern — im Informationssytem der Polizei (INPOL) beim Bundeskriminalamt gespeichert werden.

Die geltenden Gesetze erlauben die erkennungsdienstliche Behandlung von Asylbewerbern nur, wenn Zweifel an ihrer Identität bestehen. Dieses kann nur in Ausnahmefällen zutreffen, wenn die Personaldokumente des Asylantragstellers erkennbar gefälscht oder verfälscht sind oder nicht vorliegen, sowie wenn im Einzelfall besondere Gründe für Zweifel an der Identität vorliegen.

Insoweit hat der Senator für Inneres im November 1991 die Unverhältnismäßigkeit des von der Ausländerbehörde durchgeführten Fingerabdruckverfahrens anerkannt und eine kurzfristige Änderung zugesagt. Ich habe allerdings noch keine Kenntnis davon, ob und wann die vielen zu Unrecht erhobenen und in INPOL gespeicherten Fingerabdruckdaten gelöscht werden.

Davon unberührt bleibt meine Kritik an dem Umfang und der Abwicklung der erkennungsdienstlichen Maßnahmen. Die Abnahme der Abdrücke aller zehn Finger ist nur bei Straftätern (sog. Spurenlegern) sinnvoll, weil am Tatort von der Polizei in der Regel nicht alle, sondern nur einzelne Fingerabdrücke sichergestellt werden. Für die Identitätsfeststellung hingegen genügt der Abdruck eines Fingers, um eine Person sicher identifizieren zu können. Würde man sich darauf beschränken, könnte nicht nur der Auswertungsaufwand beim Bundeskriminalamt reduziert werden, sondern es könnte auch der Eindruck vermieden werden, daß die Daten von Ausländern prinzipiell für Zwecke der Strafverfolgung vorgehalten werden. Eine solche Vorratsspeicherung ist ohne entsprechende Rechtsgrundlage ohnehin rechtswidrig.

Meine Hauptbedenken richten sich gegen die Auswertung der Fingerabdrücke durch das Bundeskriminalamt und die Speicherung aller Auswertungsergebnisse mit Namen der Betroffenen im Informationssystem der Polizei (INPOL). Damit stehen diese Daten im Zugriff aller Polizeidienststellen. Die Fingerabdruckblätter über Asylbewerber und die verformelt gespeicherten Fingerabdrücke werden beim BKA gemeinsam mit den Daten über Straftäter gespeichert. Diese Praxis steht im Widerspruch zu dem Beschluß der Innenministerkonferenz vom 29. 06. 1990, wonach erkennungsdienstliche Unterlagen über Asylantragsteller nicht mit den beim BKA zu anderen Zwecken gewonnen ED-Unterlagen zusammengeführt und nicht für andere Zwecke ausgewertet werden dürfen, soweit dafür eine gesetzliche Grundlage fehlt.

Eine völlig neue Qualität mit weitreichenden datenschutzrechtlichen Konsequenzen wird die geplante Einführung des automatisierten Fingerabdruckinformationssystems „AFIS" haben. Ohne zusätzliche manuelle Tätigkeit werden alle beim BKA gespeicherten Fingerabdrücke dann in automatisierter Form voll recherchierfähig sein.

Das Recht auf informationelle Selbstbestimmung gilt grundsätzlich auch für Ausländer uneingeschränkt. Schon das bisherige Verfahren verstößt gegen den vom Bundesverfassungsgericht festgestellten Grundsatz, daß angesichts der Gefahren der automatischen Datenverarbeitung ein amtshilfefester Schutz gegen Zweckentfremdung durch Weitergabe und Verwertungsverbote erforderlich ist. Dies kann nur gewährleistet werden, wenn die Ausländerdaten nicht durch das BKA, sondern durch die Ausländerbehörden geführt werden. Nur so ist eine strikte Zweckbindung der Daten zu gewährleisten.

Die Übertragung der Aufgabe der Auswertung des ED-Materials und der Speicherung in INPOL verstößt gegen Art. 87 Abs. 1 GG sowie gegen §§ 1 und 2 BKA-Gesetz. Die Vorschriften gestatten dem Bund nur die Einrichtung einer Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen, die kriminalpolizeiliche Aufgaben hat. Die Speicherung, Auswertung und Nutzung der nach ausländerrechtlichen Bestimmungen erhobenen Daten durch das BKA und das Bereithalten zum Abruf für die Polizeibehörden des Bundes und der Länder ist deshalb nur in den Fällen zulässig, in denen hinreichende Anhaltspunkte dafür bestehen, daß der einzelne Ausländer tatsächlich gegen Strafbestimmungen verstoßen hat. Die Speicherung aller Asylbewerber in der INPOL-Datei - eine Datei, in der Kriminelle mit schweren Straftaten und überregionaler Begehungsweise gespeichert sind und die der zentralen Verbrechensbekämpfung zu dienen hat — stellt eine Stigmatisierung aller Ausländer dar und rückt sie in die Nähe von Kriminellen.

Bei entsprechender Rechtsgrundlage wäre die Speicherung der Formel im AZR-Bestand denkbar und stände dann ausschließlich den Ausländerbehörden für erforderliche Identifizierungszwecke zur Verfügung. Eine Datenpflege, insbesondere die Löschung von nicht mehr erforderlichen Daten, würde dieses Verfahren erleichtern und beschleunigen. Bei dem jetzigen Verfahren habe ich Zweifel, ob die Fingerabdruckdaten im INPOL immer zeitgleich mit der Asylakte gelöscht werden.

Ich habe den Senator für Inneres im August 1991 über die datenschutzrechtlichen Probleme unterrichtet und ihn um Stellungnahme gebeten und angeregt, meine Überlegungen zu dem Verfahren auch in die Innenministerkonferenz zu tragen. Der Senator für Inneres hat daraufhin im November 1991 erklärt, er teile meine Auffassung, daß die gegenwärtige Handhabung der erkennungsdienstlichen Behandlung von Asylbewerbern zweifelhaft sei, er wolle meine Überlegungen bei Beratungen in Fachgremien mit einbeziehen. Ergebnisse liegen mir nicht vor.

2.2.5.4 Entwurf eines neuen Asylverfahrensgesetzes

Der Bundesminister des Inneren hat Ende November 1991 den Arbeitsentwurf eines Gesetzes zur Neuregelung des Asylverfahrens vorgelegt und den Innenministern u. -senatoren der Länder zur Mitberatung übersandt. Dieser Enwurf wurde zwischenzeitlich in den Deutschen Bundestag eingebracht.

Der Entwurf wirft grundsätzliche Fragen zur Datenerhebung, -übermittlung und -löschung auf. Im Gegensatz zu meinen Kollegen wurde ich über diesen Entwurf erst Mitte Januar 1992 in Kenntnis gesetzt. Eine frühzeitige Unterrichtung wäre notwendig gewesen.

Meine Bedenken richten sich gegen folgendes:

— Der Enwurf enthält generalklauselartige Normen zur Datenerhebung, obwohl präzise formulierte und am Verhältnismäßigkeitsgrundsatz orientierte Erhebungsvorschriften nötig wären.

  So erlaubt z. B. § 7 des Entwurfs, daß die mit der Ausführung des Gesetzes betrauten Behörden zum Zwecke der Ausführung des Gesetzes personenbezogene Daten erheben dürfen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Nach den in § 8 des Entwurfs formulierten Übermittlungsregelungen haben öffentliche Stellen auf Ersuchen den mit der Ausführung dieses Gesetzes betrauten Behörden ihnen bekannt gewordene Umstände mitzuteilen, soweit nicht besondere Verwendungsregelungen entgegenstehen.

  Nach diesen Vorschriften würden allein die Asylbehörden bestimmen, welche Daten sie für ihre Aufgabenerfüllung benötigen, welche sie anfordern dürfen und wie sie sie nutzen. Die Rechtsvorschrift muß präzise und normenklar die zu übermittelnden Daten und die übermittlungspflichtigen öffentlichen Stellen benennen. Darüber hinaus ist der in § 8 des Entwurfs verwendete Begriff „Umstände" vollkommen unpräzise und bedarf der Klarstellung. Solche un-

klaren Regelungen haben bereits beim Ausländergesetz zu erheblichen Auslegungsschwierigkeiten geführt, diese Entwicklung kann ich für dieses Gesetz ebenfalls voraussagen, wenn die Normen nicht präzisiert werden.

- Der Entwurf verzichtet auf eine eigenständige klare Speicherungsvorschrift sowohl für das Bundesamt für Flüchtlinge, als auch für die mit der Ausführung des Asylrechts beauftragten Ausländerbehörden. Dieses kann nicht hingenommen werden. Sowohl für die konventionelle Aktenführung als auch für die zunehmend automatisierte Aktenführung sind Festlegungen über die Datenverarbeitung unverzichtbar.

- Die vorgesehene Regelung im Entwurf über die erkennungsdienstliche Behandlung aller Asylantragsteller ist unverhältnismäßig. Danach sollen zukünftig auch erkennungsdienstliche Maßnahmen durchgeführt werden, wenn einwandfreie Dokumente vorgelegt werden oder auch wenn es sich um ein kleines Kind handelt. Ich halte die jetzige Regelung, die eine erkennungsdienstliche Behandlung von Asylantragstellern nur zuläßt, wenn Zweifel an der Identität bestehen, weil z. B. keine Dokumente vorgelegt werden oder diese offensichtlich gefälscht oder verfälscht sind, für ausreichend.

- Der Entwurf sieht die Auswertung und Speicherung bzw. Nutzung des erkennungsdienstlichen Materials durch das Bundeskriminalamt vor. Die Fingerabdruckdaten sollen vom BKA ausgewertet und im Informationssytem Polizei INPOL gespeichert werden. Damit wird die Nutzung dieser Daten durch alle angeschlossenen Polizeidienststellen ermöglicht. Durch dieses Verfahren werden die Asylantragsteller in die Nähe von Kriminellen gerückt. (vgl. auch Pkt. 2.2.5.3 des Berichts)

2.2.6 Feuerwehrangelegenheiten

2.2.6.1 Neue Einsatzleitzentrale der Feuerwehr

Aufgrund des Bremischen Brandschutzgesetzes vom 07. 05. 1991 ist die Berufsfeuerwehr im Lande Bremen u. a. verantwortlich für Brandschutz, technische Hilfeleistung, Rettungsdienst und Katastrophenschutz.

Zur Lenkung und Koordination entsprechender Einsätze schreibt dieses Gesetz (§ 2 Abs. 2) die Einrichtung einer Einsatzleitzentrale und Rettungsdienstleitstelle vor.

Für den Bereich der Einsatzleitzentrale wird die Ausstattung der Feuerwehr Bremen mit neuer Kommunikationstechnik und einem Einsatzleitrechner angestrebt. Grundlage ist ein Vernetzungskonzept, das im Rahmen eines lokalen Netzwerkes (LAN) in der Einsatzleitzentrale die Verbindung sowohl der Arbeitsplatzrechner untereinander als auch mit dem Einsatzleitrechner vorsieht. Die abgesetzten Arbeitsplätze der Berufsfeuerwehrwachen, der Notarztwagenstation und der Stationen der Hilfsorganisationen werden über ein Wide-Area-Network (WAN) mit dem Einsatzleitrechner verbunden. Als Trägersystem ist ein X.25-Netzwerk vorgesehen.

Ich habe das Projekt Einsatzleitsystem Berufsfeuerwehr Bremen im Berichtsjahr in der Planungsphase begleitet. Die normenklare Aufgabenbeschreibung und die sich daraus ergebenden bereichsspezifischen Datenschutzregelungen im Bremischen Brandschutzgesetz (vgl. 13. Jahresbericht, S. 27) haben eine klare Definition der zur Aufgabenerfüllung der Einsatzleitzentrale notwendigen zweckgebundenen Informationen und der sich daraus ergebenden Datenschutzmaßnahmen ermöglicht. Diese sind zum Teil in das Feinkonzept integriert und werden in die technische Realisierung einfließen.

Das mir am Ende des Berichtsjahres vorgelegte Feinkonzept beschränkt sich zunächst auf folgende Bereiche: Einsatzlenkung mit Bettennachweis, Berichtswesen für Brand- und Hilfeleistungen sowie den Rettungsdienst, Wachbucherstellung und Dienstplaneinteilung.

Die im Rahmen dieses Konzeptes geplanten Dateien enthalten neben reinen Sachinformationen personenbezogene Mitarbeiter- und Betroffenendaten. Die Verarbeitung dieser Daten ist in der mir vorgelegten Form aufgrund der im Brandschutzgesetz definierten Aufgaben erforderlich. Eine abschließende Beurteilung ist erst nach Vorliegen des dv-technischen Dateikonzeptes möglich.

Vor der technischen Realisierung ist das Feinkonzept u. a. in folgenden Bereichen zu verändern bzw. zu ergänzen:

- In bezug auf die Auslagerung und Auswertung der Einsatzdatenbestände ist eine klare Definition der Auswertungskriterien erforderlich.
- Das Verfahren der Anonymisierung der für die Feuerwehr nicht mehr erforderlichen Einsatzdaten zur Aufarbeitung für statistische Zwecke ist zu beschreiben.
- Lösch- und Sperrfristen für Daten aus den Bereichen Archiv, Personal- und Berichtswesen sind festzulegen.

2.2.6.2 Entwurf eines Rettungsdienstgesetzes

Der Senator für Inneres hat mir den Entwurf eines Bremischen Rettungsdienstgesetzes zur Stellungnahme zugeleitet. Dieser Entwurf stellt einen weitgehenden Bezug zu den Datenschutzbestimmungen im Brem. Brandschutzgesetz her. Er sieht jedoch für spezielle Datenverarbeitungen, die nur den Rettungsdienst betreffen, darüber hinausgehende Datenverarbeitungsregelungen vor. Diese Regelungen halte ich für zu weitgehend, denn durch die Beteiligung der Hilfsorganisationen durch die Feuerwehr sind neben der Datenverarbeitung in der Einsatzleitzentrale zusätzliche Datenverarbeitungen bei den Helfern vorgesehen. Ich habe dem Senator mitgeteilt, daß die Datenverarbeitungen bei den Hilfsorganisationen auf das unbedingt notwendige Maß reduziert werden sollten. Auch sollten die Dokumentationsdaten, die statistischen Daten, die Daten zur Unterrichtung von Angehörigen, die Daten zur Abrechnung des Rettungseinsatzes und die Datenübermittlungen im Rahmen des Rettungsgeschehens grundsätzlich auf die Berufsfeuerwehr beschränkt werden. Erforderliche Ausnahmen davon wären präzise und normenklar zu gestalten.

Mit dem Senator für Inneres befinde ich mich in weiteren Abstimmungsgesprächen.

2.2.6.3 Europaweit einheitliche Notrufnummer von Polizei und Feuerwehr

Auf der Grundlage einer Entscheidung des Rates der EG — veröffentlicht im Amtsblatt der EG Nr. C 275/4 vom 1. 11. 1990 — hat der Bundesrat die Übernahme der Einführung einer europaweit einheitlichen Notrufnummer — 112 — auch in der Bundesrepublik Deutschland beschlossen. Diese einheitliche Notrufnummer war bisher für die Feuerwehr als sogenannter Feuerwehrruf reserviert.

Es wurde überlegt, alle Notrufe sowohl die der Polizei als auch die der Feuerwehr, über diese Rufnummer abzuwickeln. Die Zusammenlegung der Meldewege hätte zu einem datenschutzrechtlichen Problem geführt, weil die Polizei von Daten, die für die Feuerwehr bestimmt gewesen wären, Kenntnis erhalten hätte. Eine solche Verknüpfung der Informationswege wäre wegen des Verfolgungs- und Anklagezwanges (Legalitätsprinzip), der für die Polizei gilt, problematisch. Da die Meldungen an die Feuerwehr aber zweckgerichtet zur Rettung von Menschen, zur Bekämpfung von Bränden und zur Abwehr anderer Gefahren dienen, wäre eine Verwertung durch die Polizei eine Zweckänderung, die durch keine Rechtsnorm gedeckt ist.

Ich habe meine Bedenken dem Senator für Inneres vorgetragen. Dieser hat nunmehr erklärt, daß die Notrufnummer 112 bei der Feuerwehr verbleiben wird. Sollten sich unter den dann eingehenden Meldungen solche für die Polizei befinden, so wird durch eine entsprechende Leitung die Polizei direkt von der Feuerwehreinsatzleitzentrale zugeschaltet.

2.2.7 Fundämter

Datenverarbeitung bei den Fundämtern Bremen und Bremerhaven

Jeder Bürger und jede Bürgerin ist nach den Vorschriften des Bürgerlichen Gesetzbuches (§§ 965-984) verpflichtet, Fundsachen, deren Wert DM 10,— übersteigt, der zuständigen Behörde, in Bremen dem Fundamt oder der beauftragten Polizei anzuzeigen und dort evtl. abzuliefern. Dieser Verpflichtung kommen in Bremen jährlich ca. 6.000 ehrliche Finder nach.

Durch eine Meldung des neuen Stadtamtes Bremen zum Dateienregister über eine „Fundsachendatei" wurde ich auf die Datenverarbeitung in diesem Zusammenhang aufmerksam. Bei meiner Prüfung stellte ich folgendes fest:

- Die meisten Fundsachen werden wegen der örtlichen Nähe bei den Polizeirevieren abgegeben bzw. angezeigt.
- Bei der Abgabe bzw. Anzeige der Fundsache wird eine Vielzahl von Daten erhoben. Nicht nur die Fundsache wird beschrieben, der Fundort und die Fundzeit festgehalten sowie der Wert geschätzt, sondern es werden die Daten des Finders und bei Minderjährigen auch die Daten des/der gesetzlichen Vertreter, die Bankverbindung, die Telefonnummer, das Alter des Finders, Name, Anschrift und Telefonnummer des Ablieferers und evtl. auch des Eigentümers erfaßt. Des weiteren wird festgehalten, ob der Finder Finderlohn oder Auslagenersatz beansprucht und ob er auf das Eigentum an der Fundsache verzichtet.
- Diese Daten werden in eine Fundkarte eingetragen. Diese Fundkarte besteht aus einem Durchschreibesatz, wobei das Original und die 1. Durchschrift an das Fundamt weitergeleitet werden bzw. beim Fundamt verbleiben.
- Eine Durchschrift erhält der Finder bzw. Ablieferer als Nachweis für die Anzeige bzw. Ablieferung der Fundsache.
- Zwei weitere Durchschriften werden an die Kriminalpolizei „zur weiteren Auswertung und Veranlassung" übersandt.
- Für bestimmte Fundsachen (Tiere, Kfz, Ausweispapiere, Fundsachen auf der Autobahn) bestehen daneben besondere Spezialregelungen über die Behandlung und Unterrichtung dritter Stellen (Tierheim, ADAC u. a.).

Der Umfang der Datenerhebung bei der Ablieferung der Fundsache ist zu umfassend. So ist z. B. die Angabe des/der gesetzlichen Vertreter nur erforderlich, wenn der Minderjährige auf das Eigentum an der Fundsache verzichten will, denn nur dazu bedarf es der Einwilligung des gesetzlichen Vertreters.

Mir ist zwar ersichtlich, daß es durch die Fundsachenbeschreibung einschließlich des Fundortes und der Fundzeit in einigen Fällen möglich wird, die Sache einer Straftat zuzuordnen. Unbeschadet dessen habe ich datenschutzrechtliche Bedenken, daß in diesem Zusammenhang die Daten des Finders, evtl. seines gesetzlichen Vertreters, des Ablieferers und evtl. des Eigentümers für die Aufgabenerfüllung der Kriminalpolizei in jedem Fall erforderlich sind und an sie übermittelt werden müssen. Die Kriminalpolizei benötigt diese personenbezogenen Daten in keinem Fall für die Sachfahndung. Man wird sicher auch nicht behaupten wollen, daß stets (für jeden Regenschirm und jedes Fahrrad) eine Verbindung von Finder und Täter hergestellt werden kann. An diesem Beispiel wird die Absurdität dieser ungebremsten Datenübermittlung deutlich, die offensichtlich aus reiner Verwaltungsroutine entstanden ist und durch keine Rechtsnorm gedeckt ist.

Ich bin Ende 1991 mit dem Fundamt Bremen in Überlegungen eingetreten, wie dieses Verfahren datenschutzgerecht umgestaltet werden kann.

2.3 Justiz

2.3.1 PC am Richter- und Dezernentenarbeitsplatz

Das in meinem letzten Jahresbericht angesprochene Projekt „BREMIT" (vgl. 13. Jahresbericht, S. 29) hat im Berichtsjahr konkrete Formen angenommen. Mehrere Anträge auf PC-Einsätze am Richterarbeitsplatz sind mir zur Stellungnahme vorgelegt worden. Um den arbeitsplatzspezifischen Besonderheiten dieser Art des PC-Einsatzes konkrete Schutzmaßnahmen entgegenzustellen, habe ich mit dem Senator für Justiz und Verfassung den folgenden Maßnahmeplan erörtert und abgestimmt:

- Für die Regelungen an den Richterarbeitsplätzen werden die Bedingungen der Richtlinien für den Datenschutz am Arbeitsplatz übernommen. Eine Datensicherungs-Software wird eingesetzt.
- Der Aufbau von PC-Netzen erfolgt zum gegenwärtigen Zeitpunkt nicht; der Informationsaustausch zwischen Richter- und Kanzleiarbeitsplatz erfolgt per Diskette.
- Für den Diskettenaustausch werden Regelungen erarbeitet, um zu erreichen, daß Fehlleitungen ausgeschlossen werden.
- Dateien, die Verwaltungsangelegenheiten betreffen, werden aus Datenschutzkontrollgründen grundsätzlich auf den in den Kanzleien eingesetzten Rechnern geführt. Sollten für den Einzelfall Daten hieraus auf den Rechner am Richterarbeitsplatz übertragen werden, sind diese nach Abschluss des Verfahrens zu löschen.

- Für den Aufbau eigener Fundstellensammlungen werden keine personenbezogenen Daten gespeichert.
- Alle Softwareprodukte für richterspezifische Tätigkeiten werden vor Einsatz dahingehend getestet, daß sie mit den eingesetzten Datenschutzmechanismen kompatibel sind.
- Zusätzlich zu diesen allgemeinen Regelungen werden je nach Einsatzumgebung spezifische Maßnahmen ergriffen.

2.3.2 Novellierung des Strafvollzugsgesetzes

Den Justizvollzugsanstalten werden bei ihrer Aufgabenerfüllung zahlreiche Daten der Gefangenen und anderer Bezugspersonen, wie z. B. die von Angehörigen und Freunden, bekannt; Stationen des Vollzugs müssen dokumentiert werden, Lohnabrechnungen und Konten müssen geführt werden, um nur einige Beispiele zu nennen. Die daraus resultierenden Daten werden in verschiedenen Büchern, Karteien, automatisierten Dateien und Akten gespeichert. An diesen Daten bestehen vielfältige Interessen. Neben externen Interessenten, wie z. B. Kreiswehrersatzämter oder Gläubiger, sind die Interessen z. B. der Seelsorge, der ärztlichen Versorgung und der Mitgefangenen zu befriedigen.

Für die vielfältigen Formen der Datenverarbeitung im Strafvollzug gibt es keine gesetzliche Grundlage, denn das Strafvollzugsgesetz enthält keine ausreichenden gesetzlichen Regelungen zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Deshalb hat der Bundesminister der Justiz im Berichtszeitraum einen Referentenentwurf eines 4. Gesetzes zur Änderung des Strafvollzugsgesetzes vorgelegt. Ich habe in einer Stellungnahme gegenüber dem Senator für Justiz und Verfassung über diesen Gesetzgebungsentwurf hinausgehend umfassend zu Fragen der Regelung des Datenschutzes im Strafvollzug Stellung genommen.

2.3.3 Auskünfte aus dem Schuldnerverzeichnis

Ein in Hamburg angesiedeltes privates Rechenzentrum plant den Aufbau eines bundesweiten Schuldnerregisters. Hierzu ist es an das Amtsgericht Bremen herangetreten mit dem Antrag, Abschriften aus dem dort geführten Schuldnerverzeichnis zu erhalten. Das Rechenzentrum will die so gewonnenen Daten in eine zentrale Datei einstellen und gegen Vergütung ausgewählten Anwendern (z. B. Rechtsanwälten) ermöglichen, auf Datensätze zu Schuldnern zuzugreifen.

Der Präsident des Amtsgerichts Bremen hat den Antrag abgelehnt mit der Begründung, die Errichtung eines bundesweiten automatisierten Schuldnerregisters sei mit der Regelung des § 915 Abs. 4 Zivilprozeßordnung nicht vereinbar. Daraufhin hat das antragstellende Rechenzentrum einen Beschluß des Oberlandesgerichts Bremen (OLG) erwirkt, der das Amtsgericht zu einer erneuten Antragsbearbeitung verpflichtet. In seiner Begründung führt das OLG insbesondere aus, daß § 915 Abs.4 Zivilprozeßordnung (ZPO) in Verbindung mit den Allgemeinen Vorschriften über die Erteilung und Entnahme von Abschriften und Auszügen (AV) aus dem Schuldnerverzeichnis den Aufbau eines bundesweiten automatisierten Schuldnerregisters nicht ausschließe. Außerdem hat es auf den Gleichheitsgrundsatz verwiesen, indem festgestellt wurde, daß das beantragende Rechenzentrum die Auskünfte zum Aufbau eines Auskunfteibetriebes nutzen wolle und auch anderen Auskunfteien Auskünfte aus dem Schuldnerregister erteilt würden.

Zur erneuten Antragsbescheidung hat der Senator für Justiz und Verfassung meine Beratung erbeten. Ich habe darauf hingewiesen, daß sich die Erteilung von Abschriften zum Aufbau eines bundesweiten, automatisiert abrufbaren Schuldnerregisters nicht auf eine ausreichende Rechtsgrundlage stützen kann. § 915 Abs. 4 ZPO stellt bestimmte Bedingungen an die Erteilung von Abschriften; so muß sichergestellt werden, daß Löschungsfristen eingehalten werden und die Abschriften nicht in jedermann zugänglichen Druckerzeugnissen veröffentlicht werden. Außerdem enthält diese Regelung eine Ermächtigung für den Bundesminister der Justiz, konkretisierende Vorschriften zu erlassen. Diese liegen in der Form der Allgemeinen Vorschriften von 1955 vor. Diese AV, die auch nach Auffassung des Bundesministers der Justiz nicht die Rechtsqualität einer Rechtsverordnung einnehmen, bilden keine hinreichende Rechtsgrundlage für eine Datenübermittlung zum Zwecke des Aufbaus eines bundesweiten automatisierten Schuldnerverzeichnisses, zumal seinerzeit nicht die Vorgaben des Bundesverfassungsgerichtes zum Recht auf informationelle Selbstbestimmung berücksichtigt werden konnten.

Das Bundesverwaltungsgericht hat zur Zulässigkeit der Mikroverfilmung eines Handelsregisters für ein privates Unternehmen festgestellt, daß ein zentralisiertes und automatisiertes Register in privater Hand das informationelle Selbstbestimmungsrecht der Betroffenen in einem wesentlich größeren Ausmaß berührt als die bisher mögliche Einsicht und deshalb einer hinreichenden Rechtsgrundlage bedarf (BVerwG 7 c 48.88). Diese Aussage trifft erst recht auf das Schuldnerverzeichnis zu, das für den Betroffenen weitaus belastendere Daten enthält.

Demzufolge ist die Datenübermittlung zum Zweck des Aufbaus eines bundesweiten privaten Schuldnerverzeichnisses nicht zulässig. Der Senator für Justiz und Verfassung folgt dem im Ergebnis und hat dem Antragssteller mitgeteilt, daß er beabsichtige, bei einer Neubescheidung den Antrag erneut zurückzuweisen. Vorher wolle er aber noch die Stellungnahme der anderen Justizverwaltungen einholen. Das Verfahren ist noch nicht abgeschlossen.

Dieses Verfahren macht exemplarisch das gesamte Dilemma mit dem Schuldnerverzeichnis deutlich. Staatliche Stellen erstellen mit zwangsweise erhobenen Schuldnerdaten ein Register. Diese Daten werden zum Teil auf Umwegen Privaten ohne ausreichende Rechtsgrundlage zur Verfügung gestellt. Der Bundesgesetzgeber, der seit Jahren — nicht zuletzt von den Datenschutzbeauftragten — aufgefordert ist, datenschutzrechtlich konforme Regelungen zu erlassen, die ohne weiteres auch den modernen wirtschaftlichen Interessen Rechnung tragen können, kommt nicht schnell genug zu einem Ergebnis. Private Auskunfteien versuchen die Lücke auf ihre Art zu schließen. Ich vertrete die Auffassung, daß die Auskunft und Pflege der zwangsweise den Bürgern abverlangten Daten unter staatlicher Obhut bleiben muß. Durch die zögerliche Haltung auf Bundesebene in dieser Frage ermuntert, hat die Wirtschaft zusammen mit Auskunfteien bereits Fakten geschaffen.

2.3.4 Auskünfte aus dem Schuldnerverzeichnis auf Diskette

Das ADV-Programm „SIJUS-VOLLSTRECKUNG" beim Amtsgericht Bremen bietet die Möglichkeit, die im Schuldnerverzeichnis gespeicherten Daten auf elektronischen Datenträgern (Disketten) zu speichern und den Beziehern von fortlaufenden Abschriften aus dem Schuldnerverzeichnis in dieser Form zu übersenden. Der Senator für Justiz und Verfassung will der Regelung der im Entwurf vorliegenden Neufassung des § 915 ZPO vorgreifen, die eine Erteilung von Abschriften per Diskette ausdrücklich zuläßt. Er hat mich hierzu um Stellungnahme gebeten.

Die geltende Regelung des § 915 Abs. 4 Zivilprozeßordnung (ZPO) sowie die dazu erlassenen Allgemeinen Vorschriften über die Erteilung und Entnahme von Abschriften und Auszügen (AV) sehen nur eine Auskunfterteilung in Form von Listen vor. Ich habe gegenüber dem Senator für Justiz und Verfassung aber auch deshalb Bedenken geäußert, weil die Speicherung von Schuldnerdaten auf Diskette dem Empfänger eine Vielzahl von Nutzungsmöglichkeiten bietet. Er kann durch einfache Verarbeitungsschritte Daten vervielfältigen und nach bestimmten Kriterien auswerten. Eine derartige Form der Übermittlung könnte auch das Bestreben fördern, ein bundesweites automatisiertes Schuldnerverzeichnis aufzubauen (vgl. Pkt. 2.3.3).

Vor allem habe ich aber darauf hingewiesen, daß man nicht nur den belastenden Teil einer Vorschrift umsetzen kann, ohne gleichzeitig die geplante Verbesserung der Rechtsstellung der Bürger zu verwirklichen. Der Neuentwurf des § 915 ZPO enthält nämlich u. a. Regelungen zu den Rechten der durch die Speicherung im Schuldnerverzeichnis Betroffenen. Solange diese Regelungen keine Gesetzeskraft haben und die Betroffenen diese Rechte nicht einfordern können, sah ich mich außer Stande, der technischen Ausweitung der Übermittlungen aus dem Schuldnerregister zuzustimmen. Trotz meiner Bedenken hat der Senator für Justiz und Verfassung dieses Verfahren eingeführt.

2.3.5 Versteigerung von Beweismitteln

Durch einen Zeitungsbericht wurde ich darauf aufmerksam gemacht, daß ein durch die Staatsanwaltschaft Bremen beauftragter Gerichtsvollzieher sichergestelltes Diebesgut versteigerte, an dem noch der Anhänger für Beweisstücke befestigt war. So waren an gestohlenen Autoradios Karten angebracht, auf denen für die Bürger, die den Zuschlag erhielten, u. a. das Delikt (z. B. Diebstahl, Hehlerei), der Name des Geschädigten, der Name des Tatverdächtigen und der Name des Sachbearbeiters der Kriminalpolizei zu lesen waren.

Der Leitende Oberstaatsanwalt entschuldigte diesen Vorfall damit, daß der beauftragte Versteigerer vergessen habe, die Karten vor der Versteigerung zu entfernen. Die Übermittlung der Daten an den beauftragten Gerichtsvollzieher begründete die Staatsanwaltschaft mit der Regelung des § 64 Abs. 5 Strafvollstreckungsordnung (StVollstrO), wonach Beweisstücke an den Täter oder Teilnehmer einer Straftat in der Regel nicht veräußert werden dürfen.

Die Vorschriften des § 64 StVollstrO rechtfertigen nicht, daß z. B. Daten über den Geschädigten oder den Sachbearbeiter an den Gerichtsvollzieher weitergeleitet werden. Ich habe die Staatsanwaltschaft aufgefordert, unverzüglich eine Dienstanweisung zu treffen, in der das Verfahren zur Übergabe von Beweismitteln an den Versteigerer geregelt wird. Da auch die Übermittlung der Täterdaten nach Aussage der Staatsanwaltschaft kaum praktische Relevanz habe, will diese auf die Datenübermittlung ganz verzichten. In jedem Fall ist aber sicherzustellen, daß die Informationen nicht dem Auktionspublikum bekannt werden.

2.3.6 Weitergabe von Daten aus Strafverfahren an gemeinnützige Organisationen

Bei Strafverfahren besteht die Möglichkeit, daß das Verfahren gegen die Zahlung einer Geldbuße eingestellt wird. Das Bußgeld muß dann an eine gemeinnützige Organisation gezahlt werden. Zu diesem Zwecke werden von den Gerichten Überweisungsvordrucke ausgehändigt, aus denen nach dem Ausfüllen Name und Kontonummer des Betroffenen sowie das Aktenzeichen des Strafverfahrens ersichtlich sind. Gehen die Zahlungsanweisungen bei den Organisationen ein, können diese, wie darüber hinaus auch die Kreditinstitute erkennen, daß es sich bei der Überweisung nicht um eine freiwillige Spende, sondern um ein Bußgeld handelt. Das Amtsgericht Bremen benutzt zusätzlich ein Formular, aus dem neben den o. g. Angaben auch noch der Wohnort des Betroffenen ersichtlich ist. Dieses Formular wird den Organisationen mit der Bitte um Rückmeldung bei eingegangener Zahlung übersandt.

Die so entstehende Preisgabe von Daten aus Strafverfahren ist dem Betroffenen nicht unbedingt bewußt. Sie wird auch vom Gesetz nicht verlangt. § 153 a Abs. 2 StPO, der die Einstellung von Verfahren nach Erfüllung von Auflagen regelt, besagt, daß der Beschuldigte einen Geldbetrag zugunsten einer gemeinnützigen Einrichtung oder der Staatskasse zu zahlen hat. Es wird also nicht vorgeschrieben, daß der Betrag direkt an die Organisation gezahlt werden muß.

Die Verwendung der Überweisungsträger führt bei den gemeinnützigen Organisationen zu Sammlungen von Daten über Personen, die mit einem Strafverfahren überzogen worden sind. Diese Praxis halte ich für datenschutzrechtlich bedenklich.

Deshalb habe ich mich an den Senator für Justiz und Verfassung gewandt und ihn gebeten, ein anderes Verfahren zu ermöglichen, bei dem keine personenbezogenen Daten aus Strafverfahren an gemeinnützige Einrichtungen weitergeleitet werden. Ich habe angeregt, ein Verfahren zu wählen, bei dem entweder die zuständige öffentliche Stelle direkt das Bußgeld einzieht oder der Betroffene eine Zahlung an die Landeshauptkasse leistet. Die Bußgeldbeträge könnten dann in regelmäßigen Abständen anonymisiert an die einzelnen gemeinnützigen Einrichtungen weitergeleitet werden.

2.4 Bildung und Wissenschaft

Bremisches Archivgesetz

Im Berichtsjahr wurde das Bremische Archivgesetz von der Bremischen Bürgerschaft verabschiedet; es ist mit wenigen Ausnahmen seit Mitte Mai 1991 in Kraft. Mit diesem Gesetz haben die jahrelangen Bemühungen um eine Rechtsgrundlage für die öffentlichen Archive ein erfolgreiches Ende gefunden.

Es bleibt jetzt nur noch, die Benutzungsordnungen der Archive (Staatsarchiv Bremen, Stadtarchiv Bremerhaven) dem neuen Recht anzupassen und neu zu erlassen.

2.5 Jugend und Soziales

2.5.1 Online-Zugriff auf Daten bei der Landeshauptkasse

Der Senator für Jugend und Soziales erbat meine baldige Stellungnahme zu seiner Absicht, sein Rechtsreferat mit der Möglichkeit auszustatten, auf Datenbestände

der Landeshauptkasse beim Rechenzentrum der bremischen Verwaltung im Online-Verfahren zuzugreifen. Als Ausgleich für die Einsparung einer halben Stelle — so der ADV-Antrag — wolle er die zuständigen Sachbearbeiter/innen in seiner Vollstreckungsstelle in die Lage versetzen, sich jederzeit über den aktuellen Kontostand der von ihnen bearbeiteten Vollstreckungsfälle zu informieren. Ich fragte nach der Rechtsgrundlage und wies auf § 14 Abs. 1 BrDSG hin, der für automatisierte Verfahren, die die Übermittlung personenbezogener Daten auf Abruf ermöglichen, eine Erlaubnis durch Bundes- oder Landesrecht verlangt. Darauf erhielt ich zur Antwort, man wolle gar nicht auf „fremde" Datenbestände zugreifen, da die Landeshauptkasse lediglich Zahlungseingänge von Schuldnern zu Buchhaltungszwecken registriere und dem Haushalt des Ressorts gutschreibe.

Ich bat daraufhin die Landeshauptkasse zu bestätigen, daß sie die betreffenden Daten im Auftrag des Senators für Jugend und Soziales verarbeite. In diesem Fall fände § 14 BrDSG keine Anwendung, weil es am Tatbestand der Übermittlung im Sinne von § 2 Abs. 2 Nr. 4 BrDSG fehlen würde (siehe auch § 2 Abs. 3 Nr. 3 BrDSG, wonach der Auftragnehmer nicht Dritter ist). Zugleich machte ich auf die inhaltlichen und verfahrensmäßigen Voraussetzungen aufmerksam, an die §§ 80 SGB X, 11 BDSG die Datenverarbeitung im Auftrag eines Sozialleistungsträgers knüpfen. Auf meine wiederholt geäußerte Bitte um Stellungnahme erklärte die Landeshauptkasse zunächst, sie verarbeite die betreffenden Daten in ihrer eigenen Zuständigkeit nach der LHO, ausdrücklich nicht im Auftrag des Senators für Jugend und Soziales. Dennoch hatte dieser zuvor mit der Versicherung, die Landeshauptkasse habe bestätigt, daß sie die Daten in seinem Auftrag verarbeite und meine Bedenken seien deshalb ausgeräumt, einen zustimmenden Beschluß des ADV-Ausschusses herbeigeführt. Erst auf meine nochmalige Intervention bei allen beteiligten Stellen hin erklärte die Landeshauptkasse, es handele sich „im weitesten Sinne" um Datenverarbeitung im Auftrag. Sie sei lediglich mit der Datenverarbeitung befaßt. Die sonstige Verfolgung der in Rede stehenden Forderungen — es handelt sich dabei um übergeleitete zivilrechtliche Unterhaltsforderungen — betreibe die Vollstreckungsstelle des Senators für Jugend und Soziales. Ich habe daraufhin anerkannt, daß für dieses spezielle Vollstreckungsverfahren ausnahmsweise die Landeshauptkasse nicht in eigener Zuständigkeit, sondern im Auftrag des Fachressorts tätig wird.

Auf meine wiederholte Bitte, den Auftrag — wie von § 11 Abs. 2 Satz 2 BDSG verlangt — schriftlich zu erteilen und mir zur Kenntnis zu geben, erhielt ich schließlich vom Senator für Jugend und Soziales die Nachricht, derzeit sei noch nicht abzusehen, wann die Mittel für die Beschaffung bzw. Installation der Geräte zur Verfügung stünden. Deshalb sei die Erteilung des Auftrags zugunsten vordringlicherer Arbeiten zurückgestellt worden. Dabei verkennt der Senator für Jugend und Soziales, daß der schriftliche Auftrag schon vor Installation des automatisierten Abrufverfahrens auch für das jetzige Verfahren erforderlich ist.

Der Vorgang gibt zu folgenden allgemeinen Bemerkungen Anlaß:

— Die Vorschriften des § 14 BrDSG über den Direktabruf von Daten und des § 8 BrDSG bzw. der §§ 80 SGB X, 11 BDSG über die Datenverarbeitung im Auftrag scheinen noch nicht Eingang in die Praxis des Verwaltungshandelns gefunden zu haben (vgl. zur Datenverarbeitung im Auftrag auch meinen 12. Jahresbericht, S. 50).

— Die Datenverarbeitung der Landeshauptkasse bedarf über die Aufgabenzuweisung in § 79 LHO hinaus dringend einer normenklaren bereichsspezifischen Rechtsgrundlage. Dabei müßten dann auch die Rechtsbeziehungen zwischen der Landeshauptkasse und den Fachressorts geklärt werden.

2.5.2 Datenschutz in der Kinder- und Jugendhilfe

Zum 01. 01. 1991 ist als SGB VIII das neue Kinder- und Jugendhilfegesetz (KJHG) in Kraft getreten. Auf Betreiben des Bundesrats und der Datenschutzbeauftragten von Bund und Ländern enthält es ein Kapitel „Schutz personenbezogener Daten", §§ 61 bis 68, das die Erhebung, Speicherung, Verwendung, Offenbarung, Löschung und Sperrung der Daten sowie die Auskunftsansprüche der Klienten der Kinder- und Jugendhilfe regelt. Vor allem vier Regelungen sind wegen ihrer neuen Inhalte bemerkenswert:

— Das KJHG unterscheidet in § 2 Abs. 2 und 3 die Aufgaben der Jugendhilfe nach freiwilligen Leistungen und nach anderen Aufgaben, deren Erfüllung durchaus mit Zwangsmaßnahmen verbunden sein kann. § 63 Abs. 2 Satz 2 bestimmt, daß

Daten, die zu Leistungszwecken, mit solchen, die für andere Aufgaben erhoben worden sind, nur zusammengeführt werden dürfen, soweit dies zur Erfüllung der jeweiligen Aufgabe erforderlich ist. Damit wird grundsätzlich eine getrennte Aktenführung je nach Hilfe- und Aufgabenart gefordert.

- Nach § 64 Abs. 1 dürfen Daten nur zu dem Zweck verwendet werden, zu dem sie erhoben worden sind. Dies betrifft auch den Fall, daß die Daten zwar in derselben Behörde, aber für andere Zwecke genutzt werden sollen. Auch dies bedeutet eine Übermittlung bzw. Offenbarung und ist zwar im Prinzip nach § 69 Abs. 1 Nr. 1 SGB X zulässig, ist aber nach § 64 Abs. 2 dann unzulässig, wenn dadurch der Erfolg einer zu gewährenden Leistung in Frage gestellt wird.
- § 65 ergänzt die vorstehenden Regelungen durch einen besonderen Schutz, den Klientendaten genießen, die dem Mitarbeiter eines Trägers der öffentlichen Jugendhilfe zum Zwecke persönlicher und erzieherischer Hilfen anvertraut worden sind. Hiermit wird die bisher nur für bestimmte Berufsgruppen (wie etwa Psychologen, Sozialpädagogen, Sozialarbeiter) gesetzlich bestimmte Schweigepflicht auf alle Mitarbeiter des Jugendhilfeträgers ausgedehnt.
- Schließlich gibt § 68 Abs. 3 jeder volljährigen Person, die unter Amtspflegschaft oder Amtsvormundschaft gestanden hat, über die allgemeinen Auskunfts- und Einsichtsrechte hinaus das Recht, auf Kenntnis der zu ihrer Person gespeicherten Informationen, soweit nicht berechtigte Interessen Dritter entgegenstehen.

Diese Regelungen müssen erhebliche Konsequenzen für den Umgang des Jugendamtes Bremerhaven und des Amtes für Soziale Dienste in Bremen mit Klientendaten nach sich ziehen.

Insbesondere verbietet der zitierte § 65 SGB VIII jetzt ausdrücklich die im Amt für Soziale Dienste immer noch weit verbreitete Praxis, daß die Abteilung Wirtschaftliche Hilfen nur dann die Kosten für Leistungen der Jugendhilfe übernimmt, wenn ihr zuvor Entwicklungsberichte, psychosoziale Diagnosen und ärztliche Gutachten vorgelegt worden sind, mit der Folge, daß diese Unterlagen auf Dauer zu den Akten der Sozialhilfe bzw. Wirtschaftlichen Jugendhilfe genommen werden. Diese Unterlagen sind allein dazu geeignet und erforderlich, die hierfür qualifizierten und zuständigen Mitarbeiter der Sozialen Dienste für Kinder und Jugendliche und ihre Familien in die Lage zu versetzen, ein fachliches Urteil darüber abgeben zu können, ob eine bestimmte Leistung angebracht ist. Deren plausibel begründetes Votum wiederum sollte die Grundlage für die Entscheidung über die Kosten sein. Entsprechend sieht § 36 Abs. 2 lediglich vor, daß mehrere Fachkräfte der Kinder- und Jugendhilfe, nicht aber Mitarbeiter des Trägers der Sozialhilfe bei der Entscheidung über langfristige Hilfe zur Erziehung zusammenwirken sollen. Die Tatsache, daß im Amt für Soziale Dienste Bremen der Träger der Kinder- und Jugendhilfe und der Träger der Sozialhilfe organisatorisch zusammengefaßt sind, setzt die eindeutigen Regelungen des KJHG nicht außer Kraft.

Eine Übermittlung der o.g. Unterlagen an die Abteilung Wirtschaftliche Hilfen ist somit nicht erforderlich und verstößt gegen §§ 35 SGB I, 69, 76 SGB X. Zugleich zwingt das Jugend- und Sozialressort mit seiner Praxis Ärzte, Psychologen, Sozialarbeiter und Sozialpädagogen dazu, ihre berufliche Schweigepflicht zu verletzen und sich damit der Strafdrohung des § 203 StGB auszusetzen.

Eine mögliche Folge der kritisierten Praxis ist mir kürzlich vor Augen geführt worden: In einem Beschwerdefall hatte mich ein Abschnittsleiter der Wirtschaftlichen Hilfen unter Berufung und Wiedergabe der ungünstigen psychosozialen Diagnose des zuständigen ambulanten Sozialdienstes davor gewarnt, den Angaben des betroffenen Beschwerdeführers zu vertrauen. Dieses Beispiel illustriert deutlich, wie die von einer bestimmten Stelle zu einem bestimmten Zweck zulässigerweise erhobenen Daten andern Orts in einem anderen Zusammenhang unzulässigerweise gegen den Betroffenen verwendet werden können.

Der Senat hat in seiner Stellungnahme zu meinem 13. Jahresbericht angekündigt, daß das Amt für Soziale Dienste auf der Grundlage des KJHG alle bisherigen Dienstanweisungen überarbeiten, die aus der Sicht des Datenschutzes erforderlichen Änderungen vornehmen und mich daran beteiligen werde. Seither ist mir lediglich ein Entwurf für die Neuregelung des Verfahrens für die Aufnahme behinderter oder entwicklungsgestörter Kinder in Kindertagesheime vorgelegt worden. Für dessen inzwischen mit mir abgestimmte Fassung soll nunmehr das Mitbestimmungsverfahren eingeleitet werden. Ich habe die Hoffnung, daß diese Regelung, die endlich den Schutz der Persönlichkeitsrechte von Kindern und

Eltern zu gewährleisten geeignet ist, bereits im bevorstehenden Aufnahmeverfahren für das Kindergartenjahr 1992/1993 Anwendung findet. Die Überarbeitung der anderen Verwaltungsvorschriften steht noch aus.

2.5.3 Neuregelung des Sozialdatenschutzes

Im März 1991 leitete mir der Senator für Arbeit mit der Bitte um Stellungnahme einen Referentenentwurf zur Änderung des Sozialgesetzbuches aus dem Bundesministerium für Arbeit und Sozialordnung zu. Der Entwurf enthält neben Ergänzungen des Abschnitts zur Datenverarbeitung und zum Datenschutz in der gesetzlichen Krankenversicherung im SGB V (vgl. dazu Pkt. 2.6.1) eine völlige Neuregelung der Bestimmungen des § 35 SGB I und der §§ 67 bis 85 SGB X zum Schutz des Sozialgeheimnisses. Diese Neuregelung ist zwar überfällig, würde aber in der vorgelegten Fassung zu Lasten des Datenschutzes gehen.

Das SGB regelt bislang — für alle Sozialleistungsträger, auch für die der Länder und Gemeinden — lediglich einzelne Phasen der Datenverarbeitung, so z. B. in §§ 60 ff. SGB I die Datenerhebung bei Antragstellern und in §§ 35 SGB I, 67 bis 78 SGB X den Schutz des Sozialgeheimnisses und die Offenbarungsbefugnisse der Leistungsträger. Im übrigen verweist § 79 SGB X auf bestimmte Abschnitte und Vorschriften des bis zum 31.05.1991 gültigen Bundesdatenschutzgesetzes aus dem Jahre 1977. Nach dessen Neufassung im Jahre 1990 war eine Anpassung des SGB ohnehin überfällig. So hat das neue BDSG die Datenverarbeitung in Akten in seinen Schutzbereich einbezogen, wohingegen der Wortlaut des § 79 Abs. 1 Satz 1 SGB X weiterhin sich nur auf Daten bezieht, die in Dateien verarbeitet werden. Ich begrüße es, daß inzwischen der Bundesminister für Arbeit und Sozialordnung die seiner Aufsicht unterstehenden Sozialleistungsträger und die Spitzenverbände der Sozialversicherungsträger darauf aufmerksam gemacht hat, daß die Verweisung in § 79 SGB X auf das BDSG nach dessen Neufassung auch die in Akten verarbeiteten Daten erfaßt. Ich gehe davon aus, daß die Sozialleistungsträger des Landes Bremen und seiner Stadtgemeinden entsprechend verfahren. Im übrigen aber ist die Rechtslage derzeit von Unklarheit gekennzeichnet, da §§ 79 bis 84 SGB X eine Fülle von Verweisen auf das BDSG 77 enthalten.

Überdies üben die Datenschutzbeauftragten von Bund und Ländern seit langem Kritik daran, daß § 69 Abs. 1 SGB X für den Datenaustausch der Sozialleistungsträger untereinander das Gebot der Bindung des Zwecks der Datenverarbeitung an die Rechtsgrundlage für die Erhebung außer Kraft setze, indem die Vorschrift einen „Sozialdatenpool" legitimiere. Es gibt denn auch Bestrebungen, die Übermittlungsbefugnis des § 69 SGB X unter Beachtung des Zweckbindungsgebots einschränkend auszulegen, leider bisher ohne Auswirkung auf die Praxis. Mehrere Länder (so Bremen in §§ 12, 13 BrDSG 1987) und nun auch der Bund (in §§ 14, 15 BDSG 1990) lassen inzwischen die Übermittlung von Daten an eine andere Stelle, die sie zu einem anderen Zweck verarbeiten will, nur ausnahmsweise unter bestimmten Voraussetzungen zu. Die Folge ist, daß Sozialdaten derzeit einen schwächeren Schutz genießen als andere von öffentlichen Stellen verarbeitete personenbezogene Daten. Angesichts der Schutzbedürftigkeit der Klienten von Sozialleistungsträgern und ihrer Sozialdaten sowie angesichts der Ausdifferenzierung des für den betroffenen Bürger längst unübersichtlich gewordenen Sozialleistungsbereichs ist dies unerträglich.

Leider wird der Referentenentwurf der Notwendigkeit, die Grundrechte der Sozialversicherten und der anderen Empfänger von Sozialleistungen zu gewährleisten, in keiner Weise gerecht. Im Gegenteil, er zementiert den verfassungsrechtlich fragwürdigen „Sozialdatenpool", indem er den Wortlaut des geltenden § 69 Abs. 1 Nr. 1 SGB X übernimmt. Außerdem höhlt er die engeren Erhebungs- bzw. Mitwirkungsregelungen der geltenden §§ 60 ff. SGB I aus, indem er den Sozialleistungsträgern gestatten will, Daten weitgehend ohne Mitwirkung des Betroffenen zu erheben. Das BrDSG und das BDSG 1990 binden in ihren §§ 10 bzw. 13 diese Befugnis an sehr viel engere Voraussetzungen. Ich erwarte von einer Neuregelung des Sozialdatenschutzes, daß sie den Schutz des Sozialgeheimnisses konkretisiert und stärkt, nicht aber aushöhlt. In diesem Sinne habe ich wie auch der Bundesbeauftragte und andere Landesbeauftragte für den Datenschutz Stellung genommen.

2.5.4 Versuchter Schutz des Bürgers vor der Kenntnisnahme seiner Daten

Ein Bürger hatte sich an mich gewandt, der Einsicht in „seine" bereits 1977 abgeschlossene Pflegschaftsakte genommen und vergeblich darum gebeten hatte, sie aus persönlichem Interesse an seiner Lebensgeschichte kopieren zu dürfen. Ich

habe das Amt für Soziale Dienste auf § 68 Abs. 3 KJHG sowie darauf hingewiesen, daß § 25 Abs. 5 SGB X mit dem Anspruch auf Akteneinsicht das Recht verbinde, sich von der Behörde gegen angemessenen Ersatz ihrer Aufwendungen Ablichtungen erteilen zu lassen. Trotz der eindeutigen Rechtslage bestand das Amt auf seiner Weigerung. Es wurde angeführt, daß die Rechte der beteiligten Mitarbeiter tangiert seien, daß man künftig Akten „ganz anders" führen müsse, kurz, der Datenschutz sei verletzt. Diese Argumentation wird im Zusammenhang mit Auskunfts- und Einsichtsrechten der Betroffenen, etwa auch in der Psychiatrie, immer wieder verwandt. Ihr ist entgegenzuhalten, daß §§ 25 SGB X, 68 Abs. 3 KJHG und entsprechende Regelungen unter entgegenstehenden berechtigten Interessen Dritter lediglich diejenigen von außenstehenden Privatpersonen (z. B. Angehörigen oder Nachbarn) verstehen, nicht aber die der Personen, die von Amts wegen gegenüber dem Betroffenen tätig geworden sind. Das Auskunfts- und Einsichtsrecht ist in seinem Kern gerade darauf ausgerichtet, daß sich diese Personen dem Rechtsinhaber gegenüber für ihre Aufgabenerfüllung einschließlich der Verarbeitung seiner Daten verantworten müssen. Es bedurfte einiger Hartnäckigkeit, ehe nach etwa einem Jahr der Antragsteller zu seinem Recht kam. Dem Vernehmen nach will das Amt nunmehr eine Dienstanweisung zu den Auskunfts- und Einsichtsrechten seiner Klienten erarbeiten.

2.5.5 Amtliche Kinder- und Jugendhilfestatistik

Das KJHG trifft in §§ 98-103 Regelungen zur Kinder- und Jugendhilfestatistik. Seitens des Jugendamtes Bremerhaven und von Mitarbeitern des Amtes für Soziale Dienste in Bremen (AfSD) wurde ich gebeten, zu Befürchtungen Stellung zu nehmen, diese amtliche Statistik höhle das Sozialgeheimnis aus.

Ausgangspunkt hierbei war, daß das KJHG eine Rechtsgrundlage geschaffen hat, die es erlaubt, zu Zwecken der Statistik einen umfangreichen Katalog von Angaben über Empfänger der entsprechenden Hilfeleistungen zu erheben und zur weiteren statistischen Bearbeitung an das Statistische Landesamt weiterzuleiten. Dabei gilt es sicherzustellen, daß

- die Verarbeitung der Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, auf das gesetzlich erlaubte Maß beschränkt bleibt (z. B. keine Verarbeitung des Aktenzeichens, keine Angabe des Gemeindeteils durch die Mitarbeiter/innen, Regionalisierung höchstens bis zur Stadtteilebene),
- entsprechend § 5 Landesstatistikgesetz mit der Einsammlung der ausgefüllten Erhebungsbögen, ihrer Kontrolle und ihrer Weiterleitung an das Statistische Landesamt nur Personen beauftragt werden, die nicht zugleich mit anderen Aufgaben des Verwaltungsvollzugs betraut sind.

Das Statistische Landesamt hat auf meine Intervention hin inzwischen aufgrund seiner Befugnis nach § 12 Nr. 3 Landesstatistikgesetz organisatorische und technische Anordnungen für eine einheitliche gesetzmäßige Durchführung dieser Statistik getroffen. Damit dürften auch die Befürchtungen der Mitarbeiter ausgeräumt sein, denn obwohl das KJHG die Erhebung und Bearbeitung einer Fülle sehr sensibler Daten zu statistischen Zwecken erlaubt und im wichtigen Punkt ihrer regionalisierten Aufbereitung leider keine normenklare Regelung trifft, ist es doch gelungen, die Grundlage für ein datenschutzgerechtes Verfahren im Lande Bremen zu schaffen.

2.5.6 Geschäftsstatistiken im Amt für Soziale Dienste

Im Amt für Soziale Dienste in Bremen wurden neue Statistiken für die Sozialdienste Erwachsene ohne Kinder, ältere Menschen und im Krankenhaus vorbereitet. Ich habe das Sozialressort darauf hingewiesen, daß es sich hierbei mangels gesetzlicher Anordnung lediglich um ressortinterne Geschäftsstatistiken nach § 11 Landesstatistikgesetz handeln könne. Dies habe zur Folge, daß für eine derartige Statistik nur bei der Aufgabenerledigung ohnehin angefallene Einzelangaben genutzt werden dürften, zusätzliche oder gesonderte Datenerhebungen seien nicht zulässig. Zudem sei zu gewährleisten, daß nur solche Ergebnisse der Statistik weitergegeben oder veröffentlicht werden, die keine Angaben enthalten, die einen Bezug auf einen Betroffenen zulassen. Das Sozialressort hat meine Vorschläge durchweg aufgenommen. Außerdem habe ich darauf hingewiesen, daß der Verarbeitung der Erhebungsbögen im RbV ein schriftlicher Auftrag zugrunde liegen müsse, der es dem Sozialressort ermögliche, seiner gesetzlichen Verantwortung aus §§ 80 SGB X, 11 BDSG nachzukommen.

2.5.7 Übermittlungen von Heimträgern an den Sozialhilfeträger

Von Seiten eines Trägers der Altenhilfe bin ich darauf hingewiesen worden, es sei weit verbreitete Praxis, daß Heimträger das Amt für Soziale Dienste auf dessen Verlangen darüber unterrichten, wenn ein Bewohner mehr als DM 4.500,— auf seinem Heimkonto angespart habe. Dies stößt auf datenschutzrechtliche Bedenken. Zwar ist das Datum für die Leistung von Sozialhilfe erheblich, weil ein Betrag in dieser Höhe nach § 88 BSHG als Vermögen einzusetzen ist. Es ist aber nach § 60 SGB I Sache des Betroffenen selbst, eine Veränderung seiner für die Leistung erheblichen Verhältnisse anzuzeigen. Ebensowenig ist der Sozialhilfeträger ohne weiteres befugt, Daten über den Leistungsempfänger ohne dessen Mitwirkung zu erheben, §§ 79 SGB X, 13 BDSG.. Ich habe das Sozialressort und den Träger der Altenhilfe auf die Rechtslage hingewiesen und um Stellungnahme gebeten.

Auch das ZKH Bremen-Ost unterrichtete bislang das Amt für Soziale Dienste, wenn das Guthaben eines von Sozialhilfe abhängigen Patienten auf dem für ihn geführten „Patienteneigengeldkonto" den Betrag von DM 4.500,— überschritt (vgl. 12. Jahresbericht, S. 42). Kürzlich hat der Senator für Gesundheit mitgeteilt, das ZKH Bremen-Ost werde seine entsprechende Richtlinie dahingehend ändern, daß künftig nur der Patient über seine Pflichten gegenüber dem Sozialhilfeträger, aber nicht mehr der letztere über die Höhe des Betrags auf dem Eigengeldkonto informiert werde.

2.6 Gesundheit

2.6.1 Datenschutz und Krankenversicherung

In meinem 13. Jahresbericht hatte ich auf S. 37/38 gewürdigt, daß das Gesundheitsreformgesetz (SGB V) von 1989 wesentlich präziser als vor ihm die Reichsversicherungsordnung die Befugnisse der an der Gesundheitsversorgung beteiligten Stellen zur Verarbeitung von Versicherten- bzw. Patientendaten festlegt. Ich hatte zugleich Bestrebungen der Krankenkassen kritisiert, Ärzte und Krankenhäuser zur Übermittlung von Daten ihrer Patienten zu veranlassen, die über das durch das neue Gesetz erlaubte Maß hinausgehen. Vielfältige Entwicklungen veranlassen mich, meine Kritik fortzuführen.

— Kontrolle der Verweildauer in Krankenhäusern

Ich berichtete u. a. darüber, daß die Krankenkassen von den Krankenhäusern verlangen, ihnen Berichte über die Gründe für eine drei Wochen übersteigende Verweildauer ihrer Patienten zu geben und hatte dies kritisiert, weil die einschlägige Gesetzesvorschrift, § 301 SGB V, derartige Verlängerungsanzeigen nicht vorsieht. Die Landesverbände der Krankenkassen wollen an der Praxis festhalten. Auf den Hinweis eines Krankenhauses, die Kassen befristeten zunehmend ihre Kostenzusagen und verlangten bei Überschreitung der Fristen zusätzliche Berichte, habe ich kürzlich die Landesverbände erneut angeschrieben. Eine Antwort steht aus.

— Kontrolle durch Anforderung der Entlassungsberichte

Ein ähnliches Beispiel wird bundesweit erörtert. Von Seiten der Datenschützer wird seit langem bestritten, daß ein Krankenhaus bzw. eine Rehabilitations- oder Kurklinik befugt oder verpflichtet sei, auf deren Anforderung hin der Krankenkasse den für den behandelnden Arzt bestimmten Entlassungsbericht über einen Patienten zu übersenden. Genau dies aber verlangen zunehmend die Kassen mit der Begründung, sie benötigten die Berichte für die Prüfung ihrer Leistungspflicht oder aber für Zwecke der Planung oder Statistik. Das Zentralkrankenhaus Bremen-Ost machte mich darauf aufmerksam, daß auch Entlassungsberichte der Psychiatrie angefordert würden. Das Krankenhaus will dem entgegenhalten, daß diese Berichte besonders sensible Daten enthielten und möchte nur solche Berichte übersenden, die sich auf die Beurteilung der stationären Handlungsbedürftigkeit beschränken oder aber lediglich zur Beantwortung übermittelte Fragen beantworten. Ich habe die Landesverbände der Krankenkassen darauf hingewiesen, daß § 301 SGB V die Krankenhäuser weder befugt noch verpflichtet, Entlassungsberichte zu übermitteln. Lediglich dem Medizinischen Dienst der Krankenkassen ist es nach § 276 Abs. 4 SGB V gestattet, in den aufgeführten Fällen die Krankenunterlagen der Krankenhäuser an Ort und Stelle einzusehen. Die Kassenverbände haben bislang nicht geantwortet. Ich habe sie deshalb kürzlich noch einmal angeschrieben.

— Kontrolle des Verbrauchs an Hilfsmitteln

Jüngst wies mich ein Wohlfahrtsverband darauf hin, daß die Krankenkassen von ihm Angaben darüber verlangten, in welcher Menge die einzelnen Bewohner seiner Pflegeeinrichtungen bestimmte medizinische Hilfsmittel verbrauchten. Ich habe dem Verband bestätigt, daß er weder befugt noch verpflichtet ist, dies den Kassen zu übermitteln, zumal § 302 SGB V, der die Übermittlung von Leistungsdaten durch „sonstige Leistungserbringer" regelt, derartiges nicht vorsieht.

— Müssen Rettungsdienste Diagnosen übermitteln?

Ebenso wenig gerechtfertigt ist das Ansinnen, das die Kassen an Rettungsdienste richten, ihnen Befunde/Diagnosen zu übermitteln, die an Ort und Stelle bei den Unfallopfern festgestellt werden sollen. Es ist schon zu bezweifeln, ob die Fahrer und Sanitäter der Rettungsdienste ausreichend geschult sind bzw. Zeit und Ruhe haben, zuverlässige Aussagen zu treffen. Vor allem aber fehlt auch insoweit eine Befugnis in der einschlägigen Vorschrift des § 302 SGB V.

— Änderung eines unbequemen Gesetzes

Die Kassen argumentieren in den dargestellten Fällen, daß sie alle diese Daten, Berichte etc. benötigten, um ihren Aufgaben gerecht zu werden, und lassen dabei außer acht, daß es dem Gesetzgeber vorbehalten ist zu entscheiden, welche Befugnisse zur Datenverarbeitung er ihnen und den Leistungserbringern einräumt. Zugleich aber bemühen sich die Kassen um einen Ausgleich des aus ihrer Sicht festzustellenden gesetzgeberischen Defizits. Der Referentenentwurf aus dem Bundesministerium für Arbeit und Sozialordnung von 1991 für ein Zweites SGB-Änderungsgesetz jedenfalls sieht neben der bereits unter Pkt. 2.5.3 kritisierten Neuregelung der Datenverarbeitung aller Sozialleistungsträger auch eine Erweiterung der Befugnis und Verpflichtung von Ärzten und Krankenhäusern vor, Patientendaten an Krankenkassen zu übermitteln. Zwar fehlen weiterhin z. B. die Entlassungsberichte, die Übermittlung von Verlängerungsanzeigen durch die Krankenhäuser soll aber ausdrücklich in das Gesetz aufgenommen werden.

Ich befürchte, daß die Krankenkassen selbst dann, wenn das SGB V ihren Wünschen entsprechend geändert worden sein sollte, je nach Bedürfnis zusätzlich Versichertendaten zu erheben versuchen werden. Nach Aussage der Landesverbände der Betriebskrankenkassen gehen die Kassen ohnehin davon aus, daß das Gesetz nur einen Mindestkatalog der von den Leistungserbringern zu übermittelnden Daten enthalte.

2.6.2 Ärztliche Behandlung und Abrechnung der Leistungen demnächst nur noch mit Chipkarte?

Ein anderes Beispiel zeigt, daß auch eindeutige gesetzgeberische Entscheidungen keine ausreichenden Garantien für den Datenschutz darstellen. Zum 01. 01. 1992 sollten die gesetzlichen Krankenkassen für jeden Versicherten eine Krankenversichertenkarte ausstellen, die ausschließlich für den Nachweis der Berechtigung zur Inanspruchnahme von medizinischen Leistungen und zur Abrechnung der Kosten verwendet werden darf. Zugleich legt § 291 SGB V abschließend die Daten fest, die diese Karte enthalten darf. Im wesentlichen sind dies die zur Identifizierung des Versicherten erforderlichen Angaben, jedenfalls nicht solche Daten, die irgendwelche Rückschlüsse auf den Gesundheitszustand des Versicherten zulassen.

Zwar hat sich die Einführung der Krankenversichertenkarte — wohl in Folge technischer Probleme und mangels Akzeptanz seitens der Ärzte — verzögert. Jüngst kündigten aber die Spitzenverbände der Kassenärzte und der Ortskrankenkassen an, die Krankenversichertenkarte zum 01.07.1992 in einigen Regionen in Gestalt einer elektronischen Chipkarte einführen zu wollen. Dies überrascht, da für die Speicherung der gesetzlich zugelassenen Daten eine Magnetstreifenkarte — vergleichbar mit der Scheckkarte — völlig ausreichende Kapazitäten bieten würde. Chipkarten aber haben im Gegensatz dazu eine so hohe Speicherkapazität, daß es geradezu widersinnig erscheint, auf ihnen lediglich einige Grunddaten und nicht etwa auch Verschreibungen, Befunde, Berichte, Gutachten, Krankengeschichten etc. zu speichern. Überdies sind sie nur für den lesbar, der entsprechend technisch ausgestattet und qualifiziert ist, also in der Regel nicht für den betroffenen Versicherten. Wechselt z. B. künftig ein Versicherter seinen Arzt, läuft er Gefahr, daß dieser von Anfang an über die Chipkarte mehr über ihn weiß als er selbst und als ihm unter Umständen lieb sein kann, etwa im Fall eines Arztwechsels mit dem Ziel, eine zweite von der ersten unbeeinflußte Diagnose gestellt zu bekommen.

Das ungute Gefühl angesichts der Chipkarte schlägt vollends in offenen Argwohn um, wenn man sich mit dem AIM-Programm der Europäischen Gemeinschaften beschäftigt (AIM: Advanced Informations in Medicine), das mit erheblichen Geldmitteln neben anderen Methoden zur Rationalisierung des Gesundheitswesens auch die Entwicklung einer Patientendatenkarte vorantreibt, die auch medizinische Daten speichern soll. In Frankreich, Italien und Belgien werden denn auch schon Chipkarten getestet, die Gesundheitsdaten bis hin zu kompletten Krankengeschichten speichern.

Jüngst ist in der Presse auf die Gefahren und auf die eindeutige, dem entgegenstehende Gesetzeslage, aber auch auf die Möglichkeit hingewiesen worden, über die gesetzliche Krankenversichertenkarte hinaus eine „freiwillige Gesundheitskarte" einzuführen, auf der mit einer besonderen Einwilligung des Betroffenen auch Gesundheitsdaten gespeichert werden dürften. Dann müsse kein Patient mehr befürchten, daß über seine Krankenversichertenkarte, also die Pflichtkarte, ärztliche Daten unzulässigerweise z. B. an die Krankenkasse gelangten. Letzteres ist eine fragwürdige Begründung, sollte man doch davon ausgehen dürfen, daß auch ohnedies die an der Gesundheitsversorgung beteiligten Stellen bereit sind, das geltende Gesetz zu respektieren. Ohnehin ist es Ziel der Verbände der Kassen und Kassenärzte, die Gesundheitsdaten auf der Krankenversichertenkarte selbst zu speichern, d. h. deren Speicherkapazität unter Anwendung der Chiptechnik so zu erweitern, daß sie zugleich Funktionen als Informationsträger für medizinische Daten erfüllen kann. Es ist damit zu rechnen, daß der Druck auf den Gesetzgeber wachsen wird, § 291 SGB V diesen Vorstellungen anzupassen.

Aber auch ohne Gesetzesänderung ist die Gefahr offensichtlich, daß ein indirekter Zwang ausgeübt werden kann, sich mit der Ausstellung einer zusätzlichen Gesundheitskarte bzw. der Speicherung von Gesundheitsdaten auf der Krankenversichertenkarte einverstanden zu erklären. Kann dies nicht verhindert werden — und genau damit muß gerechnet werden —, laufen sowohl der gesetzliche Datenkatalog für die Krankenversichertenkarte als auch die angebliche Freiwilligkeit der „Gesundheitskarte" leer. Die Folge wird sein, daß die Stellen, die technisch hierfür ausgerüstet sind — und dies werden alle Sozialleistungsträger, Krankenhäuser, Ärzte und viele Arbeitgeber sein —, die Gesundheitsdaten jedes einzelnen auf Verlangen sofort verfügbar haben, speichern und untereinander austauschen. Das Arztgeheimnis und das informationelle Selbstbestimmungsrecht der Patienten/Versicherten wird dann der Vergangenheit angehören. Es wird möglich sein, über den Einzelnen „Gesundheitsprofile" zu erstellen. Ich verkenne nicht, daß die steigenden Kosten mehr Effizienz im Gesundheitsbereich verlangen, bezweifle aber, ob es der richtige Weg sein kann, sie über Verdatung, Kontrolle und Kürzung der Grundrechte der Patienten/Versicherten erreichen zu wollen. Könnte dies nicht lediglich dem Versuch dienen, zu verschleiern, daß man sich nicht traut, an die eigentlichen kostentreibenden Faktoren heranzugehen?

Die Chipkarte soll eingeführt werden, ohne daß die zuvor erforderliche öffentliche Diskussion geführt und die gebotene gesetzgeberische Entscheidung getroffen worden wäre. Schon dies muß bedenklich stimmen, wie immer man zu einzelnen Problemaspekten stehen mag.

2.6.3 Datenverarbeitung im Rahmen des Methadon-Programms

Die viel diskutierte Versorgung von Rauschgiftabhängigen mit der Ersatzdroge Methadon wirft neben anderen auch datenschutzrechtliche Probleme auf. Im Juni 1989 beschloß der Senat ein Programm zum Einsatz von Methadon zur Substitution von Drogenabhängigen bei bestimmten Indikationen (Schwangerschaft, schwere Krankheit oder etwa AIDS). Im Januar 1990 einigten sich der Senator für Gesundheit, die Ärztekammer und die Kassenärztliche Vereinigung Bremen auf eine gemeinsame Empfehlung, die die Voraussetzungen und das Verfahren für die ärztliche Verschreibung von Methadon durch die sich beteiligenden Ärzte regelte. Es sollte eine Kommission gebildet werden, die in den Fällen, die über die „unbestrittenen" Indikationen hinausgehen, den einzelnen Arzt bzw. den Senator für Gesundheit beraten sollte. Die Krankenkassen weigerten sich zunächst, die Kosten zu tragen. Deshalb war das Amt für Soziale Dienste einziger Kostenträger. Regelungsbedürftig war, inwieweit personenbezogene Daten der betroffenen Drogenabhängigen an den Senator für Gesundheit, an die Kommission sowie an den Kostenträger übermittelt werden mußten oder durften. Nach § 203 StGB waren die Ärzte dazu nur aufgrund der Einwilligung ihrer Patienten bzw. einer gesetzlichen Regelung befugt. Im März 1991 endlich legte mir der Senator für

Gesundheit den Entwurf einer Verfahrensordnung vor, die folgende Datenübermittlungen vorsah:

- Anonymisierte Meldung eines Substitutionsfalles durch den Arzt an den Senator für Gesundheit bzw. an die Kommission,
- personenbezogene Übermittlung der Grunddaten des einzelnen Patienten und der Indikation an die Arbeitsgruppe für Drogenabhängige des Amtes für Soziale Dienste als Kostenträger,
- anonymisierte Bestätigung des Senators für Gesundheit an das Amt für Soziale Dienste, daß die Substitution medizinisch indiziert sei.

Alle Übermittlungen sind mit dem Namen des Arztes und einer fortlaufenden Nummer versehen, die dieser dem einzelnen Patienten gegeben hat. Auf diese Weise können der Arzt selbst sowie der Kostenträger, nicht aber der Senator für Gesundheit oder die Kommission, den Personenbezug herstellen.

Diesem Verfahren konnte ich grundsätzlich zustimmen, da die Datenübermittlung des Arztes an den Kostenträger durch die Mitwirkungspflicht des Antragstellers auf Sozialleistungen (§ 60 SGB I) legitimiert und im übrigen die Anonymität des Betroffenen gewährleistet war.

Nunmehr haben sich die gesetzlichen Krankenkassen bereiterklärt, für ihre Versicherten die Kosten eines Teils der ärztlich indizierten Methadon-Substitution (die sog. „unbestrittenen Fälle") zu übernehmen. Es bestehen keine datenschutzrechtlichen Bedenken dagegen, daß die behandelnden Ärzte im gesetzlich vorgesehenen Rahmen der §§ 294, 295 SGB V personenbezogene Daten der Substituierten zu Abrechnungszwecken an die Kassenärztlichen Vereinigungen übermitteln.

Jetzt will aber der Senator für Gesundheit die bislang von ihm gespeicherten Daten der einzelnen Substituierten (jedenfalls soweit es sich um die sog. „unbestrittenen Fälle" handelt) insgesamt an die Kassenärztliche Vereinigung übermitteln, die ihrerseits den Personenbezug herstellen will. Er meint, daß es sich nicht um personenbezogene Daten handele, da er selbst einen Personenbezug nicht herstellen könne. Dem habe ich widersprochen. Nach § 2 Abs. 1 BrDSG sind auch Einzelangaben über die Verhältnisse bestimmbarer Personen personenbezogene Daten. Da die Kassenärztliche Vereinigung die Daten nach Empfang deanonymisieren will, kann sie die betroffenen Personen bestimmen. Folglich handelt es sich um personenbezogene Daten, für deren Übermittlung die erforderliche Rechtsgrundlage fehlt.

Zudem habe ich bei dieser Gelegenheit erfahren, daß die Krankenkassen über die Versichertendaten hinaus, zu deren Übermittlung an die Kassenärztliche Vereinigung die Ärzte durch § 295 SGB V befugt und verpflichtet sind, weitere personenbezogene Patientendaten direkt bei den an der Substitution beteiligten Ärzten bereits jetzt erheben bzw. künftig erheben wollen. Grundlagen seien die Richtlinien über neue Untersuchungs- und Behandlungsmethoden vom 01. 10. 1991. Ich habe darum gebeten, mir diese sogenannten NUB-Richtlinien zur Verfügung zu stellen, zugleich aber betont, daß der ihnen zugrundeliegende § 135 SGB V eine Befugnis für Datenübermittlungen nicht vorsehe. Ich habe die Kassenärztliche Vereinigung von meinen Bedenken in Kenntnis gesetzt.

Ich erwarte, daß die von mir kritisierten Übermittlungen bzw. Datenerhebungen unterbleiben.

2.6.4 Erforschung der Ursachen für den Tod von Drogensüchtigen

Angesichts des Anstiegs der Zahl der Drogentoten ist es sicherlich sinnvoll, die Ursachen und Umstände von durch Drogen bedingten Todesfällen zu erforschen. Es ist möglich, Forschungsprojekte zu konzipieren, die die Persönlichkeitsrechte betroffener lebender oder verstorbener Personen respektieren sowie die beruflichen Schweigepflichten von Ärzten und Beratern und die Forschungsklauseln in den Datenschutzgesetzen beachten. Zuweilen fällt es aber deshalb schwer, ein positives Votum zu einem Projekt abzugeben, weil seine datenschutzrechtliche Vorbereitung mangelhaft ist. Mit einer solchen unerfreulichen Situation wurden der Berliner, der Hamburger Landesbeauftragte für den Datenschutz und ich durch ein Forschungsinstitut im Falle von dessen Drogenmortalitäts- und Drogennotfallstudie konfrontiert.

Das Institut bereitete gemeinsam mit der Abteilung für Rechtsmedizin des Hauptgesundheitsamtes Bremen und den entsprechenden Stellen in Hamburg und Berlin eine Vor- und eine Hauptstudie zur Untersuchung von Drogentodesfällen in den drei Städten vor. Die Landesbeauftragten für den Datenschutz wurden erst beteiligt, als die Finanzierungsentscheidung des zuständigen Bundesministeriums, das eine positive datenschutzrechtliche Beurteilung voraussetzte, unmittelbar bevorstand. Zudem sollte sofort mit der Vorstudie begonnen werden. Weder wurde eine vollständige Forschungskonzeption noch ein ausformuliertes Datenschutzkonzept vorgelegt. So kam ein schwieriges datenschutzrechtliches Problem nach dem anderen zum Vorschein, das jeweils unter Zeitdruck im Sinne der Betreiber gelöst werden sollte. Ein Ende ist noch nicht absehbar.

Zu klären war etwa, ob schweigepflichtige Mitarbeiter von Drogenberatungsstellen über ihre verstorbenen Klienten Auskunft geben dürfen. Auch Verstorbene sind durch das Beratungsgeheimnis geschützt, § 203 Abs. 4 StGB. Eine Befugnis der Mitarbeiter zu dessen Durchbrechung kann weder über eine gesetzliche Erlaubnis noch über die unterstellte Einwilligung des Verstorbenen noch durch die Einwilligung von Angehörigen legitimiert werden. Es gelang dann aber doch, ein Verfahren zu vereinbaren, das einen Ausweg aus dem Dilemma bietet. Danach dürfen die Berater einem im Datenschutzkonzept namentlich aufgeführten Mitarbeiter des Projekts auf dessen Einzelfallanfrage über einen verstorbenen Klienten Auskunft geben. Die Daten werden an Ort und Stelle in einen Erhebungsbogen eingetragen, der nicht mit dem Namen des Betroffenen, sondern mit einer Code-Nummer versehen ist, die nur in der Abteilung für Rechtsmedizin entschlüsselt werden kann. Die statistische Auswertung für das Projekt erfolgt ausschließlich mit Hilfe des codierten Erhebungsbogens. Es gelang gleichfalls, datenschutzgerechte Lösungen für die Ausgestaltung des Erhebungsbogens und für die Anschreiben an die Angehörigen mit der Bitte um ein Interview zu entwickeln.

Neue Schwierigkeiten tauchten auf, als auch „Drogennotfälle" in das Projekt einbezogen wurden mit dem Ziel, die Umstände der Einlieferung von Drogenabhängigen in Notaufnahmestationen von Krankenhäusern zu erhellen. Hier wurde klargestellt, daß die Betroffenen zunächst vom behandelnden Arzt angesprochen werden müssen, und es wurde geklärt, unter welchen Voraussetzungen Unterlagen der Krankenhäuser bzw. der Rettungsdienste herangezogen werden dürfen. In diesem Zusammenhang habe ich die beteiligten Krankenhäuser darauf hingewiesen, daß § 7 Abs. 2 Sätze 2-4 KHDSG sie verpflichtet, die Übermittlung von Patientendaten an ein Forschungsinstitut dem Senator für Gesundheit anzuzeigen, bestimmte Aufzeichnungen vorzunehmen und ihre betrieblichen Datenschutzbeauftragten zu beteiligen.

Inzwischen bin ich vom nachträglich eingeschalteten Bremer Institut für Präventionsforschung und Sozialmedizin (BIPS), von Krankenhäusern und vom Senator für Inneres wegen neuer Teilaspekte des sich weiter entwickelnden Projekts eingeschaltet worden. So soll den „Drogennotfällen" Blut abgenommen und sollen „Polizeiregister" eingesehen werden. Ich werde mich in Abstimmung mit den anderen beteiligten Datenschutzbeauftragten weiterhin um einen datenschutzgerechten Ablauf des Forschungsprojekts bemühen.

2.6.5 Medizinische Forschung und AIDS-Bekämpfung/KLIMACS

Der Bundesminister für Gesundheit fördert im Rahmen des Sofortprogramms der Bundesregierung zur AIDS-Bekämpfung ein Projekt, in dessen Rahmen ein Forschungsinstitut in 24 Krankenhäusern, darunter im ZKH St.-Jürgen-Str, die computergestützte Krankendokumentation KLIMACS installiert. Es liegt auf der Hand, daß die automatisierte Verarbeitung der Daten von an AIDS erkrankten Patienten besonders sorgfältiger technischer und organisatorischer Vorkehrungen zum Schutz der Betroffenen vor einer Verletzung ihrer Persönlichkeitsrechte bedarf. Demzufolge hat ein Arbeitskreis der Datenschutzbeauftragten Anforderungen an die Verbesserung der „Datenschutzanforderungen an KLIMACS und seine Anwender" erarbeitet. Das Bundesministerium für Gesundheit hatte den Einsatz des Programms in den einzelnen Kliniken von der vorherigen Beratung und Kontrolle des jeweils zuständigen Landesbeauftragten für den Datenschutz abhängig gemacht.

Zwischen den Unterlagen des Forschungsinstituts, einer Stellungnahme des Bundesministers für Gesundheit und meinen eigenen Feststellungen im Verlauf meiner Beratung des ZKH St.-Jürgen-Str. ergaben sich Widersprüche. Nach Aussage des Bundesministers für Gesundheit ist KLIMACS so konzipiert, daß es nur der ärztlichen Versorgung einzelner AIDS-Patienten dienen kann; es speichere nur

die jeweiligen individuellen Labordaten und enthalte ein Programm für Arztbriefe. Die Zusammenschau von Labordaten mehrerer Patienten, die für die Forschung erforderlich sei, sei nicht möglich. Dem stehen sowohl die Erfahrungen anderer Landesdatenschutzbeauftragter mit bereits installierten PC mit dem Programm KLIMACS als auch der Abschnitt „Datenanalyse" des Handbuchs des Forschungsinstituts „KLIMACS-Version 2.0" gegenüber. Zudem erklärte mir der zuständige Arzt des ZKH St.-Jürgen-Str., es sei sehr wohl beabsichtigt, die Daten mehrerer Patienten miteinander zu verknüpfen, um daraus Erkenntnisse für die AIDS-Therapie zu gewinnen. Die Aussage des Bundesministers für Gesundheit ist auch deshalb wenig überzeugend, weil gerade in der Verknüpfung und Auswertung verschiedener gespeicherter Daten die spezifische Qualität der EDV liegt.

Ich habe daraufhin meine Zustimmung zum Einsatz von KLIMACS für Forschungszwecke verweigert, solange dieser Widerspruch nicht geklärt ist. Ich habe dies auch damit begründet, daß der Bundesminister für Gesundheit außerdem behauptet hat, das Programm ermögliche es nicht, die Identifikationsdaten der einzelnen Patienten getrennt von den Stamm- und Verlaufsdaten zu speichern, eine Trennung, die aber § 7 Abs. 4 Bremisches KHDSG verlangt. Schließlich habe ich noch unzureichende Aussagen zur Verschlüsselung und zum Löschen der Daten bemängelt. Hiervon habe ich den Bundesbeauftragten für den Datenschutz und den Senator für Gesundheit als zuständige Aufsichtsbehörde in Kenntnis gesetzt. Einem Schreiben des Bundesbeauftragten für den Datenschutz an den Bundesminister für Gesundheit entnehme ich, daß er meine datenschutzrechtlichen Bedenken teilt.

2.6.6 Datenschutz im öffentlichen Gesundheitsdienst

Der Senat hatte in seiner Stellungnahme zu meinem 12. Jahresbericht mitgeteilt, der Senator für Gesundheit habe begonnen, den Entwurf eines Gesetzes über den öffentlichen Gesundheitsdienst zu erarbeiten, in das auch datenschutzrechtliche Regelungen aufgenommen werden sollten. Nach Abschluß der Vorarbeiten werde er mich daran beteiligen (vgl. 13. Jahresbericht, S. 38). Bislang bin ich an dem Vorhaben nicht beteiligt worden, so daß ich davon ausgehe, daß — aus welchen Gründen auch immer — die Vorarbeiten nicht abgeschlossen sind. Ich halte nach wie vor die Verabschiedung eines Gesetzes mit einer genauen Aufgabenzuweisung und normenklaren Befugnissen zur Datenverarbeitung für die Gesundheitsämter für dringlich.

2.7 Umweltschutz und Stadtentwicklung

2.7.1 Verarbeitung von Abwasserdaten

Kleingärtner haben sich an mich gewandt und sich darüber beschwert, daß das Amt für Stadtentwässerung und Abfallwirtschaft (ASA) die zum Zwecke der Organisation der kommunalen Abwasserbeseitigung, insbesondere einer regelmäßigen Entleerung der Schmutzwassersammelgruben und Kleinkläranlagen, erhobenen und gespeicherten Wasserverbrauchs- und Fäkaliendaten an das Bauordnungsamt übermittelt. Sie befürchteten, daß diese Daten zur Prüfung der Wohnberechtigung verwendet werden.

Nach § 18 Abs. 5 Entwässerungsortsgesetz dürfen bei begründetem Verdacht eines Verstoßes gegen bauordnungsrechtliche Vorschriften im Zusammenhang mit der Grundstücksentwässerung an Bauordnungsbehörden Daten übermittelt werden. Ich habe das ASA darauf hingewiesen, daß diese Vorschrift der Behörde eine Ermessensentscheidung einräumt.

Das ASA hat mir inzwischen mündlich zugesagt, Daten der Überlassungspflichtigen nur noch eingeschränkt unter strikter Beachtung des § 18 Abs. 5 Entwässerungsortsgesetz und generell ohne die Wasserverbrauchs- und Fäkalienmengen an die Bauordnungsbehörde zu übermitteln.

2.7.2 Mangelnde Datensicherheit in der Registratur der Umweltbehörde

Ich habe anläßlich einer Prüfung festgestellt, daß beim Senator für Umweltschutz und Stadtentwicklung die Vorschriften zur Datensicherung nicht eingehalten werden. Die Registratur der senatorischen Dienststelle befindet sich in unverschlossenen Aktenschränken auf dem Flur des Dienstgebäudes Am Wall 177 (II. Stock). Sowohl das Dienstgebäude als auch der Flur sind allgemein zugänglich. In den unverschlossenen Aktenschränken werden u. a. komplette Bußgeldakten, Ordnungswidrigkeitenanzeigen der Behörde gegenüber dem Stadtamt sowie Anträge von Privatpersonen auf Befreiung von der Baumschutzverordnung aufbewahrt. Sämtliche Akten enthalten personenbezogene Daten.

Ich habe dem Senator für Umweltschutz und Stadtentwicklung dargelegt, daß diese Art der Aufbewahrung von Akten mit personenbezogenen Daten gegen die Vorschriften zur Datensicherung verstößt. Eine Antwort steht noch aus.

2.7.3 Öffentliche Bekanntmachung von Baumschutzbefreiungen

Aus einem Beirat kam der Vorschlag, vor der Entscheidung über das Fällen von geschützten Bäumen (Baumschutzbefreiungen) dieses künftig mindestens zwei Monate vor der Freigabe öffentlich bekannt zu machen.

Ich habe darauf hingewiesen, daß durch die Veröffentlichung von beabsichtigten Baumschutzbefreiungen als amtliche Bekanntmachungen personenbezogene Daten übermittelt werden, soweit es sich bei den Antragstellern um private Grundstückseigentümer handelt. Die damit zusammenhängende Einschränkung des informationellen Selbstbestimmungsrechts wäre nur auf einer verfassungsgemäßen Rechtsgrundlage zulässig.

Anders verhält es sich jedoch bei Befreiungsverfahren, in denen ausschließlich Gebietskörperschaften als Grundstückseigentümer in Frage kommen. Soweit Baumschutzbefreiungen auf öffentlichen Flächen vorgesehen sind, wäre gegen eine amtliche Bekanntmachung in diesem Zusammenhang nichts einzuwenden.

2.8 Wirtschaft, Technologie und Außenhandel

2.8.1 Vernetzte Datenverarbeitung für das Wirtschaftspolitische Aktionsprogramm

Die geplante Realisierung des DV-Rahmenkonzeptes zur Umsetzung und zur Kontrolle des Wirtschaftsstrukturpolitischen Aktionsprogramms (WAP) (vgl. 13. Jahresbericht, S. 44), ist im Berichtszeitraum durch die Entwicklung von fachlichen Feinkonzepten für die Bereiche der integrierten Antragsbearbeitung und des Haushalts-, Planungs- und Kontrollsystems konkretisiert worden.

Diese Feinkonzepte bestätigen sehr differenziert durch die Darstellung von Masken mit entsprechenden Eingabefeldern meine Aussage zum Grobkonzept im Vorjahr, daß sehr sensible, personenbezogene Daten verarbeitet werden. Diese Daten werden zum Teil beim Betroffenen, zum Teil über angeforderte Stellungnahmen von öffentlichen und nichtöffentlichen Stellen erhoben (z. B. Gewerbeaufsichtsämter, Arbeitsämter, Banken etc.).

Es ist eine Vernetzung von 49 PC-Arbeitsplätzen vorgesehen, die bereits beim ADV-Ausschuß beantragt worden ist.

Die Realisierung des DV-Rahmenkonzeptes zur Umsetzung und Kontrolle des WAP ist nur unter folgenden Voraussetzungen zulässig:

- Ich halte weiterhin den Erlaß einer ausreichenden, bereichsspezifischen Rechtsnorm für die Wirtschaftsförderung zur Regelung der Datenerhebung, der Datenübermittlung und sonstiger Verarbeitungsschritte für erforderlich, da ich weiterhin im Gegensatz zur senatorischen Behörde (vgl. Stellungnahme des Senats zum 13. Jahresbericht) nicht von der Freiwilligkeit der Zustimmung des Antragstellers in die Datenverarbeitung ausgehen kann.

- Es liegt mir immer noch kein Datenschutzkonzept vor, in dem technische und organisatorische Maßnahmen gem. § 6 BrDSG beschrieben werden. Entsprechend ist in der im Feinkonzept dargestellten Anwendungslösung keine ausreichende technische Umsetzung von Datenschutzmaßnahmen vorgesehen. Im Rahmen der software-technischen Merkmale wird lediglich von Datenschutzmaßnahmen über Paßwortschutz ausgegangen, laut der letzten Vorlage für die Sitzung des ADV-Ausschusses soll die Gewährleistung von Datenschutz und Datensicherheit „. . . durch die volle Ausschöpfung der Sicherheitsfunktionalitäten des Netzwerk-Betriebssystems garantiert" werden. Diese Garantie ist ohne zusätzliche technische und organisatorische Maßnahmen nicht möglich. Deshalb ist die Schaffung eines umfassenden und verbindlichen Datenschutzkonzeptes erforderlich, das alle Komponenten (Arbeitsplatz-PC, Vernetzung, Datenbankzugang, Telekommunikation, Datenübermittlung an Dritte, Organisation des Paßwortschutzes und der Systemverwaltung) enthält und die Wechselwirkungen zwischen den verschiedenen Ebenen berücksichtigt.

- Es ist die Beschaffung eines relationalen Datenbanksystems für sieben Arbeitsplätze vorgesehen. Es soll eine Differenzierung auf drei Zugriffsebenen

erfolgen, die von der Nutzung einer begrenzten Anzahl von Datenbankoperationen bis zur Erstellung komplexer Abfragen reicht. Das geplante Datenbankverwaltungssystem SQL ermöglicht durch die Erzeugung sogenannter logischer Sichten auf die in der physischen Datenbank enthaltenen Grundtabellen vielfältige Verknüpfungen und Auswertungen der dort gespeicherten Grunddaten. Das unbefugte Auswerten muß u. a. auch durch geeignete technische Maßnahmen verhindert werden.

— Im Rahmen der Entwicklung des Datenmodells der integrierten Sachbearbeitung wird sichergestellt, daß Daten aus der zentralen Datenhaltung bereichs- und anwendungsübergreifend genutzt werden können. Es fehlt eine differenzierte Regelung für die Gewährleistung der Einhaltung des Zweckbindungsprinzips, die ich schon in meinem letzten Jahresbericht gefordert habe. In diesem Zusammenhang halte ich es für erforderlich, sowohl den Austausch von Daten mit anderen Behörden als auch mit Gesellschaften und Kammern über öffentliche Netze (entsprechende Schnittstellen sind vorgesehen) sowie sonstige regelmäßige Datenübermittlungen auf eine gesetzliche Grundlage zu stellen und ggf. entsprechende technische Restriktionen zu schaffen.

Im Herbst des Berichtsjahres wurde die hier skizzierte datenschutzrechtliche Problematik mit der senatorischen Behörde erörtert, dabei sind mir entsprechende weitergehende Auskünfte zugesagt worden. Dies erfolgte bis zum Redaktionsschluß nicht. Ich wurde lediglich vom ADV-Ausschuß aufgefordert, bis Jahresende etwaige Einwände zu formulieren, die allerdings beim Senator für Wirtschaft, Technologie und Außenhandel bereits bekannt waren und bisher unberücksichtigt geblieben sind. Ich habe mich in dem o. g. Sinn beim ADV-Ausschuß geäußert.

2.8.2 Änderung der Gewerbeordnung

Seit einigen Jahren ist die Novellierung der Gewerbeordnung auf Grund der Vorgaben des Bundesverfassungsgerichts zum Volkszählungsurteil überfällig. Nunmehr hat der Bundesminister für Wirtschaft in Zusammenarbeit mit den Gewerbereferenten der Länder einen neuen Entwurf zur Änderung der Gewerbeordnung erarbeitet. Dieser Entwurf enthält bereichsspezifische Bestimmungen über die Erhebung und Verarbeitung von personenbezogenen Daten.

Ich prüfe derzeit, ob und wie die Datenerhebung und die sonstige Datenverarbeitung bei den Detektiven, die nach deutschem Recht einer Gewerbeerlaubnis bedürfen, transparenter und damit nachprüfbarer gestaltet werden kann. Ich stehe auf dem Standpunkt, daß es mit unserer Rechtsordnung nicht zu vereinbaren ist, daß der Staat z. B. für Pfandleiher und Wertsachenbewacher bestimmte Zuverlässigkeitsvoraussetzungen, Buchführungs- und Dokumentationspflichten und Eignungen vorschreibt, dieses für Detektive aber nicht regelt. Ich halte Regelungen aber für unerläßlich, weil Detektive bei Recherchen in besonderem Maße in das informationelle Selbstbestimmungsrecht eindringen. Dabei werden oftmals geheime Informationsbeschaffungsmethoden angewendet, die zum Teil über das hinausgehen, was der Kriminalpolizei zugestanden wird. Wie für die Polizei muß der Gesetzgeber auch für die Befugnisse der Detektive Grenzen für die Art der Informationsbeschaffung setzen. Der Gesetzgeber ist aufgefordert, Rechtsvorschriften über den Erlaubnisumfang für das Tätigwerden, über eine Berufsordnung für die Ausbildung und über die Dokumentationspflichten bezüglich Auftraggeber, Auskunftspersonen bzw. eingesetzte technische Mittel und Betroffene zu schaffen. Diese Rechtsvorschriften könnten in der Gewerbeordnung aufgenommen werden und müßten Kontrollrechte der Aufsichtsbehörden enthalten.

2.8.3 Bremisches Energiegesetz

Auf Nachfrage bin ich über den Entwurf eines Bremischen Energiegesetzes informiert worden. Nach dem Gesetzentwurf sollte für jede Wohnung, die sich mittelbar oder unmittelbar im Eigentum der Kommunen Bremen und Bremerhaven befindet, ein Energiepaß eingeführt werden. Dieser Energiepaß sollte neben baulichen und energietechnischen Angaben auch die Verbrauchsangaben des jeweiligen Mieters über Strom, Brennstoffe, Nah- und Fernwärme und die Betriebskosten der Anlagen enthalten. Aus diesen Angaben können sowohl das individuelle Wärmebedürfnis, das Hygieneverhalten, die zeitweise Nichtnutzung der Wohnung als auch das unerwünschte Energieverhalten entnommen werden. Dabei war vorgesehen, diese Daten vom Eigentümer der Wohnung erheben zu lassen, der damit ebenfalls einen Einblick in die Lebensgewohnheiten seines Mieters erhalten hätte. Darüber hinaus sollten auch zukünftige Mieter oder Mietinteres-

senten Einblick in diesen Energiepaß erhalten. Eine solch weite Öffnung der personenbezogenen Daten des Energieverbrauchers hielt ich für unverhältnismäßig, da die erhofften Energiedaten sehr stark von eben den individuellen Lebensgewohnheiten des einzelnen Nutzers abhängig sind und nicht auf den Energieverbrauch des zukünftigen Nutzers übertragen werden können.

In der weiteren Beratung konnte erreicht werden, daß Verbrauchsdaten für den Energiepaß nicht personenbezogen erhoben werden und demzufolge auch nicht übermittelt oder für andere Zwecke genutzt werden können. Der Energiepaß wird neben den technischen Daten der Wohnung sogenannte Energiekennzahlen enthalten, die aus Musterwohnungen gewonnen werden. Entsprechend sind die Auskunftspflichten der Energieversorgungsunternehmen und der Hauseigentümer für Zwecke der Ausarbeitung und Fortschreibung eines Landesenergieprogramms zu gestalten. Die Auskünfte zur Enwicklung eines Energieeinsparkonzepts und die Grunddaten zur Ausarbeitung einer Verordnung zur Führung eines Energiepasses sind festzulegen und ein Landesenergiestatistikgesetz ist zu erarbeiten.

Durch die Beratungen sind im neuen Energiegesetz die Ziele des sinnvollen Einsatzes der Energie und das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger in Einklang gebracht worden.

2.8.4 Bremisches Fischereigesetz

An den Arbeiten zum neuen Bremischen Fischereigesetz wurde ich nicht beteiligt, von dem Gesetzesvorhaben erhielt ich kurz vor der parlamentarischen Verabschiedung aus der Presse Kenntnis.

Der Gedanke liegt nahe, bei dieser Rechtsmaterie könnten sich keine besonderen datenschutzrechtlichen Probleme ergeben und deshalb reiche das Bremische Datenschutzgesetz aus. Eine Durchsicht des Gesetzes ergibt jedoch, daß vielfältige Daten erhoben und weiter verarbeitet werden sollen. Dieses gilt nicht nur für die Fischereiprüfung durch den Fischereiverband zur Erlangung des Fischereischeines, sondern auch bei der Regelung der Ausübung, Nutzung und Verpachtung der Fischereirechte. Des weiteren regelt das Gesetz die Rechte und Pflichten der Fischereivereinigungen und ihres Verbandes einschließlich der Sanktionsmaßnahmen bei Verstößen von Mitgliedern gegen dieses Gesetz oder das Tierschutzgesetz. Datenschutzrechtliche Probleme erwachsen in den Fällen, in denen z. B. der Fischereischein versagt oder entzogen werden soll. Das Gesetz regelt nicht präzise und normenklar in welchen Fällen, in welchem Umfang und von wem z. B. Verstöße gegen das Bremische Fischereigesetz oder gegen andere Tierschutzbestimmungen zu melden sind. Die jetzt getroffenen Regelungen überlassen den Anwendern ein weites Interpretationsfeld. Auch ist nicht präzise geregelt, wer welche Daten zur Vorbereitung einer Versagung oder Entziehung eines Fischereischeines erheben und speichern darf.

Auch die Verwendung der nach dem Entwurf des Justizmitteilungsgesetzes zu übermittelnden Daten wäre im Bremischen Fischereigesetz zu regeln gewesen.

2.9 Häfen, Schiffahrt und Verkehr

BREPOS (Bremen Port Operating System)

Das Projekt BREPOS für die Häfen Bremen und Bremerhaven wurde seit 1986 entwickelt. Durch das Projekt BREPOS (Stufe 1) sollen der Verkehrsablauf bei den Schiffsbewegungen in den Häfen, insbesondere bei den Schleusungen, verbessert und die Sicherheit der Kajenbelegung erhöht werden. Bei der Behandlung von Gefahrgütern während des Transports und der Lagerung sollen die Informationsflüße verbessert werden, um bei Schadensereignissen schnelle Informationen für Feuerwehr oder Wasserschutzpolizei bereitstellen zu können. Das Abrechnungsverfahren bei den Hafengebühren und den anderen Entgelten soll beschleunigt und rentabler gestaltet werden. Die für Planung und Kontrolle wichtigen statistischen Daten sollen jederzeit bereitstehen.

Die rechtlich notwendigen Grundlagen für die Datenverarbeitung wurden im Hafengesetz (1989), in der Hafenordnung (1990) und in der Hafengebührenordnung (1991) sowie im Brem. Brandschutzgesetz (1991) geschaffen. Jetzt fehlen noch die entsprechenden Datenübermittlungsverordnungen, um das Projekt (Stufe 1) umzusetzen.

Mit der Bereitstellung von Rechnerleistung soll die Datenbank bremische Häfen (dbh) beauftragt werden. Dem Senator für Häfen, Schiffahrt und Außenhandel

liegt z. Z. ein entsprechender Rahmenvertragsentwurf der „dbh" vor, der nach meiner Beratung nunmehr den Anforderungen des § 8 BrDSG Auftragsdatenverarbeitung entspricht.

2.10 Finanzen

2.10.1 Weitergabe der Steuerkarte im laufenden Kalenderjahr an den neuen Arbeitgeber

Durch Eingaben von Bürgern wurde ich erneut auf die Problematik der Abgabe der Steuerkarte eines Arbeitnehmers bei einem Arbeitgeberwechsel im laufenden Kalenderjahr aufmerksam gemacht. Nach der bisherigen Rechtslage wird den Arbeitnehmern zum Ende eines Jahres für das nächste Kalenderjahr von der Gemeinde eine Steuerkarte ausgestellt. Die Steuerkarte erhält die Steuerklasse aufgrund des Familienstandes und die Kinderfreibeträge entsprechend der Anzahl der Kinder unter 18 Jahren.

Bei einem Wechsel des Arbeitgebers erhält dieser durch die Vorlage der bereits verwendeten Steuerkarte von den Eintragungen des vorherigen Arbeitgebers Kenntnis. So kann er feststellen, ob der neue Mitarbeiter bei dem Bewerbungsgespräch z. B. sein bisheriges Einkommen korrekt angegeben oder evtl. „gepokert" hat. Diese Kenntnis könnte das neue Arbeitsverhältnis von vornherein belasten. Die Offenbarung dieser Daten bei dem neuen Arbeitgeber ist für das neue Arbeitsverhältnis nicht erforderlich.

Nach der derzeitigen Rechtslage kann der Arbeitnehmer, der seine bisherigen Einkünfte dem neuen Arbeitgeber nicht offenbaren will, sich nur eine weitere Steuerkarte ausstellen lassen. Diese ist dann eine Steuerkarte, die üblicherweise für ein weiteres Arbeitsverhältnis ausgestellt wird, sie wird grundsätzlich mit der Steuerklasse 6 ausgestellt und enthält keine steuerbegünstigenden Merkmale. Die Verwendung dieser Karte führt aufgrund der höheren Steuerabzüge zu einer erheblichen finanziellen Belastung der Arbeitnehmer.

Es muß ein Verfahren entwickelt werden, das den Arbeitnehmern ermöglicht, sich auf Wunsch eine Ersatzsteuerkarte ausstellen zu lassen, in der alle Freibeträge und die richtige Steuerklasse eingetragen sind, auf der aber weder der frühere Arbeitgeber noch die erzielten Einkünfte eingetragen sind.

2.10.2 Datenerhebung durch die Steuerfahndung

Von einer Bürgerin wurde ich darüber informiert, daß die Steuerfahndung in Ermittlungsfällen neben den Daten des verdächtigen Steuerpflichtigen auch die Daten des Ehepartners und der minderjährigen Kinder erhebt, selbst dann wenn zum Zeitpunkt des die Steuerpflicht auslösenden Sachverhalts die Ehe nicht bestand oder die Kinder nicht geboren waren. Des weiteren sollte die betreffende Steuerpflichtige Angaben zum Arbeitgeber des Ehepartners machen. Im Falle der Weigerung wollte die Steuerfahndung von Amts wegen Ermittlungen anstellen.

Weder die Abgabenordnung noch andere Steuergesetze erlauben eine derartige Datenerhebung. Deshalb habe ich die Oberfinanzdirektion Bremen von der Vorgehensweise der Steuerfahndung in Kenntnis gesetzt. Sie teilte mir daraufhin mit, daß sie die Steuerfahndung angewiesen habe, derartige Angaben nicht mehr abzuverlangen und die Erhebungsvordrucke entsprechend zu ändern.

2.11 Rechnungshof

2.11.1 Aufbewahrungsfristen von Verkehrsordnungswidrigkeiten für Zwecke der Rechnungsprüfung

Aus den Verwaltungsvorschriften zu § 71 Landeshaushaltsordnung (VV-LHO) ergibt sich eine Aufbewahrungsfrist von fünf Jahren für rechnungsbegründende Unterlagen, zu denen nach Auffassung des Rechnungshofs auch die kompletten Bußgeldakten gehörten. Der Senator für Inneres sieht sich außerstande, ohne Beachtung der Vorgaben des Rechnungshofs kürzere und insbesondere den gesetzlichen Tilgungsfristen entsprechende Aufbewahrungsfristen für die Bußgeldakten festzulegen (vgl. Pkt. 2.2.4.1 des Berichts).

Ich habe mich deshalb an den Rechnungshof gewandt und die Problematik erörtert. Der Rechnungshof vertritt die Ansicht, aufgrund der Rechtsprechung des Bundesverfassungsgerichts habe die Prüfkompetenz der Rechnungshöfe Verfassungsrang, so daß es ausschließlich dem Rechnungshof obliege, den Umfang und die Tiefe seiner Prüfungen festzulegen. Im Rahmen dieser Aufgabe obliege es ihm

auch, vollständige Bußgeldakten zu überprüfen. Dadurch solle festgestellt werden, ob die Bußgeldstelle Ordnungswidrigkeitenverfahren nach wirtschaftlichen Grundsätzen durchführt. Die gesetzlichen Tilgungsfristen für Verkehrsordnungswidrigkeiten, die auch für die Aufbewahrung der Bußgeldakten Wirkung entfalten, seien nach Auffassung des Rechnungshofes für diesen nicht beachtlich. Der Rechnungshof orientiere sich ausschließlich an der einvernehmlichen Regelung mit dem Senator für Finanzen, der in den VV-LHO die fünfjährige Aufbewahrungsfrist für rechnungsbegründende Unterlagen festgelegt habe. Außerdem sei die mit der Rechnungsprüfung verbundene Verarbeitung personenbezogener Daten und damit die Einschränkung des informationellen Selbstbestimmungsrechts der Betroffenen wegen der verfassungsrechtlichen Bedeutung dieser Aufgabe hinnehmbar.

Ich habe erklärt, daß ich weder den Umfang des Aktenmaterials noch die Intensität der Prüfung des Rechnungshofs beeinflußen wolle. Gleichwohl war darauf hinzuweisen, daß ein Interessenausgleich zwischen den Prüfrechten des Rechnungshofs und dem verfassungsrechtlich garantierten Recht auf informationelle Selbstbestimmung gefunden werden müsse. Dies könne nicht durch eine von der Exekutive erlassene Verwaltungsvorschrift allein festgelegt werden. Vielmehr sei der Rechnungshof gehalten, seine Prüfungen im Rahmen der gesetzlich vorgeschriebenen Löschungsfristen durchzuführen. Unabhängig davon, daß der Rechnungshof im Lande Bremen derzeit nur einfachgesetzlich abgesichert ist, bestehen auch nach Auffassung der am Gespräch beteiligten Vertreter des Rechnungshofs keine gesetzlich geregelten Aufbewahrungsbestimmungen.

Das Bremische Datenschutzgesetz sieht insoweit keinen Handlungsspielraum vor. Gemäß § 20 Abs. 3 BrDSG sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Wie im letzten Jahresbericht dargelegt, muß die Akte dann vernichtet werden, wenn das Bußgeld bezahlt ist und die ggf. damit verbundenen Punkte im Führerscheinregister beim KBA in Flensburg gelöscht worden sind. Da das Gesetz an das Recht der speichernden Stelle anknüpft, bleiben die Interessen des Rechnungshofes an einer längeren Aufbewahrung unberücksichtigt. Nach der derzeit geltenden Rechtslage ist die Straßenverkehrsbehörde somit verpflichtet, den Vorgang zu löschen bzw. die Akten zu vernichten. Hinter dieser klaren gesetzlichen Regelung treten die Verwaltungsvorschriften zur LHO, die eine Aufbewahrungsfrist für alle rechnungsrelevanten Vorgänge vorsehen, zurück. Eine spezialgesetzliche Rechtsgrundlage, die die allgemeinen Vorschriften des Bremischen Datenschutzgesetzes verdrängt, wurde mir nicht benannt.

Schließlich ist zu bemerken, daß das Bremische Datenschutzgesetz auch keine Möglichkeit vorsieht, die Akten durch Sperrung der Verwaltungsbehörde zu entziehen, die gesperrten Akten aber für Zwecke der Rechnungsprüfung für den Rechnungshof weiter aufzubewahren.

Gleichwohl habe ich Verständnis dafür geäußert, daß der Rechnungshof für umfassende Querschnittsprüfungen auch auf bereits abgeschlossene Akten zugreifen will. Es bleibt daher dem Gesetzgeber überlassen, durch entsprechende gesetzliche Regelungen z. B. in § 20 Abs. 2 Nr. 3 BrDSG und in der LHO oder im Rechnungshofgesetz die hierfür erforderlichen gesetzlichen Grundlagen zu schaffen.

Zu der eindeutigen Rechtslage tritt hinzu, daß der Senat in seiner Stellungnahme zum 8. Jahresbericht erklärt hat, der Übergangsbonus sei abgelaufen. Andererseits ist diese Konfliktlage erst jetzt zum Tragen gekommen. Ich bin daher bemüht, zusammen mit dem Rechnungshof und dem Senator für Finanzen nach rechtlich haltbaren Lösungen zu suchen. Weitere Klärung erhoffe ich mir von einem demnächst vereinbarten Gespräch mit dem Präsidenten des Rechnungshofs.

2.11.2 DV-Verfahren beim Rechnungshof

Der Rechnungshof hat beantragt, 14 PC für Zwecke der Rechnungsprüfung nach der Landeshaushaltsordnung und nach dem Gesetz über die Rechnungsprüfung im Lande Bremen zu beschaffen. Ich habe den Rechnungshof gem. § 27 BrDSG beraten.

Soweit die PC für das Berichtswesen bzw. für die Textverarbeitung verwendet werden sollen, habe ich empfohlen, im Sinne von § 6 BrDSG technische und organisatorische Sicherungsmaßnahmen zu treffen und insbesondere eine Sicherungssoftware einzusetzen, da die Feststellungen und Gutachten aus meiner Sicht stets personenbezogene oder zumindest personenbeziehbare Daten über Verantwort-

liche, Zahlungsempfänger, Steuerpflichtige u. a. enthalten. Des weiteren habe ich empfohlen, für den gesamten DV-Einsatz ein einheitliches Datenschutzkonzept zu entwickeln, um abschließende Regelungen über alle Datenverarbeitungsphasen und die angemessenen Schutzmaßnahmen zu treffen.

Darüber hinaus beabsichtigt der Rechnungshof einen Teil der beantragten PC mit Terminalemulationen auszustatten, um im Direktabrufverfahren beim Rechenzentrum der bremischen Verwaltung aus zentralen DV-Verfahren anderer Verwaltungsbereiche, wie z. B. PROSOZ, Daten abrufen zu können. Die Einrichtung eines solchen Verfahrens bedarf nicht nur im Hinblick auf § 14 BrDSG noch weiterer Erörterungen.

2.12 Rechenzentrum der bremischen Verwaltung, Auftragsdatenverarbeitung, Geräteverzeichnis und Register

2.12.1 Vorübergehende Auslagerung des RZ-Betriebes des RbV

Im Dienstgebäude des RbV wurde gesundheitsgefährdendes Spritzasbest festgestellt und daraufhin eine bauliche „Veränderungssperre" verfügt. Da die Asbestsanierung nicht parallel zum laufenden RZ-Betrieb durchgeführt werden kann, ist es erforderlich, den eigentlichen RZ-Betrieb des RbV (Rechner samt Bedienpersonal, Datenträgerarchiv, Druckbereich, Papierlager, Nachbehandlung, Teile der Arbeitsvorbereitung und die Annahme-/Ausgabestelle) vorübergehend, d. h. für ca. sechs bis acht Monate auszulagern und an anderer Stelle unterzubringen. Nach dem derzeitigen Planungsstand sollen die auszulagernden Betriebsteile des RbV im Mehrzweckhochhaus der Universität Bremen, im wesentlichen in den Räumlichkeiten des Universitätsrechenzentrums (Ebene 0/MZH), untergebracht werden.

Ich wurde im September des Berichtsjahres von der Auslagerungsnotwendigkeit in Kenntnis gesetzt und um beratende Unterstützung gebeten, der ich nachgekommen bin. Aus meiner Sicht habe ich gefordert, daß auch für die Zeit der Auslagerung des Rechenzentrumsbetriebes des RbV eine unter Datenschutzaspekten sichere und ordnungsgemäße Datenverarbeitung gewährleistet bleiben muß. Das bedeutet, daß die §§ 5 und 6 BrDSG (Datengeheimnis, technischorganisatorische Sicherungsmaßnahmen) beachtet werden und die Datenverarbeitung selbst den Vorgaben und Weisungen der Auftraggeber des RbV sowie den gesetzlichen Regelungen zur Amtsverschwiegenheit, zum Sozialgeheimnis, Steuer- und Statistikgeheimnis etc. entspricht. Die gefundene planerische Lösung wurde von mir als vorübergehende Möglichkeit grundsätzlich akzeptiert, ich habe jedoch einige zusätzliche Maßnahmen zur strikteren Trennung der beiden Rechenzentrumsbetriebe und zur Erhöhung der Zugangs- und Ablaufsicherung gefordert. Die Diskussion hierüber ist noch nicht abgeschlossen.

2.12.2 Datenverarbeitung im Auftrag öffentlicher Stellen

Zuletzt im 13. Jahresbericht (S. 47) habe ich gefordert, Musterverträge für die Vergabe von Datenverarbeitungsaufträgen durch öffentliche Stellen zu erarbeiten. Der Senat hat in seiner Stellungnahme zum 13. Jahresbericht erklärt, er habe die Senatskommission für das Personalwesen beauftragt, Muster für Ausschreibungen, Verträge und Datenschutzerklärungen zu erstellen. Nach Abstimmung mit den Ressorts sollten mir die Entwürfe zugeleitet werden, die ich bis heute nicht erhalten habe. Auch das Ergebnis der vom Senat angekündigten Prüfung der zentralen Vergabe der Aufträge steht noch aus.

Indes wurden im Berichtsjahr weiterhin Aufträge für Datenverarbeitung von verschiedenen Dienststellen der bremischen Verwaltung vergeben. Erneut waren Aufträge auch zur Bearbeitung von Steuerdaten und von Daten der Staatsanwaltschaft an nicht-öffentliche Stellen darunter. Wiederholt habe ich darauf hingewiesen, daß nach den AVV-BrDSG (Nr. 8.1.2) öffentliche Stellen an nicht-öffentliche Stellen keine Aufträge vergeben sollen, die die Verarbeitung von Daten betreffen, die einem Berufs- oder besonderem Amtsgeheimnis unterliegen. Dies gilt auch für die Datenerfassung als eine Phase der Datenverarbeitung. Daten über steuerliche Verhältnisse, strafbare Handlungen und Ordnungswidrigkeiten sollen deshalb ausschließlich von öffentlichen Stellen verarbeitet werden.

2.12.3 Führung von Geräteverzeichnissen

Gem. § 7 Abs. 3 BrDSG sind die datenverarbeitenden Stellen verpflichtet, ein Verzeichnis der Geräte, mit denen personenbezogene Daten automatisiert verarbeitet werden, zu führen. Das Verzeichnis enthält hard- und softwaretechnische

Merkmale sowie Angaben über die Anzahl und den Standort der Geräte. Gem. Nr. 7 der AVV zum BrDSG wird das Geräteverzeichnis zentral beim Rechenzentrum der bremischen Verwaltung geführt und verwaltet. Nach den Richtlinien für den Datenschutz am Arbeitsplatz liegt die Verantwortung für die Führung des Geräteverzeichnisses aber bei der speichernden Stelle.

Zentral beim RbV wird das Geräteverzeichnis bislang nicht geführt. Ich habe deshalb bei verschiedenen für die Führung verantwortlichen Stellen stichprobenartig geprüft, ob diese über ein Geräteverzeichnis verfügen. Als Ergebnis ist festzustellen, daß dies bei der überwiegenden Zahl der zwölf geprüften Stellen nicht der Fall war. Häufig war die Regelung, daß ein solches Verzeichnis zu führen ist, noch nicht einmal bekannt, bei anderen geprüften Stellen war das Geräteverzeichnis unvollständig. Da das zentrale Geräteverzeichnis beim RbV immer noch nicht eingerichtet ist, sind die datenverarbeitenden Stellen aufgefordert, die gesetzlichen Vorgaben des § 7 Abs. 3 BrDSG eigenverantwortlich zu erfüllen.

2.12.4 Neufassung der Dateienregisterverordnung

Seit der Änderung des Brem. Datenschutzgesetzes im Jahre 1987 ist die Neufassung der Dateienregisterverordnung überfällig. Darauf habe ich bereits mehrmals — zuletzt im 13. Jahresbericht (S. 48) — hingewiesen. Im Berichtsjahr wurde mit der Senatskommission für das Personalwesen, dem Rechenzentrum und dem Senator für Justiz und Verfassung die Neufassung der Dateienregisterverordnung beraten. Insbesondere wurden abschließend die Inhalte der Dateimeldungen und deren Wege von den speichernden Stellen zum Rechenzentrum und zu meiner Dienststelle festgelegt.

3. Nicht-öffentlicher Bereich

3.1 Fragen zum neuen Bundesdatenschutzgesetz

Das neue Bundesdatenschutzgesetz (BDSG) vom 20. Dez. 1990, das am 1. Juni 1991 in Kraft getreten ist, stand im Mittelpunkt der Beratungen der obersten Aufsichtsbehörden für den Datenschutz im Düsseldorfer Kreis. In diesem Zusammenhang fanden Anfang 1991 auch Erörterungen mit Datenschutzbeauftragen der Wirtschaft und Verbandsvertretern statt.

Ergebnis der Beratungen war, keine neuen, bundesweit einheitlichen Richtlinien zum BDSG zu erarbeiten. Der Düsseldorfer Kreis hat in zwei Sitzungen u. a. Auslegungs- und Anwendungsfragen neuer oder neugefaßter Rechtsvorschriften des BDSG erörtert. Folgende Rechtsprobleme wurden diskutiert:

— **Der Begriff der Geschäftsmäßigkeit (§ 1 Abs.2 Nr.3 BDSG)**

Es gab Bestrebungen den Begriff der Geschäftsmäßigkeit in dem Sinne auszulegen, daß von dem BDSG nicht mehr gemeinnützige, vereinsmäßige u. ä. ideelle Tätigkeiten erfaßt würden. Sie wären damit aus dem Zuständigkeitsbereich des Datenschutzbeauftragten herausgefallen.

Da der Gesetzgeber die Begrifflichkeit gegenüber dem alten BDSG nicht verändert hat, waren die Aufsichtsbehörden einhellig der Meinung, daß kein Grund für eine andere Auslegung bestehe.

Damit fällt weiterhin unter den Anwendungsbereich des BDSG geschäftsmäßige Datenverarbeitung, wenn sie auf Dauer oder Wiederholung gerichtet ist, ohne Rücksicht auf eine Gewinnerzielungsabsicht.

— **Der Begriff der Datei (§§ 1 Abs.3, 3 u. 33 Abs.2 Nr. 5 BDSG)**

Im neuen BDSG wurde der Dateibegriff inhaltlich neu gefaßt, es kommt danach bei automatisierten Dateien nicht mehr auf umordnungsfähige Merkmale an, sondern darauf, daß die Datei nach bestimmten Merkmalen automatisiert ausgewertet werden kann. Damit fallen auch Texte (Textdateien) unter den Dateibegriff, da sie mit entsprechenden Hilfsmitteln nach bestimmten Kriterien ausgewertet werden können. Das neue BDSG unterscheidet drei weitere Dateitypen, und zwar

- solche, die nur kurzfristig (bis drei Monate) bestehen und dann wieder vollständig gelöscht werden,
- solche, die nur zu Datenschutzkontroll- oder Datensicherungszwecken erzeugt werden und für andere Zwecke nicht genutzt werden dürfen und
- nach manuellen Dateien, aus denen nicht übermittelt wird (interne Dateien).

— **Das Widerspruchsrecht gegen Kontrollen (§ 38 Abs. 4 i.V.m.§ 24 Abs.6 BDSG)**

Diese Rechtsvorschrift schränkt die Kontrollkompetenz der Aufsichtsbehörden in einigen eng umgrenzten Tätigkeitsbereichen (Personalakte, Arztgeheimnis, Sicherheitsakten) ein. Diese Einschränkung wird durch den Einspruch des Betroffenen bei der Aufsichtsbehörde ausgelöst und entfaltet eine Sperre gegen die Kenntnisnahme der Daten durch die Aufsichtsbehörde.

Auch ohne diese Regelung haben die Aufsichtsbehörden die Wünsche der Bürger stets berücksichtigt und ggf. die Kontrollen so gestaltet, daß die Identität von Beschwerdeführern möglichst nicht preisgegeben wurde.

Die aus Sicht der Aufsichtsbehörden verunglückte Rechtsvorschrift hat zu Auslegungsproblemen geführt. So wird gefordert, daß der Widerspruch bei der speichernden Stelle einzulegen sei und diese hätte sie an die Aufsichtsbehörde entweder weiterzuleiten oder bei einer Prüfung vorzulegen. Daß auf diesem Wege die speichernden Stellen massiv auf die Ausübung des Widerspruchsrechts Einfluß nehmen können, liegt auf der Hand. Weiter wurde verlangt, daß bei einer Kontrolle durch die Aufsichtsbehörden von der speichernden Stelle alle erreichbaren Betroffenen befragt werden müßten, ob sie gegen die Kontrolle ihrer Daten durch die Aufsichtsbehörde Widerspruch erheben würden. Erst dann könne die Kontrolle beginnen.

Der Widerspruch ist höchstpersönlich; er vermag eine Datenschutzkontrolle nur in Bezug auf die Daten des Widersprechenden („der auf ihn bezogenen Daten"), nicht auch in Bezug auf die Daten Dritter, zu unterbinden.

Der Widerspruch muß nach dem Wortlaut des Gesetzes „gegenüber" der mit der Datenschutzkontrolle betrauten Behörde erfolgen. Von einer gegenüber dem Betroffenen bestehenden rechtlichen Verpflichtung der datenverarbeitenden Stelle, den bei ihr erklärten Widerspruch unverzüglich an die Kontrollbehörde weiterzuleiten, ist auszugehen.

Hat ein Betroffener für die Kontrollbehörde erkennbar der Datenschutzkontrolle — wenn auch lediglich in allgemeiner Form („auf Vorrat") — widersprochen, so sollte in diesen Fällen des Widerspruchs durch Rückfrage bei dem Betroffenen geklärt werden, ob dieser der Kontrolle im konkreten Einzelfall widersprechen will.

Da das Widerspruchsrecht sich im Bereich von § 24 Abs.2 Satz 4 Nr. 2 Buchst. c nicht nur auf die Datenverarbeitung in Akten in konventioneller Form, sondern auch auf Akten, die in automatisierter Form geführt werden, d. h. auf Personal- und Sicherheitsakten im materiellen Sinne, bezieht, kommt insoweit dem Widerspruchsrecht auch im nicht-öffentlichen Bereich Bedeutung zu.

— **Die Stärkung der Rechte der Aufsichtsbehörden (§ 38 BDSG)**

Nach dem bisherigen BDSG konnten die Aufsichtsbehörden nur aus Anlaß eines Einzelfalls tätig werden, wenn von einem Betroffenen die konkrete Verletzung von Datenschutzvorschriften dargelegt wurde.

Durch das neue BDSG sind die Rechte der Aufsichtsbehörden wesentlich gestärkt worden. Die Aufsichtsbehörden können nunmehr auch Kontrollen durchführen, wenn hinreichende Anhaltspunkte für die Verletzung von Datenschutzbestimmungen vorliegen. Es kommt somit nicht mehr auf die Beschwerde eines Betroffenen an. Damit ist sichergestellt, daß die Aufsichtsbehörden auch Hinweisen von z. B. Betriebsratsmitgliedern oder Journalisten nachgehen können.

— **Die Führung der Dateiübersichten (§ 37 Abs.2 BDSG)**

Die betrieblichen Datenschutzbeauftragten selbst sind nach dem neuen Recht nicht mehr verpflichtet, die Übersichten über die im Betrieb geführten Dateien anzufertigen, sondern die speichernde Stelle (in den meisten Fällen ein Betrieb) ist dazu verpflichtet und muß sie dem betrieblichen Datenschutzbeauftragten zur Verfügung stellen. Diese Rechtsänderung hat einen praktischen Sinn, denn sie ermöglicht auch die Führung dezentraler Übersichten.

— **Die Ausgestaltung automatisierter Abrufverfahren, insbesondere das Stichprobenverfahren (§ 10 BDSG)**

Ab 01. 12. 1992 sind die speichernden Stellen, bei denen Abrufverfahren für Dritte eingerichtet wurden, verpflichtet, Vorkehrungen zur stichproben-

artigen Prüfung der Abrufe einzurichten. Durch diese Verfahren soll die speichernde Stelle in die Lage versetzt werden, die gesetzlich oder vertraglich festgelegten Voraussetzungen für den Abruf zu überprüfen.

Das Stichprobeverfahren ist von der Frage der Protokollierung von Abrufen zu trennen. Zum Umfang der Stichprobenverfahren trifft das Gesetz keine näheren Festlegungen. Wenn auch nicht jeder einzelne Abruf kontrolliert werden soll, läßt sich eine generelle Aussage zur Begrenzung des Umfangs von Stichprobenverfahren dem Gesetz nicht entnehmen. Der Umfang ist jeweils im Einzelfall zu bestimmen und hängt u. a. von der Ausgestaltung der Abrufverfahren, vom Kreis der Datenempfänger und insbesondere von der Art der zu übermittelnden personenbezogenen Daten ab.

— **Den Begriff „Offensichtlich aus einer Datei" (27 Abs.2 BDSG)**

Diese Erweiterung der Anwendbarkeit des BDSG soll z. B. Schriftstücke, die nach ihrem äußeren Erscheinungsbild (Computerauszüge, Hardkopien) zweifelsfrei als aus einer Datei entnommen zu erkennen sind, erfassen. Diese Vorschrift soll verhindern, daß durch die Übertragung von Dateiinhalten auf Papier, z. B. in Listenform, die Schutzbestimmungen des BDSG im nicht-öffentlichen Bereich umgangen werden können.

Im **ERFA-Kreis Bremen** (ein Arbeitskreis der betrieblichen Datenschutzbeauftragten im Lande Bremen) konnte ich in mehreren Besprechungen neben den oben genannten Themen zu weiteren Fragen des neuen BDSG, wie Schadensersatz bei Verletzung des Datenschutzes, verbesserte Rechtsstellung der betrieblichen Datenschutzbeauftragten durch erhöhten Kündigungsschutz, als auch zu anderen Fragen des Datenschutzes, wie Datenübermittlungen durch Telefax, Mitbestimmungs- und Beteiligungsrechte des Betriebsrates in Fragen des Datenschutzes für Arbeitnehmer, Regeln über Nutzung und Sicherung von PC, Stellung nehmen.

3.2 Register der meldepflichtigen Stellen

Als zuständige Datenschutzaufsichtsbehörde für das Land Bremen führe ich das Register der meldepflichtigen Stellen gem. § 32 BDSG. Die Zusammenstellung der Eintragungen am Stichtag 12. 02. 1992 ergibt folgende Übersicht:

Art der Tätigkeit	Bremen	Bremerhaven	insgesamt
Speichern von Daten zum Zwecke der Übermittlung, z. B. Auskunfteien, Adreßhandel	4	3	7
Speichern von Daten zum Zwecke der anonymisierten Übermittlung, z. B. Markt- und Meinungsforschung	1	—	1
Verarbeiten oder Nutzen von Daten im Auftrag als Dienstleistungsunternehmen	86	13	99
	91	16	107

Im Berichtsjahr habe ich das Register der neuen Rechtslage angepaßt und aktualisiert. Das bisher auf einem Großrechnersystem als Stapelanwendung ablaufende DV-Verfahren wurde als PC-Anwendung neu auf einem in meiner Dienststelle vorhandenen PC eingerichtet. Die Umstellungs- und Aktualisierungsarbeiten konnten im Berichtsjahr nicht mehr vollständig abgeschlossen werden; mit ihrem Abschluß ist jedoch im ersten Quartal 1992 zu rechnen. Festzustellen ist dabei, daß viele meldepflichtige Stellen ihren Meldepflichten nicht oder nur unvollständig nachgekommen sind. Ich habe deshalb zu prüfen, ob in diesen Fällen Ordnungswidrigkeitsverfahren einzuleiten sind.

3.3 Bankgeheimnis

In Eingaben beschweren sich Bürgerinnen und Bürger häufig darüber, daß Mitarbeiter von Kreditinstituten die ihnen anvertrauten Daten zu anderen Zwecken genutzt haben sollen. So wurden mir Fälle vorgetragen, in denen z. B. der bei der

Bank angestellte Ehemann Kontoauszüge seiner geschiedenen Ehefrau eingesehen haben soll, ein Bankangestellter Kundendaten im Zusammenhang mit einer weiteren Beschäftigung genutzt haben soll oder Arbeitnehmer über persönliche Beziehungen zu Bankangestellten Auskünfte über Konten ihrer Arbeitgeber erhalten haben sollen. Da zum Teil geeignete Protokollierungen und Recherche-instrumente fehlen oder unzureichend sind, kann in solchen Fällen dieser Verdacht häufig nicht aufgeklärt werden. Es sollte im Eigeninteresse der Kreditinstitute liegen, zur Aufklärung solcher Mutmaßungen eigene geeignete Maßnahmen zu treffen. Die Zugriffsberechtigungen sind so zu gestalten, daß nur unmittelbar mit der Kontoführung beauftragte Mitarbeiter in die Konten ihres Bereiches einsehen können, und es sind geeignete Recherchemittel einzusetzen, um die Zulässigkeit des Zugriffes auf Kundendaten zu überprüfen. Von der Kreditwirtschaft sollte überlegt werden, ob der Zugriff auf Kontendaten (in anderen als der kontoführenden Stelle) nicht auf Wunsch des Kunden von der Legitimation des Kunden abhängig gemacht werden kann, z. B. indem ein Zugriff auf die Daten nur mit der Kontokarte des Kunden möglich ist.

Weitere Eingaben richteten sich erneut dagegen, daß postalisch versandte Kontoauszüge an die falsche Adresse gehen. Hier kann man nur zu größter Sorgfalt aufrufen.

3.4 Weitergabe von Bruttolohnlisten an den Betriebsrat

Mehrere Eingaben wandten sich dagegen, daß ein Arbeitgeber sämtlichen Mitgliedern des Betriebsrats Listen über die Bruttolöhne und Gehälter der Beschäftigten zur Verfügung gestellt hat.

Ich habe den Arbeitgeber darauf hingewiesen, daß lediglich der Betriebsausschuß bzw. ein vom Betriebsrat mit bestimmten Aufgaben gebildeter sonstiger Ausschuß nach § 80 Abs. 2 Satz 2 Betriebsverfassungsgesetz Einblick in die Listen über die Bruttolöhne und Gehälter nehmen darf, nicht jedoch sämtliche Mitglieder des Betriebsrats.

3.5 Ärztliche Schweigepflicht und Einziehung ärztlicher Honorarforderungen durch Verrechnungsstellen

Seit Jahren ist streitig, ob Ärzte ohne Einwilligung ihrer Privatpatienten deren Daten zwecks Einbeziehung ihrer Honorarforderungen an dritte Stellen, z. B. privatärztliche Verrechnungsstellen, übermitteln dürfen. Der Bundesgerichtshof hat mit seiner Entscheidung vom 10. 07. 1991 (Az.: VIII ZR 296/90, abgedruckt in NJW 91, 2955) diese Frage nunmehr entschieden: Ein Patient müsse nicht ohne weiteres davon ausgehen, daß der Arzt, den er zur Behandlung aufsuche, sein Honorar durch eine berufsständische privatärztliche Verrechnungsstelle abrechnen und einziehen lasse. Noch viel weniger gelte dies für gewerbliche Abrechnungsstellen, die von einer für den Patienten anonymen, in erster Linie auf Gewinnerzielung ausgerichteten juristischen Person des Handelsrechts betrieben würden. Die häufig über intimste Dinge des Patienten genaue Auskunft gebenden Abrechnungsunterlagen verdienten einen besonders wirksamen Schutz. Dieser sei grundsätzlich nur gewährleistet, wenn die Honorarabrechnung in einem von vornherein und sicher für den Patienten überschaubaren Bereich erfolge; das aber sei in der Regel allein die Praxis des behandelnden Arztes, einschließlich der für die Abrechnung zuständigen Mitarbeiter. Jedes Überschreiten der Grenzen dieses Bereichs stelle ein Offenbaren des dem Arzt anvertrauten Patientengeheimnisses dar, wobei es ohne Bedeutung sei, ob der Mitteilungsempfänger seinerseits — etwa als Arzt oder privatärztliche Verrechnungsstelle — der Schweigepflicht unterliege. Der Bundesgerichtshof kommt zu dem Schluß, daß der Arzt zur Übermittlung von Patientendaten an eine berufsständische privatärztliche oder an eine gewerbliche Verrechnungsstelle nur befugt sei, wenn der Patient ausdrücklich darin eingewilligt habe. Folglich sei die Abtretung der Forderung wegen Gesetzesverstoßes nichtig und eine Klage der Verrechnungsstelle auf Zahlung des Honorars abzuweisen.

Ich habe den Senator für Gesundheit, den Magistrat der Stadt Bremerhaven, die Ärzte- und die Zahnärztekammer Bremen sowie die Krankenhausgesellschaft der Freien Hansestadt Bremen angeschrieben und gefragt, wie sie auf die Entscheidung zu reagieren gedächten. Die Zahnärztekammer und die Privatverrechnungsstelle für Ärzte und Zahnärzte des Landes Bremen e. V. haben mir inzwischen mitgeteilt, sie hätten ihre Mitglieder über das Urteil und seine Konsequenzen informiert. Die Krankenhausgesellschaft hat, wie sie mir mitgeteilt hat, ihre Mitglieder darauf hingewiesen, daß die Einwilligung der Privatpatienten von Kran-

kenhausärzten eingeholt werden müsse, wenn Verrechnungsstellen eingeschaltet werden sollen.

Schließlich hat der Senator für Gesundheit die Krankenhausbetriebe der Stadtgemeinde Bremen über das Urteil und mein Schreiben unterrichtet, sie gebeten zu prüfen, welche organisatorischen Maßnahmen daraufhin ergriffen werden müssen und ihn darüber zu unterrichten.

Ich begrüße die höchstrichterliche Klarstellung der Rechtslage als wichtigen Beitrag zum Schutz der Patientendaten und halte es für wichtig, daß die Patienten auf die Einhaltung der ihnen durch richterliches Urteil zugesprochenen Rechte bestehen, und werde sie dabei unterstützen.

3.6 Ärztliche Schweigepflicht und Übergabe der Patientenkartei an den Käufer einer Arztpraxis

Nachwievor ist es üblich, daß niedergelassene Ärzte beim Verkauf ihrer Praxis die Patientenkartei dem Praxisnachfolger übergeben, ohne die Patienten zuvor um Einwilligung gebeten zu haben. Zwar fehlte es bislang an einem höchstrichterlichen Urteil, gleichwohl — darüber habe ich im 12. Jahresbericht (S. 56) informiert — wurde von den Datenschutzbeauftragten in Bund und Ländern, in der Literatur und in zuständigen Ministerien der Länder einhellig die Auffassung vertreten, dies verstoße gegen die ärztliche Schweigepflicht. Auf meine Anregung hin hatte der Senator für Gesundheit, wie er mir im April 1990 mitteilte, der Ärzte- und der Zahnärztekammer vorgeschlagen, in ihre Berufsordnungen Regelungen aufzunehmen, die der ärztlichen Schweigepflicht auch in diesem Punkt Rechnung tragen. Auf meine Frage nach dem Stand der Dinge hat der Senator für Gesundheit mir jüngst geantwortet, er habe aus diesem Anlaß die Kammern zu nunmehr kurzfristigem Handeln aufgefordert.

Ich sehe mich in meiner Rechtsauffassung durch das inzwischen bekanntgewordene Urteil des Bundesgerichtshofs vom 11. 12. 1991 — Az.: VIII 4/91 — bestätigt. Der BGH entschied, daß ein Vertrag, der die Übergabe der Patientenkartei ohne Einwilligung der Betroffenen enthält, das informationelle Selbstbestimmungsrecht der Patienten und die ärztliche Schweigepflicht verletze; er sei wegen Verstoßes gegen ein gesetzliches Verbot nichtig. Das Gericht verlangt grundsätzlich eine ausdrücklich erklärte Zustimmung des einzelnen Patienten. Daneben läßt es eine Zustimmung durch schlüssiges Verhalten nur für den Fall gelten, daß der Patient sich auch dem Übernehmer der Praxis zur ärztlichen Behandlung anvertraut.

3.7 Kundenkarteien in Apotheken

Seit einigen Jahren setzen Apotheker zunehmend PC ein, auf denen sie auch Kundendaten verarbeiten. Diese erhalten sie meist, weil gesetzlich krankenversicherte Kunden ihnen die Rezepte zwecks Weiterleitung an die Kassen überlassen müssen. Dieses Verfahren ist in § 300 Abs. 1 SGB V geregelt, enthält aber keine Befugnis für die Apotheker, die auf den Rezepten enthaltenen Daten zu anderen Zwecken zu speichern. Derartige andere Zwecke könnten etwa die Zusendung von Werbematerial, die Einladung zu Informationsveranstaltungen über gesundheitliche Themen, Glückwünsche zu Geburtstagen oder auch die Kontrolle schwer lesbarer Rezepte sein.

Auf einen entsprechenden Hinweis hin habe ich die Verarbeitung von Kundendaten in einer Apotheke überprüft. Der Apotheker speichert Namen, Geburtsdaten, Anschriften, Medikamente und den Arzt der Kunden, die er in die Kategorien „Asthmatiker" oder „Diabetiker" einordnet. Er nutzt die Kartei für gezielte Informationen und Einladungen sowie zur Überprüfung unklarer Rezepte. Er erklärte mir, die Einwilligung habe er jeweils zuvor mündlich eingeholt. Er legte mir den Entwurf für eine vorgedruckte Einwilligungserklärung vor, die er künftig den Betroffenen einschließlich der bereits gespeicherten Kunden vorlegen wolle. Ich habe der Datenverarbeitung unter der Voraussetzung grundsätzlich zugestimmt, daß der Apotheker wie zugesagt verfahre und den Vordruck um den Zweck der Verarbeitung und um Hinweise auf die Freiwilligkeit und Widerrufbarkeit der Unterschrift ergänze. Außerdem sei sicherzustellen, daß die Daten gelöscht würden, wenn die nachträgliche Einwilligung verweigert werde, ein Widerruf erklärt werde oder erkennbar sei, daß der Patient — aus welchen Gründen auch immer — nicht mehr Kunde der Apotheke sei. Für den Fall, daß die Kartei wie geplant auf den bereits installierten PC übernommen wird, habe ich darauf hingewiesen, daß eine Datenschutzsoftware zu implementieren sei, die die

gerade angesichts der Speicherung von gesundheitlichen Daten erforderliche Datensicherheit gewährleistet.

Ich habe bereits in 1984 die Apothekerkammer darauf hingewiesen, daß Kauf und Abrechnung von ärztlich verschriebenen Medikamenten eine derartige Datenverarbeitung nicht legitimierten, so daß der Kunde ihr zuvor ausdrücklich schriftlich zugestimmt haben müsse. Die Kammer erklärte mir damals, ihr seien keine Apotheken bekannt, die Datenverarbeitungsgeräte besäßen, die Kundendaten speichern könnten. Falls dies aber in Zukunft der Fall sein und damit Kundenwerbung betrieben werden sollte, verstoße das gegen ihre Berufsordnung. Aus Anlaß des Inkrafttretens des neuen Bundesdatenschutzgesetzes zum 01. 06. 1991 hat die Kammer ihre Mitglieder inzwischen darauf hingewiesen, daß § 33 dieses Gesetzes sie verpflichte, ihre Kunden von der erstmaligen Speicherung ihrer Daten zu benachrichtigen. Außerdem hat die Kammer an meine in 1984 geäußerte Rechtsauffassung erinnert. Die Apothekerkammer hat inzwischen ihre Mitglieder in diesem Sinne informiert.

3.8 Telefonische Anwerbung für Forschungsprojekte

Seit 1984 hat das Bremer Institut für Präventionsforschung und Sozialmedizin (BIPS) wiederholt durch Befragung und Untersuchung von Bremer Bürgern Risikofaktoren für Herz- und Kreislauferkrankungen erforscht. Die „Probanden" wurden jedesmal nach dem Zufallsprinzip aus dem Melderegister übermittelt.

Im Verlauf des 1991 durchgeführten dritten Durchlaufs (3. Bremer Gesundheitssurvey) hat sich ein erstmals ausgewählter und angesprochener Bürger über die Art und Weise beschwert, mit der das vom BIPS beauftragte Meinungsforschungsinstitut FORSA ihn zur Beteiligung habe bewegen wollen. Er sei insgesamt dreimal angerufen worden, seine Weigerung sei nicht akzeptiert worden, man habe ihm gesagt, er stehe für 100 Bremer, auf ihn komme es an usw.

Den Auftragsunterlagen, die mir das BIPS auf Anfrage zur Verfügung stellte, entnahm ich, daß sich FORSA verpflichtet hatte, eine „Ausschöpfungsrate" von mindestens 70 % zu erreichen, und andernfalls Kürzungen ihres Honorars zu befürchten hatte. Zur Respektierung der Persönlichkeitsrechte der Angesprochenen enthielt der Vertragstext lediglich die abstrakte Aussage, FORSA unterwerfe sich der Aufsicht des Bremischen Landesbeauftragten für den Datenschutz. Meine Versuche, die mir auf diese Weise bekannt gewordenen Aufsichtsbefugnisse auch wirklich wahrzunehmen, wurden von FORSA anscheinend nicht so ernst genommen. Jedenfalls lehnte man meinen Vorschlag ab, die Interviewerinnen über ihre Verpflichtung zu belehren, die Persönlichkeitsrechte zu respektieren. Von Anfang an sei sowohl diesen als auch den „Probanden" gegenüber klargestellt worden, daß die Teilnahme freiwillig sei.

Ich mußte befürchten, daß das Vorgehen von FORSA gegen Ablauf der Ausführungsfrist noch „energischer" werden würde. Deshalb habe ich das BIPS darauf hingewiesen, daß die gewählte Methode, die Probanden mit nicht angemeldeten Telefonanrufen anzusprechen, einen erheblichen Eingriff in die Privatsphäre der Betroffenen darstelle.

Ich habe das BIPS darauf hingewiesen, daß die Telefonwerbung für Forschungszwecke aus der Sicht des Datenschutzes kritisch zu betrachten sei. Ich habe angekündigt, daß ich bei seinem Einsatz bei künftigen Projekten zusätzliche Garantien verlangen werde. Daraufhin erklärte das BIPS, es werde mit den FORSA-Mitarbeiterinnen in Bremen ein Gespräch führen. Außerdem wolle es FORSA anbieten, mit seinen Telefoninterviewerinnen am Sitz in Dortmund über die geschilderten Probleme zu sprechen.

4. Entwicklung der Dienststelle

Auch in diesem Berichtsjahr ist es nicht gelungen, die Stelle des Landesbeauftragten für den Datenschutz wieder zu besetzen. Die gesamten Umstände des Verfahrens gingen an der Dienststelle nicht spurlos vorüber, sie befand sich zeitweilig in einer Wartestellung und war nicht voll handlungsfähig. Nicht zuletzt wegen dieser Umstände konnte auch eine leitende Stelle im Informatik- und Technikreferat nicht besetzt werden. Es bedurfte daher erneut besonderer Anstrengungen, den Dienstbetrieb entsprechend der gesetzlichen Verpflichtungen bei vielseitigen Anforderungen aufrecht zu erhalten.

Im Berichtsjahr habe ich mit Beschäftigten der Dienststelle ein integriertes DV-Projekt für Beratungs- und Prüftätigkeit des LfD (DV-Projekt LfD) entworfen. Dieses Projekt soll die Aufgabenerfüllung der Dienststelle unterstützen und effektivieren. Ich strebe eine entwicklungsfähige und in den Dienstbetrieb integrierbare DV-Lösung an. Zur Zeit werden Arbeits- und Aufgabenstrukturen analysiert. Für diese Analyse und die sich daraus ergebenden Realisierungsmöglichkeiten ist die Kooperation mit dem Fachbereich Informatik der Universität Bremen vereinbart worden, um die Entwicklung schneller voranzutreiben und auf eine breitere Basis zu stellen. Zunächst sollen die Bereiche Beratungs- und Prüftätigkeit dv-technisch unterstützt werden. Hierzu gehören u. a.

- die Entwicklung eines Informationspools mit Ergebnissen von Schwachstellenanalysen zu Telekommunikationseinrichtungen, zu Überwachungsanlagen, zu PC-Arbeitsplätzen und zu Netzstrukturen,
- die Kontrolle von Hard- und Software (Testung und Schwachstellenanalyse),
- die Effektivierung der Datenschutzkontrolle von PC-Anwendung in der bremischen Verwaltung,
- die Automatisierung und strukturelle Auswertungen der zu führenden Register.
- der Aufbau eines Recherchesystems, das Gesetze, Urteile, Aufsätze, datenschutzrelevante Drucksachen u. v. m. enthalten soll.
- die Erstellung eines Akten- und Archivnachweissystems.

Voraussetzung für die zukünftigen Entwicklungsschritte ist eine adäquate personelle und sachlich-technische Ausstattung.

5. Schluß

Die geschilderte personelle Situation der Dienststelle des Landesbeauftragten für den Datenschutz führte dazu, daß im Berichtsjahr im leitenden Bereich rund 1/3 der personellen Kapazitäten fehlte. Daß in einer solchen Situation keine arbeits- und personalintensiven Entwicklungsarbeiten geleistet werden konnten, liegt auf der Hand. Die Arbeit mußte auf wenige Schultern verteilt werden, alle Beschäftigten der Dienststelle wurden stärker in Anspruch genommen. Trotz starker Belastungen ist es bei den Beschäftigten zu keinen gravierenden Motivationseinbrüchen gekommen. Ich möchte mich bei all den Kolleginnen und Kollegen bedanken, die über das dienstrechtlich geschuldete Maß weit hinaus mich bei der Aufgabenerfüllung unterstützt und sich für den Datenschutz eingesetzt haben.

Sven Holst

Vertreter des Landesbeauftragten für den Datenschutz

Bremerhaven, den 09. 03. 1991

Anlage

Entschließung der 42. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1991 zum Datenschutz im Recht des öffentlichen Dienstes

I.

Die Daten von Arbeitnehmern werden im Laufe ihres beruflichen Lebens in vielfältiger Weise vom Arbeitgeber verarbeitet. Allein schon im Hinblick auf die große Zahl der über Arbeitnehmer erhobenen Daten und mit Rücksicht auf die Abhängigkeit des Arbeitnehmers vom Arbeitgeber ist eine gesetzliche Regelung der Verarbeitung von Personaldaten zwingend erforderlich. Auch gegenüber Beamten und anderen im öffentlichen Dienst Tätigen kann die Verarbeitung ihrer Daten nicht allein auf die hergebrachten Grundsätze des Berufsbeamtentums gestützt oder in Verwaltungsvorschriften geregelt werden. Vielmehr ist eine gesetzliche Grundlage vonnöten. Sie muß umso konkreter sein, je tiefer in das Persönlichkeitsrecht der Betroffenen eingegriffen wird.

II.

In der Auseinandersetzung um das Recht des öffentlichen Dienstes beeinträchtigen zwei grundlegende Fehleinschätzungen eine angemessene Regelung des Datenschutzes. Es trifft nicht zu, daß die Kenntnis des Dienstherrn über seine

Bediensteten alle persönlichen Lebensumstände vollständig und lückenlos umfassen muß. Es ist ferner unrichtig, daß gesetzliche Regelungen überflüssig sind, weil stets die Einwilligung der Betroffenen eingeholt werden kann.

Zum einen wäre es mit der Würde des Menschen unvereinbar, wollte man ihn in seiner ganzen Persönlichkeit registrieren. Zwar ist der Angehörige des öffentlichen Dienstes dem Staat gegenüber besonders eng verpflichtet; er bleibt aber auch gegenüber seinem Dienstherrn Grundrechtsträger: Auch seine personenbezogenen Daten dürfen nur erhoben und verarbeitet werden, soweit das für die Begründung und Abwicklung des Dienstverhältnisses erforderlich ist.

Zum anderen macht der Rückgriff auf die Einwilligung gesetzliche Regelungen keineswegs überflüssig. Zwar ist die Erhebung und Verarbeitung personenbezogener Daten mit Einwilligung des Betroffenen grundsätzlich auch dann zulässig, wenn eine gesetzliche Grundlage fehlt. Die Einwilligung wird jedoch zur Farce, wenn sie faktisch erzwungen wird, weil z. B. eine Bewerbung ohne Einwilligung nicht berücksichtigt wird. Soweit bestimmte Angaben verfügbar sein müssen, sind sie gesetzlich präzise vorzuschreiben, aber zugleich auf den erforderlichen Umfang zu begrenzen.

III.

Neben der Neuordnung des Personalaktenrechts bedürfen auch andere Teilbereiche des öffentlichen Dienstrechts der datenschutzgerechten gesetzlichen Regelung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere die Lösung folgender Probleme für vorrangig:

1. **Bewerbung um Einstellung in den öffentlichen Dienst**

Es ist — für den Bewerber transparent — festzulegen,

- welche personenbezogenen Informationen von ihm verlangt bzw. über ihn eingeholt, wie sie genutzt werden dürfen und wann sie zu löschen sind,
- ob und unter welchen Voraussetzungen und in welchem Stadium des Verfahrens der Bewerber sich Tests, Untersuchungen und Überprüfungen zu unterziehen hat,
- ob und inwieweit private Institutionen daran mitwirken und welche vertraglichen Sicherungen zum Schutz personenbezogener Daten zu vereinbaren sind,
- daß die Daten jeweils erst zu dem Zeitpunkt, in dem sie für das Verfahren erforderlich werden, und mit dem geringstmöglichen Eingriff erhoben werden.

2. **Sicherheitsüberprüfung**

Es ist bereichsspezifisch gesetzlich festzulegen,

- wer im öffentlichen Dienst einer Sicherheitsüberprüfung unterzogen wird,
- welche personenbezogenen Daten dafür erhoben und verarbeitet werden,
- wie das Verfahren gestaltet wird, insbesondere welche Stellen mit welchen Befugnissen am Verfahren beteiligt sind und unter welchen Voraussetzungen Sicherheitsbedenken anzunehmen sind,
- daß die im Rahmen der Sicherheitsüberprüfung erhobenen Daten grundsätzlich nur für diesen Zweck verwendet werden dürfen,
- daß der Betroffene über das Ergebnis der Sicherheitsüberprüfung zu unterrichten ist.*

3. **Ärztliche Untersuchung**

Es ist durch Gesetz oder ergänzende Rechtsverordnung festzulegen,

- unter welchen Voraussetzungen die ärztliche Untersuchung eines Bewerbers oder Bediensteten angeordnet werden kann,
- daß jede ärztliche Untersuchung einen präzisen Untersuchungsauftrag voraussetzt, der Anlaß und Gegenstand der Untersuchung möglichst exakt definiert und den Umfang der Untersuchung eingrenzt,
- wie das Arztgeheimnis und der Datenschutz sicherzustellen sind,

---

* Auf ihre Forderungen zur Sicherheitsüberprüfung (Geheimschutzgesetz) in den Entschließungen vom 13. 09. 1985, 18. 04. 1986 und 22. 03. 1990 nimmt die Konferenz Bezug.

- wann und in welchem Umfang Versicherungen und früher behandelnde Ärzte über frühere Untersuchungen und Maßnahmen befragt werden und diese offenbaren dürfen,
- daß Ärzte und Versicherungen Daten nicht ohne Kenntnis des Betroffenen und nur mit Einwilligung des Bewerbers offenbaren dürfen,
- daß die Unterlagen der ärztlichen Untersuchungen nicht für andere Zwecke verwendet werden und nicht mit solchen vermengt werden dürfen, die anderen Zwecken dienen, und daß sie zu vernichten sind, sobald sie nicht mehr benötigt werden,
- daß der Arzt der personalverwaltenden Stelle nur das Endergebnis seiner Untersuchung und — soweit erforderlich — nur tätigkeitsbezogene Risiken mitzuteilen hat,
- daß dem Betroffenen ein Recht auf Einsicht in die beim Arzt verbliebenen Untersuchungsunterlagen zusteht.

4. **Beihilfen**

Gesetzlich festzulegen sind die Grundlagen eines datenschutzgerechten Beihilfeverfahrens, insbesondere die Abschottung der Beihilfestelle, das Verbot automatisierter Speicherung von Diagnosedaten und anderen medizinischen Einzelangaben, die Zweckbindung der Daten sowie ein eigener Beihilfeanspruch der Angehörigen.

5. **Personalinformationssystem**

Es muß dienstrechtlich gewährleistet sein, daß

- automatisierte Systeme zur Verarbeitung von Personaldaten zu unterschiedlichen Zwecken (z. B. Urlaubsdatei, Telefondatenerfassung, PC-Betriebsdaten) nicht zu umfassenden Persönlichkeitsprofilen verknüpft werden,
- alle vorgesehenen Auswertungen von Personaldaten in einer Übersicht, die dem Betroffenen zugänglich sein muß, zusammengefaßt werden,
- Kontrollen der Bediensteten mit Hilfe automatisierter Systeme unzulässig sind; Ausnahmen bedürfen einer gesetzlichen, insbesondere personalvertretungsrechtlichen Regelung.

IV.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die für das Personalrecht zuständigen Minister und den Gesetzgeber auf, die auf der Grundlage der Rechtsprechung des Bundesverfassungsgerichts verfassungsrechtlich notwendigen Vorschriften zu erlassen.

Druck: Anker-Druck Bremen