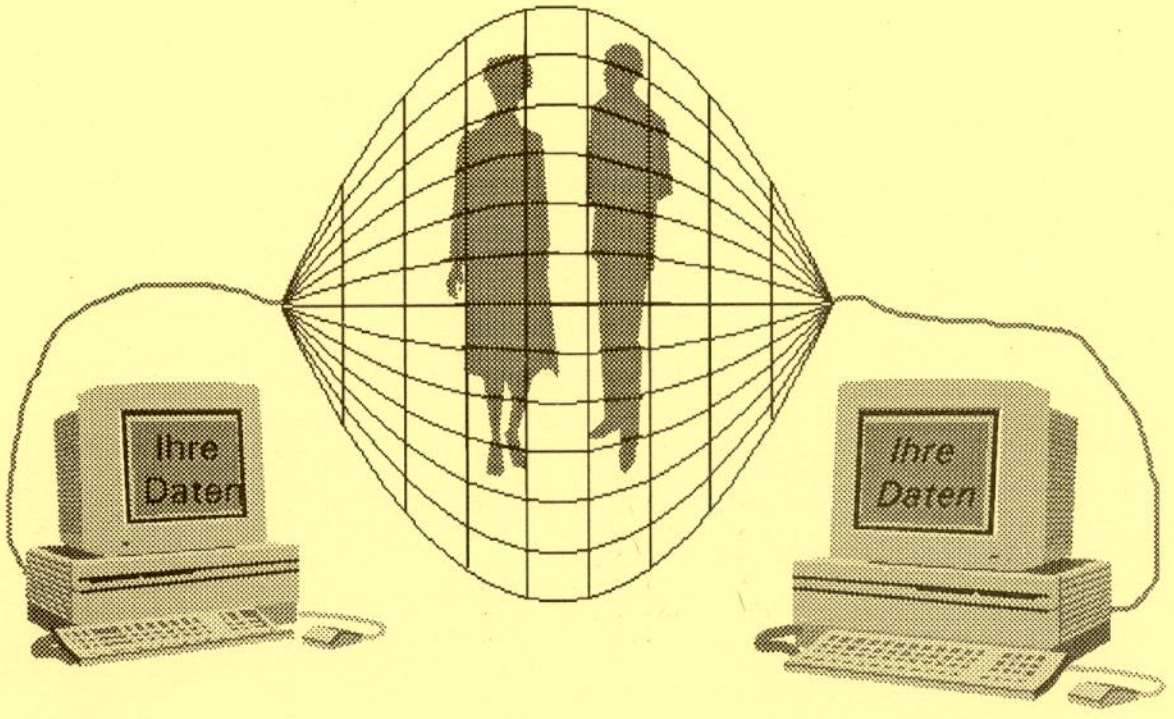
FREIE HANSESTADT BREMEN

Landesbeauftragter für den Datenschutz

16. Jahresbericht



Der Mensch steht höher als Technik und Maschinen
(Artikel 12 der Landesverfassung der Freien Hansestadt Bremen)

Vorgelegt zum 31. März 1994

95 Seiten

BREMISCHE BÜRGERSCHAFT
Landtag
13. Wahlperiode

Drucksache 13/859
31.03.94

Sechzehnter Jahresbericht des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bremischen Bürgerschaft (Landtag) und dem Präsidenten des Senats meinen 16. Bericht über das Ergebnis meiner Tätigkeit im Jahre 1993 zum 31. März 1994 (§ 33 Abs. 1 Bremisches Datenschutzgesetz - BrDSG)

Dr. Stefan Walz, Landesbeauftragter für den Datenschutz

Inhaltsübersicht:

Redaktionsschluß: 28. Februar 1994

1. Vorwort

1.1. Zur Situation

Die Jahreszahlen 1993 und 1994 geben für diesen Bericht speziellen Anlaß zum Rückblick. 1993 jährte sich zum zehnten Mal die Verkündung des Volkszählungsurteils des Bundesverfassungsgerichts, mit dem der Datenschutz als Grundrecht bestätigt und das informationelle Selbstbestimmungsrecht zum festen Bestandteil des deutschen Verfassungsrechts gemacht wurde. 1994 weckt Assoziationen an Orwells "1984" und lädt zu einem Vergleich von damaliger Vision des Autors und heutiger Realität ein. Beide symbolträchtigen Daten haben, was die Situation des Datenschutzes in diesem Land angeht, zu vorwiegend nachdenklichen und kritischen Kommentaren geführt. "Armer Datenschutz" betitelte etwa die ZEIT ihren Jubiläumsartikel zum Volkszählungsurteil.

Symptome ebenso wie Begründungen für eine negative Analyse, die den derzeitigen Zustand als Syndrom rapider technologischer Modernisierung bei gleichzeitiger datenschutzpolitischer Restauration erscheinen läßt, gibt es zuhauf. Wohl kaum in einem Jahr zuvor hat sich die "Verdatung" des Einzelnen so beschleunigt wie 1993. Die Tabelle der allein im Jahr 1993 vom Gesetzgeber neu zugelassenen Datenabgleiche, Mitteilungspflichten und Rasterkontrollen, die zur Illustration im Anschluß an dieses Vorwort abgedruckt ist, belegt die Tendenz, statt den Staat transparent den Bürger "gläsern" zu machen. Die - zweifellos auch von den Forderungen der Datenschutzbeauftragten verstärkte - Regelungsflut ist zur "Verrechtlichungsfalle" des Datenschutzes geworden. Das "überwiegende Allgemeininteresse", vom Bundesverfassungsgericht als ausnahmsweise Legitimation zum Eingriff in das Grundrecht auf informationelle Selbstbestimmung gemeint, ist zum Einfallstor einer nicht enden wollenden bürokratischen Reglementierung und Kontrolle geworden. Ressourcenknappheit, notleidende öffentliche Haushalte und der vielfach diffuse und undifferenzierte Konsens über Politikziele wie "Eindämmung des Leistungsmißbrauchs" und "Bekämpfung der Organisierten Kriminalität" dienen als Argumente dafür, das nach unserer Verfassung im Sinne liberaler Rechtsstaatlichkeit zu verstehende Verhältnis zwischen Bürger und Staat umzukehren. Nicht der Staat hat dann den Eingriff in die grundrechtlich geschützten Sphären zu legitimieren, sondern der Einzelne hat seine "weiße Weste" vorzuzeigen. In diesem Meinungsklima verwundert nicht, daß der Antrag, in ein reformiertes Grundgesetz ausdrücklich ein Grundrecht auf Datenschutz aufzunehmen, in der Gemeinsamen Verfassungskommission keine ausreichende Mehrheit gefunden hat. Ohnehin konzentriert sich der "main stream" der Politikdebatte im Superwahljahr auf die imperialen Themen Wirtschaftskrise, Arbeitslosigkeit und öffentliche wie private Armut. Vermeintlich "weiche Themen" wie die Frauenpolitik, der Umweltschutz und eben auch die Wahrung der Bürgerrechte werden dabei an den Rand gedrängt.

Doch trifft die Entwicklung vom Haushalts- zum Datenschutzdefizit keineswegs alle Bürgerinnen und Bürger gleich. 1993, vom SPIEGEL wegen der einschneidenden Kürzungen im Sozialleistungssystem als "Unglücksjahr für die Schwachen" eingestuft, hat auch die Entwicklung in Richtung auf einen "Zwei-Klassen-Datenschutz" verschärft: Es sind gerade die Bedürftigen, die Sozialleistungsempfänger, die arbeitslos Gewordenen usw., die der Bürokratie ihre Lebensverhältnisse immer detaillierter offenlegen müssen. Auch diesen speziellen Aspekt belegt die abgedruckte Übersichtstabelle; aufgeführt sind dort neue Verarbeitungsregelungen vorwiegend im Sozialrecht (vgl. S. 11 ff.).

1.2. Bremen

Dieser kritische Befund konzentriert sich jedoch auf Gesetzgebung und (Bundes-)Politik zum Datenschutz und ist daher unvollständig. Die Bilanz sieht etwas erfreulicher aus, wenn man die Bremer Situation betrachtet: Die unverminderte Zahl der bei mir eingegangenen schriftlichen und telefonischen Anfragen, Eingaben und Beschwerden belegt ebenso wie die rege Nachfrage nach Informationsmaterial, daß den Bürgerinnen und Bürgern die Sensibilität für das, was der Datenschutz schützen soll, noch keineswegs verloren gegangen ist (vgl. Ziff. 2.1.1.). Die zahlreichen Anfragen und Beratungswünsche aus den bremischen Behörden, die regen telefonischen und Gesprächskontakte mit meiner Dienst-

stelle zeigen das große Interesse vieler Mitarbeiter an der Wahrung des Datenschutzes ihrer Antragsteller, Klienten und Besucher. Verstoßfälle und Sicherungsmängel, für die dieser Jahresbericht wieder eine Reihe von Beispielen enthält, beruhen nur selten auf vorsätzlicher Nichtbeachtung datenschutzrechtlicher Bestimmungen, vielmehr in der Regel - was allerdings nicht entschuldigt - auf bürokratischer Gedankenlosigkeit. Die Bereitschaft, erkannte Fehler zu korrigieren, war bei einer Mehrzahl der Eingaben und Prüfbeanstandungen gegeben, wenn es bis zur Mängelbeseitigung gelegentlich auch zeitraubender Beharrlichkeit bedurfte.

Dieses vergleichsweise positive Bild wird allerdings getrübt durch Fälle, in denen ganze DV-Systeme mit teilweise sensiblen Daten in Betrieb genommen werden, ohne daß gleichzeitig ein - möglicherweise sogar bereits mit mir abgesprochenes - Datenschutzkonzept realisiert ist, wie dies mit dem polizeilichen Informationssystem ISA-D geschehen ist (vgl. Ziff. 5.1.1.). Für ebenso gravierend halte ich die Verlagerung umfangreicher DV-Produktionsbereiche aus Bremen heraus in externe Rechenzentren, ohne daß ich rechtzeitig vorher eingeschaltet worden bin. Beispiel dafür ist die automatisierte Personalabrechnung der Kliniken, die vom bisherigen RbV zu einem in Nordrhein-Westfalen gelegenen kirchlichen Rechenzentrum transferiert werden soll. Die Informationspolitik einer Reihe von senatorischen und sonstigen Behörden ist nach wie vor nicht zufriedenstellend; immer wieder erfahre ich entgegen der ausdrücklichen Informationspflicht in § 27 Abs. 4 BrDSG zu spät von Vorhaben mit großer datenschutzrechtlicher Relevanz. Bei der raschen Auseinanderentwicklung der DV-Landschaft, der zunehmenden Vergabe personenbezogener Datenverarbeitung an externe Dritte usw., werde ich darauf achten, daß Kontrollverluste für den Datenschutzbeauftragten so gering wie möglich bleiben (vgl. Ziff. 2.2.).

Das datenschutzbezogene Gesetzgebungsprogramm in Bremen weist noch eine Reihe von "Fehlanzeigen" auf. Eile ist hier geboten, bedenkt man das nahende Ende der Legislaturperiode. Die im letzten Jahresbericht annoncierte Novellierung des Bremischen Datenschutzgesetzes kommt erst nach der Osterpause 1994 in Gang. Für eine Änderung des Landesverfassungsschutzgesetzes gibt es noch keinen mir bekannten Entwurf. Die Arbeiten am Gesetz für einen öffentlichen Gesundheitsdienst gehen dafür offensichtlich zügiger voran (vgl. u. Ziff. 8.5.1). Für die Sicherheitsüberprüfung bedarf es nach der Verabschiedung des einschlägigen Bundesgesetzes entsprechender landesgesetzlicher Normen für die bremischen Bediensteten, wobei allerdings der Regelungsspielraum auf Landesebene für eine Einschränkung der Eingriffe in die Privatsphäre genutzt werden sollte. Vereinfacht und erweitert werden muß der Zugang zu Unterlagen der Umweltbehörden (vgl. dazu Ziff. 1.4.).

Sehr konstruktiv waren auch im Berichtsjahr wieder die Beratungen im Datenschutzausschuß der Bremischen Bürgerschaft. Die wichtigsten Ergebnisse werden erstmals in diesem Bericht in einem eigenen Abschhnitt zusammengestellt (vgl. u. Ziff. 1.4).

1.3. Perspektiven

In einem Szenario weltweiter ebenso wie lokaler Vernetzung, der Nutzung des PCs als alltäglichem Gebrauchsgegenstand wie ein Haushaltsgerät, der mobilen Allgegenwart von Kommunikation, der Internationalisierung von Datenströmen usw. werden sich auch die Standards und Aktionsformen des institutionellen Datenschutzes selbstkritisch prüfen lassen und den neuen Verhältnissen anpassen müssen. Medien- und Öffentlichkeitsarbeit, Präsenz auf IuK- Messen und Fachforen, Kontakte mit Herstellern und Anwendervereinigungen, Professionalisierung der technischen Beratung, aber auch Verbindungen zu Kontrollinstitutionen im - vor allem europäischen - Ausland gewinnen immer mehr an Bedeutung.

Wenig weiter hilft auch die gelegentlich mit etwas Selbstmitleid unterfütterte Klage, das Datenschutzbewußtsein halte nicht Schritt mit der Entwicklung der Informationsgesellschaft. Wenn der Computer schon das Klassenzimmer zu "erobern" beginnt, wenn DV-Wissen zum verbreiteten Gemeingut wird, ist eine "neue Lernkultur" gefragt, die das Bewußtsein für die Risiken der IuK-Technik weckt und fördert, ohne die Computerisierung und ihre zweifellos vorhandenen Vorteile in vielen Lebensbereichen abzuqualifizieren.

Konkrete Ansatzpunkte in Bremen bieten vor allem Kontakte zu den Ausbildungsstätten für die künftigen Planer und beruflichen Nutzer der Informations- und Kommunikationstechnik, d.h. zu den Informatikfachbereichen der Universität Bremen und der Hochschule Bremerhaven. Seit längerem übernehmen dort meine Mitarbeiter und ich regelmäßig Lehraufträge. Allerdings bleibt hier noch viel zu tun.

1.4. Ergebnisse der Beratungen des 15. Jahresberichts im Datenschutzausschuß

Der Datenschutzausschuß der Bremischen Bürgerschaft hat in insgesamt fünf Sitzungen meinen 15. Jahresbericht mit folgenden wesentlichen Ergebnissen beraten:

Ziff. 2.2.3 Abhörrisiken im Mobilfunk

Nachdem die früher gültige Beschränkung der zulässigen Empfangsbereiche für Funkfrequenzen durch das Bundespostministerium aufgehoben worden ist, hatte ich auf das Problem der Abhörmöglichkeiten für den Funkverkehr von Polizei und Rettungsdiensten hingewiesen und entsprechende organisatorische und technische Gegenmaßnahmen gefordert. Im Datenschutzausschuß hat der Senator für Inneres und Sport erklärt, in der gegenwärtigen Situtation könne kaum verhindert werden, daß der Polizeifunk abgehört werde. Auch Versuche, Sprachverschleierungsgeräte einzusetzen, seien nur eingeschränkt erfolgversprechend. Als organisatorische Konsequenz würden Funkbänder in einem wegen der geringeren Reichweite nicht so stark abhörgefährdeten Frequenzbereich verwandt. Im übrigen seien alle Beamten auf die Abhörrisiken hingewiesen, so daß die Funkübermittlung etwa in sensitiven Fällen durch telefonische Meldungen ersetzt werden könne.

Ziff. 5.1.2 Verringerung der bundesweiten Speicherung bei Staatsschutzdelikten

In Bremen wurde das bundesweite Informationssystem APIS (Arbeitsdatei "Personen, Institutionen, Objekte, Sachen") genutzt, um dort alle (!) im Bereich der Inspektion für polizeiliche und strafverfolgende Zwecke anfallenden relevanten Daten einzustellen. Um eine Trennung zwischen den in APIS zu erfassenden Personen und den nur regional im Lande Bremen zu speichernden Datensätzen aus dem Bereich des Staatsschutzes zu ermöglichen, hatte ich vorgeschlagen, die Bremer Fälle ins bremische Informationssystem der Polizei ISA ("Informationssystem Anzeigen" - ISA) und nur die schweren oder überregional tätigen Täter in das beim Bundeskriminalamt geführte APIS einzuspeichern.

Nachdem inzwischen die Inspektion 7 (Abteilung Staatsschutz) an das ISA-Verfahren angeschlossen ist, sind insoweit meine Anforderungen umgesetzt worden.

Ziff. 5.1.3 § 218: Speicherung betroffener Frauen

Ich hatte im 15. JB Zweifel geäußert, ob die Speicherung betroffener Frauen bei Vorliegen des Verdachts auf Verstoß gegen § 218 StGB im polizeilichen Informationssystem (ISA) überhaupt notwendig ist. Es sollte vielmehr angestrebt werden, die Vorgänge nur noch unmittelbar in den zuständigen Kriminalkommissariaten zu verwalten.

Im Datenschutzausschuß hat der Senator für Inneres und Sport erklärt, er wolle diese Fälle aus der Vorgangsverwaltung von ISA nicht herausnehmen, weil ansonsten wieder eine manuell geführte Registrierung eingeführt werden müßte; diese sei in der Praxis wesentlich schwieriger zu überprüfen. Eine Überwachung der Speicherung und insbesondere auch der Löschung sei im DV-gestützten Verfahren wesentlich besser möglich. Der Datenschutzausschuß hat von dem Sachstand Kenntnis genommen.

Ziff. 5.3.2 Sicherheitsüberprüfung

Mehrfach habe ich den Senator für Inneres und Sport darauf hingewiesen, daß das Verfahren der Sicherheitsüberprüfungen für die öffentlich Bediensteten Bremens einer gesetzlichen Grundlage bedarf. Der Bund hat hierzu einen Gesetzentwurf im Rahmen seiner Regelungskompetenz, d. h. für die Bundesbediensteten, vorgelegt; das Gesetzgebungsver-

fahren steht derzeit kurz vor dem Abschluß. Unabhängig davon hatte ich gefordert, nicht erst dieses Gesetzgebungsverfahren abzuwarten, sondern umgehend ein entsprechendes bremisches Gesetz zu schaffen.

Der Datenschutzausschuß teilt meine Auffassung und hat den Senator für Inneres und Sport gebeten, die landesgesetzliche Regelung für die Sicherheitsüberprüfungen vorzubereiten.

Ziff. 5.4.1 Meldung von Drogenkonsumenten an die Führerscheinstelle

Der Senator für Inneres und Sport hat unter meiner Beteiligung einen Erlaß an die Polizeidienststellen herausgegeben mit der Anweisung, Drogenkonsumenten, die beim Fahren eines Kfz angetroffen würden, den entsprechenden Führerscheinstellen mitzuteilen.

Nach der Entscheidung des Bundesverfassungsgerichts, wonach der einmalige Haschischgebrauch nicht unbedingt dazu führt, daß eine Fahreignung als nicht mehr vorhanden angesehen werden kann, hat die Führerscheinstelle auf Anweisung des Senators für Inneres und Sport die Praxis dahingehend geändert, daß bei einmaligen Fällen keine Konsequenzen gezogen werden. Der Datenschutzausschuß hat hiervon Kenntnis genommen.

Ziff. 5.5.1 Bevölkerungsstatistik

Hierbei ging es um das von mir problematisierte Verhältnis von Bundes-, Landes- und Kommunalstatistik, die in Bremen einheitlich vom Statistischen Landesamt durchgeführt werden. Nach Ansicht des Statistischen Landesamtes gibt es keine gesetzliche Pflicht zur Trennung der Statistikbereiche. Ich habe darauf hingewiesen, daß im Bundesstatistikgesetz, in Einzelgesetzen wie im Volkszählungsgesetz, aber auch im Landesstatistikgesetz zwischen Kommunal- und Landesstatistiken unterschieden wird. Kommunalstatistiken werden durch Ortsgesetz geregelt.

Der Datenschutzausschuß erwartet, daß ich die konkreten Auswirkungen der Vermischung der Statistikebenen im Hinblick auf die Reidentifizierungsmöglichkeiten prüfe und ihm dann erneut berichte.

Ziff. 5.6.1 Überholte Dienstanweisung (Standesamt)

Seitdem die bremischen Standesämter DV-Technik bei der Erledigung ihrer Aufgaben einsetzen, habe ich wiederholt darauf hingewiesen, daß Teile dieses Datenverarbeitungssystems datenschutzrechtlich nicht ausreichend legitimiert sind, weil sie nicht auf eine gesetzliche Grundlage, sondern lediglich auf die "Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden" - also Verwaltungsvorschriften - gestützt werden.

Im Datenschutzausschuß war unstreitig, daß das Personenstandsgesetz um präzise Datenverarbeitungsregelungen ergänzt werden muß. Der Senator für Inneres und Sport erklärte, es gebe zwar einen ausgearbeiteten Entwurf zur Änderung des Personenstandsgesetzes, die Aussichten seien allerdings gering, daß die Bundesregierung noch in dieser Legislaturperiode den Gesetzentwurf einbringen werde.

Ziff. 5.7.1 Fall: Komplette Strafakten beim Stadtamt

Das Standesamt hatte vor Erteilung einer Gewerbeerlaubnis neben dem polizeilichen Führungszeugnis aus dem Bundeszentralregister auch komplette Strafakten über den Antragsteller bei der Staatsanwaltschaft Bremen angefordert und erhalten. Diese Strafakten enthielten auch Ermittlungsvorgänge mit einer Vielzahl von Angaben, die dem Bundeszentralregister gar nicht mitzuteilen sind bzw. in das Führungszeugnis gerade nicht aufgenommen worden waren, weil die Tilgungsvorschriften bei seiner Ausfertigung beachtet worden waren.

Der Datenschutzausschuß teilte meine Auffassung, daß die Datenübermittlung im Zusammenhang mit beruflichen Zulassungsverfahren einer gesetzlichen Grundlage bedarf,

für die allerdings der Bundesgesetzgeber zuständig ist. Übergangsweise hält es der Ausschuß für notwendig, bei der Zuverlässigkeitsprüfung für einen Beruf oder ein Gewerbe Anfragen bei der Staatsanwaltschaft nach Straftaten, die der beantragten Erlaubnis entgegenstehen können, so konkret abzufassen, daß die Staatsanwaltschaft in die Lage versetzt wird, die Relevanz der Delikte für das Zulassungsverfahren abzuschätzen und dann nach pflichtgemäßem Ermessen über das Auskunftsersuchen zu entscheiden. Auf keinen Fall dürften komplette Ermittlungsakten übersandt werden. Der Senator für Justiz und Verfassung hat den Inhalt dieses Ausschußvotums den Staatsanwaltschaften mitgeteilt.

Ziff. 9.2 Auskunftspflicht aufgrund Unterhaltspflicht

Vgl. u. Ziff. 8.6.2.

Ziff. 11.1 Einsichtsrecht in Umweltakten

Nachdem die Frist zur Umsetzung der EG-Richtlinie über den Zugang zu Informationen bei den Umweltbehörden am 31.12.1992 abgelaufen war, ohne daß der Bundes- bzw. die Landesgesetzgeber die erforderlichen gesetzlichen Regelungen geschaffen hatten, hatte der Senator für Umweltschutz und Stadtentwicklung einen Erlaß für sein Ressort und dessen nachgeordnete Ämter herausgegeben, der auf die unmittelbare Wirkung der EG-Richtlinie hinweist und einige Fragen der Auskunftserteilung regelt.

Die Beratungen im Datenschutzausschuß haben ergeben, daß der Umweltsenator weitere Maßnahmen zur Umsetzung der Richtlinie erst dann treffen will, wenn voraussichtlich Mitte 1994 das Gesetzgebungsverfahren für ein Umweltinformationsgesetz des Bundes abgeschlossen ist. Insbesondere soll dann geklärt werden, welche eigenen Gestaltungsmöglichkeiten das Land noch hat, um abweichend von der voraussichtlich restriktiven Auslegung der EG-Richtlinie durch das Bundesgesetz in Bremen einen umfassenden Zugang zu Umweltakten zu ermöglichen.

Ziff. 13.1 Die Landeshauptkasse als Sammelstelle für Belege

Die Verwaltungsvorschriften zu § 70 Landeshaushaltsordnung (LHO) verlangen, daß allen Kassenanordnungen die jeweiligen Belege beizufügen sind. Diese Belege enthalten eine Vielzahl personenbezogener Daten, die die Kasse für ihre eigentliche Aufgabenerfüllung, die Annahme oder Auszahlung eines Betrages und dessen Buchung, nicht benötigt. Ich sehe hierin einen Verstoß gegen das Gebot der Erforderlichkeit bei der Datenübermittlung.

Der Senator für Finanzen hat dazu erklärt, daß in Zukunft die Kassenanordnungen mit Hilfe der automatisierten Datenverarbeitung über Diskette an die Landeshauptkasse gegeben werden sollen und auf die Beifügung der Belege dann verzichtet werde. Der Datenschutzausschuß ist jedoch der Auffassung, daß darauf schon jetzt verzichtet werden kann. Er erwartet, daß die Verwaltungsvorschriften zu § 70 LHO bis Mitte 1994 entsprechend geändert werden.

1.5. Tabelle der durch Gesetzesänderungen im Jahr 1993 eingeführten Mitteilungspflichten und Datenübermittlungen

Die Tabelle auf den folgenden Seiten gibt den Versuch wieder, in einer graphisch aufbereiteten Übersicht darzustellen, welche Möglichkeiten des Datenabgleichs, der Rasterkontrolle, der Mitteilung an andere Behörden und der Erhebung bei dritten Stellen der Gesetzgeber im Jahr 1993 neu geschaffen hat. Ein Anspruch auf Vollständigkeit soll und kann nicht erhoben werden.

Tabelle der durch Gesetzesänderungen im Jahr 1993 neu eingeführten Mitteilungspflichten und Datenübermittlungen

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Arbeitslose/Arbeitgeber	Arbeitgeber auch Arbeitnehmer	Arbeitsamt	Außenprüfung im Betrieb/ Einsicht in Unterlagen/ Überprüfung von Personalien/ Auskünfte der Betroffenen/ggf. Bereitstellung der Daten auf maschinenverwertbaren Datenträgern oder in Form von Listen	Identifikationsdaten und Beginn/Ende/Entgelt/ Arbeitszeit der Beschäftigung	Aufdeckung und Verfolgung von Leistungsmißbrauch	§ 132 a AFG (01.01.1993)
Arbeitslose/Arbeitgeber	Arbeitgeber auch Arbeitnehmer	Arbeitsamt/Hauptzollämter	Einsicht in Melde-, Lohnlisten o. ä./Überprüfung von Personalien/Auskünfte der Betroffenen/ggf. Bereitstellung der Daten auf maschinenverwertbaren Datenträgern oder Datenlisten/Außenprüfung im Betrieb	alle erforderlichen Daten	Unberechtigter Bezug von Leistungen	§ 132 a aufgehoben, ersetzt durch § 150 a AFG (FKPG, 01.07.1993)
Arbeitslose	Betroffene	Arbeitsamt	Hinterlegung bei Leistungsbezug	Lohnsteuerkarten	s. o.	§ 150 b AFG (FKPG, 01.07.1993)

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Arbeitslose	Krankenkassen/Träger der Rentenversicherung/Ausländerbehörden/Berufsgenossenschaften/u. a.	Arbeitsämter	Datenaustausch	alle erforderlichen Daten	Unberechtigter Bezug von Daten/Unterstützung der Prüfungen nach § 150 a AFG	§ 150 a Abs. 2 AFG (FKPG, 01.07.1993)
Arbeitslose	selbst	Arbeitsamt	regelmäßige Meldung im Amt/Teilnahme an Maßnahmen der Arbeitsberatung Aufforderung soll alle drei Monate ergehen/ärztliche, psychologische Untersuchung	Präsenz des Betroffenen Persönliche Eignung	Verhinderung von Schwarzarbeit	§ 132 Arbeitsförderungsgesetz (AFG) ergänzt durch 1. SKWPG (01.01.1994)
Asylbewerber	Arbeitgeber	Sozialämter (zuständige Asylbewerberstelle)	konventionell	Personalien und Daten über die Aufnahme bzw. Beendigung von Beschäftigung	Leistungkürzung bzw. Überwachung	Asylbewerberleistungsgesetz
Asylbewerber	Sozialbehörden (zuständige Asylbewerberstelle)	Statistisches Bundesamt Statistisches Landesamt	unbestimmt	umfangreiche Datenkategorien	Beurteilung der Wirkung des Asylbewerberleistungsgesetzes	Asylbewerberleistungsgesetz
Asylbewerber	Ausländeramt	Sozialbehörden	konventionell	Personalien und Aufenthaltstitel	Unterbringung	Asylverfahrensgesetz
Asylbewerber	Ausländeramt	Polizeibehörden	konventionell	Personalien		Asylverfahrensgesetz

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Asylbewerber	Ausländeramt	Polizeibehörden (INPOL)	Fingerabdruckbögen	Fingerabdrücke	Doppelidentitäten	Asylverfahrensgesetz
Asylbewerber	Ausländeramt	Polizeibehörden	konventionell	Personalien		Asylverfahrensgesetz
Bezieher von Erziehungsgeld	Betroffene	Sozialämter	Vorlage	Bescheinigung des Arbeitgebers über Andauer von Erziehungsurlaub/Teilzeitarbeit	Prüfung der Anspruchsberechtigung	§ 7 Abs. 3 Bundeserziehungsgeldgesetz (FKPG, 01.07.1993)
Bezieher von Wohngeld	Betroffene	Amt für Wohnung und Städtebauförderung	Mitteilung	Verringerung der Miete bzw. Erhöhung des Einkommens	Prüfung der Anspruchsberechtigung	§ 29 Abs. 3 Wohngeldgesetz (FKPG, 01.07.1993)
Eltern von Kindern, die Angebote der Jugendarbeit/der Erziehungshilfe in Anspruch nehmen bzw. einen Kindergarten besuchen	selbst	Jugendämter	Auskunft/Vorlage von Unterlagen/Zustimmung zu ihrer Vorlage	Einkommens- und Vermögensverhältnisse/ Arbeitgeber/Art des Beschäftigungsverhältnisses	Berechnung/Erlaß/ Übernahme von Teilnahmebeiträgen	§ 97 a Kinder- und Jugendhilfegesetz (1. Änderungsgesetz, 01.04.1993)
Exporteure	Bundesausfuhramt	an verschiedene andere Behörden	konventionell	alle bekanntgewordenen Daten, die mit der Ausfuhr zusammenhängen	zur Verhütung und Verfolgung von Straftaten gegen Außenwirtschaftsbestimmungen (unbestimmt)	Außenwirtschaftsgesetz

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Geldanleger (Bausparer)	Finanzbehörden	Banken und Bausparkassen	konventionell kann von den Finanzbehörden vorgeschrieben werden	Personalien und Bausparsumme und Höhe der Wohnungsbauprämie	Rationalisierung bei der Abwicklung der Sparzulage	Einkommensteuergesetz
Geldanleger (Sparer)	Banken	Bundesamt für Finanzen	Datenabgleiche und Datenübermittlung durch elektronische Datenträger	Personalien von Sparer und Ehegatten, Konto-Nr. und Verteilung des Freistellungbetrages	Unvollständige Freistellungsaufträge bzw. falsche Verteilung	Erweiterung der elektronischen Möglichkeiten der Überwachung nach dem Zinsabschlagsgesetz bzw. der entsprechenden VO
Geldanleger (Sparer)	Finanzbehörden	Arbeitgeber, Banken und andere Geldinstitute	konventionell in Listenform	Bewilligungsbescheid über die Gewährung der Arbeitnehmersparzulage einschl. Personalien, Konto-Nr., Art der Verträge, Höhe der Sparzulage	Rationalisierung bei der Abwicklung der Sparzulage	Einkommensteuergesetz
Geldanleger bzw. Geldeinzahler oder Versicherungsnehmer	Banken und Versicherungen	eigene Aufbewahrungsverpflichtung und Datenübermittlung bzw. Auskunft an Strafverfolgungsbehörden	konventionell und elektronisch	Identifizierungsdaten der Geldanleger über DM 20.000,-- und Art der Geldanlage	Verhinderung und Aufdeckung von "Geldwäsche"	Geldwäschegesetz

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Geldanleger bzw. Geldeinzahler oder Versicherungsnehmer	Banken und Versicherungen	Sicherungsmaßnahmen, d.h. Vorkehrungen zu treffen, die Geldwäsche verhindern oder aufdecken	beliebig	lfd. Aufzeichungen über alle Anlagegeschäfte und Versicherungsabschlüsse	Verhinderung und Aufdeckung von "Geldwäsche"	Geldwäschegesetz
gesetzlich Krankenversicherte	Ärzte	Kassenärztliche Vereinigungen/Krankenkassen	Datenbänder/andere maschinell verwertbare Datenträger	ärztliche Diagnose	Abrechnung	§ 295 Abs. 1 SGB V (Gesundheitsstrukturgesetz, GSG 93, 01.01.1993)
gesetzlich Krankenversicherte	Ärzte	Krankenkassen	?	Angaben über ärztliche Leistungen, die zur Prüfung späterer Leistungsgewährung durch die Kassen erforderlich sind	?	§ 295 Abs. 2 a SGB V (2. SGB-ÄndG, ...)
gesetzlich Krankenversicherte	Krankenhäuser	Krankenkassen	maschinenlesbar	Einweisungsdiagnose/ bei Änderung der Aufnahmediagnose die weiteren Diagnosen/ voraussichtliche Dauer der Behandlung/bei Überschreiten medizinische Begründung/ Datum und Art von Operationen	Abrechnung	§ 301 Abs. 1 SGB V (GSG 93, 01.01.1993)

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Im- und Exporteure	Zollbehörden	"Zollbehörden" der europäischen Union	elektronischer Datenaustausch über Zollinformationsystem	Daten über Warenverkehre und die beteiligten Händler	Beschleunigung der Zollabwicklung und der Überwachung gegen zollrechtliche und förderungsrechtliche Vorschriften	Europäischer Zollvertrag
Kfz-Halter	Finanzamt (alt)	Finanzamt (neu)	konventionell	Käuferdaten bei Veräußerung des Kfz.	Feststellung der Steuerpflicht ohne Rücksicht auf evtl. Stillegung	Kfz.-Steuer DurchführungsVO
Kfz-Halter	Kraftfahrzeugbehörden	Finanzbehörden	Datenabruf	Personalien des Halters und Einstufung des Kfz in eine Emmissionsklasse	Feststellung der Kfz.-Steuer	Kfz.-SteuerG. und FahrzeugregisterVO
Kindergeldempfänger	Arbeitsamt	Arbeitgeber	Sammellisten und Sammelüberweisungen über die Bezieher von Kindergeld im Betrieb	Personalien des Arbeitnehmers und seiner berechtigten Kinder	Auszahlung von Kindergeld	Bundeskindergeldgesetz
Landwirte	Satellitenaufnahmen der EG	Landwirtschaftsbehörden und -kammern	Datenabgleiche	Größe der Flächen, Nutzung und Anbau über eine Wachstumsperiode und vorhergehende Nutzung	Aufdeckung von falschen Angaben beim Subventionsbezug	Integriertes Verwaltungs- und Kontrollsystem der EG

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Sozialhilfeempfänger	Arbeitsämter/Träger der gesetzlichen Unfall- und Rentenversicherung (Auskunftsstellen) über zentrale Vermittlungsstellen (Kopfstellen)	Sozialämter	regelmäßiger automatisierter Datenabgleich	Bezug von Leistungen bei den Auskunftsstellen/Zeiten einer Versicherungspflicht/ Zeiten geringfügiger Beschäftigung/ Identifikationsdaten/Sozialversicherungsnummer	Ausschluß von Doppelbezug	§ 117 Abs. 1 BSHG (FKPG, 01.07.1993) und noch zu erlassende Rechtsverordnung des Bundes
Sozialhilfeempfänger	Sozialämter	Sozialämter	regelmäßiger automatisierter Datenabgleich	Sozialhilfeleistungen/ Identifikationsdaten	Ausschluß von Doppelbezug	§ 117 Abs. 2 BSHG (FKPG, 01.07.1993) und noch zu erlassende Rechtsverordnung des Bundes
Sozialhilfeempfänger	Andere Stellen der Verwaltung/Wirtschaftliche Unternehmen von Trägern der Sozialhilfe	Sozialämter	Einzelabfragen (umstritten, z. T. automatisierter Datenabgleich praktiziert!)	Identifikationsdaten/ Leistungen kommunaler Daseinsfürsorge/Eigenschaft als Kfz.-Halter	Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe	§ 117 Abs. 3 BSHG (FKPG, 01.07.1993)
Sozialleistungsempfänger bzw. Antragsteller	Sozialleistungsträger	Sozialleistungsträger	Einzelanfrage/Gruppenanfrage, nach Maßgabe von § 79 SGB X (i. d. F. des 2. SGB-ÄndG) auch automatisierter Direktabruf	alle Sozialdaten	Erfüllung der jeweiligen gesetzlichen Aufgabe	§§ 67 a Abs. 2 Nr. 1, 69 Abs. 1 Nr. 1 SGB X (2. SGB-ÄndG, ...)

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Steuerzahler	Finanzbehörden	Gemeinden und öffentlich-rechtliche Körperschaften	konventionell auf Anforderung, im Wege des Datenaustausches und durch Abruf	Daten von Grundsteuerpflichtigen	Erweiterung der Durchbrechung des Steuergeheimnisses für alle Aufgaben der öffentlichen Verwaltung	Abgabenordnung (§ 31)
Steuerzahler	Finanzbehörden	Sozialbehörden	konventionell oder durch Datenabgleich	Personalien, Steuernummer und zu versteuerndes Einkommen	Aufdeckung von Sozialbezug trotz Einkommen	Abgabenordnung (§ 31a)
Steuerzahler	Finanzbehörden	Arbeitsämter	konventionell oder durch Datenabgleich	Personalien, Steuernummer und zu versteuerndes Einkommen	Aufdeckung von Bezug von Arbeitslosengeld trotz Einkommen	Abgabenordnung (§ 31 a)
Steuerzahler	Finanzbehörden	Ausländerbehörden	konventionell oder durch Datenabgleich	Personalien, Steuernummer und zu versteuerndes Einkommen	Aufdeckung von Einkommensbezug trotz fehlender Arbeitserlaubnis	Abgabenordnung (§ 31a)
Steuerzahler	Finanzbehörden	Förderungsbehörden - Wirtschaftsförderung - Wohnnugsförderung - Inovationsförderung - Umweltförderregelung	konventionell oder durch Datenabgleich	Personalien, Steuernummer und zu versteuerndes Einkommen	Aufdeckung von Bezug von Förderungsmaßnahmen trotz Einkommen	Abgabenordnung (§ 31a)
Steuerzahler	Finanzbehörden	Gewerbebehörden	konventionell oder durch Datenabgleich	Personalien, Steuernummer und zu versteuerndes Einkommen	Aufdeckung von fehlender wirtschaftlicher Leistungsfähigkeit	Gewerbeordnung

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Steuerzahler	Lohnsteuerkartenstellen	Arbeitsämter	konventionell	Personalien und Tatsache der Ausstellung einer Ersatzlohnsteuerkarte	Aufdeckung von Arbeitsverhältnissen trotz Bezug von Arbeitslosengeld	Einkommensteuergesetz (§ 39)
Steuerzahler	Lohnsteuerkartenstellen	Finanzbehörden	konventionell	Personalien und Tatsache der Ausstellung einer Ersatzlohnsteuerkarte	unbekannt und aus der Gesetzesmaterie nicht erkennbar	Einkommensteuergesetz
Steuerzahler	Steuerzahler Arbeitgeber Banken u.a.	Finanzbehörden	Datenträgeraustausch Datenfernübertragung	je nach Steuervorschrift	Rationalisierung mit Zustimmung des Meldepflichtigen; der evtl. Betroffene (Arbeitgeber) wird nicht um Zustimmung ersucht.	Abgabenordnung (§ 150)
Steuerzahler	Finanzbehörden	Finanzbehörden	konventionell und elektronisch in jeder Form	beliebig und unbestimmt. Alle Daten, die für ein Steuerverfahren von Vergleichsinteresse sein könnten	Vergleichszahlen und -werte für zukünftige Steuerverfahren	Abgabenordnung (§ 88 a)
Touristen und Händler	Zoll	Zollinformationssystem der EU	Datenfernübertragung	Personalien, bes. Kenntnisse bei der Zollabfertigung, Fotos, Methoden beim Grenzübertritt und bes. Waren	Zollüberwachung	Amtshilfevorschriften der Mitgliedstaaten der EU in Zollangelegenheiten

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Versicherter der gesetzlichen Unfallversicherung (Arbeitnehmer)	Ärzte	Träger (Berufsgenossenschaft) oder Spitzenverband der gesetzlichen Unfallversicherung	offen	Sozialdaten	Durchführung eines bestimmten, genehmigten Forschungsvorhabens	§ 100 a SGB X (2. SGB-ÄndG, ...)
Wehrpflichtige	Meldebehörden	Kreiswehrersatzämter	Datenübermittlung	Meldedaten von männlichen Bürgern, deren Daten sich zwischen dem 17. und 32. Lebensjahr ändern	Wehrüberwachung	Wehrpflichtgesetz
Wehrpflichtige	Erfassungsbehörden Wehrersatzämter B.f. den Zivildienst	Bundesverwaltungsamt	Datenübermittlung		Wehrüberwachung und Ausschreibung	Wehrpflichtgesetz
Wehrpflichtige	Bundesverwaltungsamt	Meldebehörden Wehrersatzämter B.f. den Zivildienst Auswärtiges Amt Grenzpolizeibehörden	Datenübermittlung	Daten von Wehrpflichtigen, deren Aufenthalt unbekannt ist	Wehrüberwachung	Wehrpflichtgesetz

2. Schwerpunkte

2.1. Eingaben und Öffentlichkeitsarbeit

2.1.1. Eingaben und Bürgerkontakte

Im Berichtszeitraum erhielt ich insgesamt 143 schriftliche Beschwerden bzw. Eingaben. Die 65 Eingaben, die die Datenverarbeitung privater Unternehmen betrafen, richteten sich im wesentlichen gegen Versicherungen, Banken und Auskunfteien (vgl. Ziffern 13.2. und 13.3.). In den 78 Eingaben und Beschwerden im Bereich der öffentlichen Verwaltung Bremens und Bremerhavens ging es vorrangig um Datenschutzprobleme bei der Polizei sowie im Sozial- und Gesundheitswesen. Mehrfach angesprochen wurden auch das Einsichtsrecht in sowie die Weitergabe von Personalakten.

Nicht gezählt werden kann die Vielzahl telefonischer Anfragen, Hinweise oder Beratungsersuchen.

2.1.2. Presse- und Öffentlichkeitsarbeit

Praktizierter Datenschutz ist darauf angewiesen, daß die Bürgerinnen und Bürger ihre Rechte kennen und selbst ausüben. Immer noch wird zu wenig von den in den Datenschutzgesetzen vorgesehenen Ansprüchen auf Auskunft, Berichtigung, Sperrung und Löschung Gebrauch gemacht. Diesen Zustand zu ändern ist Daueraufgabe der Datenschutzbeauftragten.

Ich habe daher zusammen mit meinen Kollegen aus Hamburg und Niedersachsen - letzterer hatte den Hauptanteil an der Redaktion - im Dezember 1993 eine Informationsbroschüre mit der Überschrift "Tips zum Adressenhandel und gegen die Werbepapierflut im Briefkasten" herausgegeben (vgl. die Ankündigung im 15. JB, Ziff. 2.1). Sie behandelt in leicht lesbarem Stil die rechtlichen Möglichkeiten des Bürgers, sich gegen unerwünschte Direktwerbung zur Wehr zu setzen.

Diese Form des Marketings und seine Begleiterscheinungen wie Adreßhandel, lettershops usw. haben in den letzten Jahren stark zugenommen und werden durch den europäischen Binnenmarkt noch intensiviert. Zugenommen haben dementsprechend auch die Eingaben und Beschwerden von Personen, die diese Form der geschäftlichen Kontaktaufnahme als aufgezwungen und belästigend empfinden. Das durch das novellierte Bundesdatenschutzgesetz von 1990 neu eingeführte Recht auf Widerspruch gegen die Nutzung oder Übermittlung der eigenen Daten für Werbezwecke oder für die Markt- oder Meinungsforschung (§ 28 Abs. 3 BDSG) ist noch kaum bekannt. Aufgrund mehrerer Berichte in Rundfunk und Presse Bremens fand das Informationsblatt einen "reißenden Absatz". Insgesamt wurden ca. 500 Stück an Einzelpersonen und interessierte Organisationen wie Verbraucherverbände, Gewerkschaften usw. versandt.

Meine Pressemitteilungen und Rundfunkstatements zu aktuellen Themen bezogen sich u.a. auf

- die in Bremen immer noch bestehende Praxis der Regelüberprüfung von Bewerbern für den Richter- und den Polizeidienst beim Verfassungsschutz,

- das im Juni 1993 verabschiedete Gesetz zur Bekämpfung der Organisierten Kriminalität,

- die Wahrung der Vertraulichkeit in den Beratungsstellen für Schwangere nach dem § 218-Urteil des Bundesverfassungsgerichts,

- die verbreitete "Kontrollhysterie" bei der Eindämmung des sog. Leistungsmißbrauchs im Sozialbereich,

- die datenschutzrechtlichen Risiken bei einer Verarbeitung sensibler Daten von Behörden, öffentlichen Krankenhäusern etc. durch private Rechenzentren,

- die unzulängliche Berichtigungspraxis bei den Empfängern von Listen aus dem Schuldnerverzeichnis,

- die Überprüfung von Bankkunden nach dem neuen "Geldwäschegesetz",

- die Aktenfunde durch Gefangene in der Justizvollzugsanstalt Oslebshausen,

- die Gefährdung des Sozialgeheimnisses der Klienten in einigen bremischen Sozialämtern durch die dort bestehende Raumnot und

- die Risiken der Einführung einer Chipkarte für Patienten.

2.2. Auf dem Weg zur Privatisierung? - Informations- und Kommunikationsstruktur Bremens in neuen Rechtsformen

2.2.1. Eigenbetriebe statt Ämter

Am 25. Januar 1994 hat die Stadtbürgerschaft die beiden Gesetze beschlossen, mit denen die bisherigen Ämter "Rechenzentrum der Bremischen Verwaltung (RbV)" und "Fernmeldetechnisches Amt (FTA)" rückwirkend zum 1. Januar 1994 in Eigenbetriebe umgewandelt wurden (Bremisches Informations- und Datentechnikortsgesetz - BremIDOG, Bremisches Ortsgesetz Bremer Kommunikationstechnik - BremBKOG). In Teilen der Koalition bestehende Vorstellungen über eine Privatisierung dieser beiden Bereiche wurden - zumindest vorerst - nicht realisiert. Der Senat hat jedoch beschlossen, bis zum Jahresende 1994 auch Kauf- und Kooperationsangebote von privaten Unternehmen einzuholen bzw. zu prüfen sowie hierfür externe Gutachten einzuholen.

Sicherlich sind für diese Umwandlungen ebenso wie für die weitergehenden Privatisierungsüberlegungen in erster Linie durch die Haushaltsnotlage Bremens bedingte fiskalische Motive maßgeblich. Bei der Änderung von Rechtsformen in der IuK-Struktur eines Landes sind jedoch immer auch ggf. gravierende datenschutzrechtliche Konsequenzen zu gewärtigen. Im nicht-öffentlichen Bereich, also bei privaten Unternehmen, ist - vereinfacht formuliert - das Datenschutzniveau im Vergleich mit dem öffentlichen Bereich (Behörden) geringer; der Eigenbetrieb steht dazwischen. Die praktische Relevanz des jeweils gewährleisteten Datenschutzstandards für die Bürgerinnen und Bürger Bremens wird deutlicher, wenn man sich vergegenwärtigt, welche Zusammenballung teilweise sensibelster Daten im bisherigen Rechenzentrum der bremischen Verwaltung stattfindet. Verarbeitet werden dort u.a. Angaben der Polizei, der Melde-, Paß- und Personalausweisstellen, der Sozial-, Wohngeld- und BAföG-Ämter, der Steuerverwaltung und der Krankenhäuser. Das bisherige Fernmeldetechnische Amt war bzw. ist wiederum zuständig für die Abwicklung des behördlichen Telefon- und Funksprechverkehrs der gesamten bremischen Verwaltung.

Angesichts dieser Risikodimension lege ich bei wichtigen Vorhaben zur Umgestaltung der IuK-Struktur in Bremen um so größeren Wert darauf, rechtzeitig beteiligt zu werden und meine Vorstellungen einbringen zu können. Dies war aus im einzelnen nicht mehr völlig aufklärbaren Umständen bei beiden genannten Gesetzen nicht der Fall. Eine von mir erbetene Einladung zur Sitzung der Finanzdeputation, in der das BremIDOG abschließend beraten wurde, erging nicht. Korrekturwünsche konnte ich daher erst über den Datenschutzausschuß einbringen.

2.2.2. Datenschutzrechtliche Vorgaben

Der Ausschuß verständigte sich mit den Stimmen der Koalitionsvertreter darauf, die Vorschrift des § 2 Abs. 5 BremIDOG zu ergänzen. Diese Bestimmung sah zwar bereits im Entwurf vor, daß bisher beim Eigenbetrieb für bremische Behörden betriebene Datenver-

arbeitung, die aus Datenschutzgründen nicht durch Dritte vorzunehmen ist, dort verbleiben soll. Doch kann von diesem Grundsatz durch eine Ausnahmeentscheidung des Senats abgewichen werden. Die von mir initiierten Ergänzungen stellen klar, daß Rechtsvorschriften, die eine Auftragsverarbeitung "bremischer" Daten insbesondere durch private Rechenzentren ausschließen oder einschränken, auch bei solchen Ausnahmenentscheidungen des Senats unberührt bleiben (§ 2 Abs. 5 Satz 3 BremIDOG). Für den neuen Eigenbetrieb wurde in § 10 Abs. 3 Satz 2 die Restriktion aufgenommen, daß er an private DV-Firmen keine Aufträge bzw. Unteraufträge vergeben soll, wenn es sich um Daten handelt, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, also etwa Steuer-, Sozialhilfe - oder Patientendaten. Dieser Grundsatz wurde aus Ziff. 8.1.2 der Allgemeinen Vorschriften zur Durchführung des Bremischen Datenschutzgesetzes (AVV- BrDSG, Brem.ABl. 1989, S. 379) übernommen und in Gesetzesrang erhoben.

Meinen weitergehenden Änderungswunsch, ein Anhörungsrecht des Landesbeauftragten bei den im BremIDOG vorgesehenen Ausnahmeentscheidungen des Senats ausdrücklich festzuschreiben, habe ich im Hinblick auf die begrenzte Reichweite eines Ortsgesetzes zurückgestellt. Ich werde auf die notwendige rechtliche Absicherung der rechtzeitigen Einschaltung des Datenschutzbeauftragten bei der in Kürze anstehenden Novellierung des BrDSG zurückkommen.

In meiner Stellungnahme vom 8. November 1993 gegenüber der Senatskanzlei und den Senatoren für Wirtschaft, Finanzen, Justiz, Umweltschutz sowie der SKP habe ich zum einen Normen des bremischen Landesrechts in Erinnerung gebracht, die die Auslagerung behördlicher Datenverarbeitung vor allem an private DV-Unternehmen einschränken können. So erlaubt § 1o Abs. 1 des Bremischen Krankenhausdatenschutzgesetzes die externe Verarbeitung von Patientendaten nur, wenn die Wahrung der verschärften Bestimmungen dieses Gesetzes beim Auftragnehmer "sichergestellt" ist. § 1o Abs. 1 des Landesstatistikgesetzes enthält die gleiche Voraussetzung im Hinblick auf die im Statistikbereich geltenden strengeren Regelungen. Welche Dateien und Verarbeitungsverfahren der bremischen öffentlichen Verwaltung im Rahmen des geltenden Datenschutzrechts zulässigerweise von privaten Verarbeitern übernommen werden können, wäre mithin ggf. im Einzelfall sorgfältig unter dem Blickwinkel zu prüfen, ob der bisher eingehaltene rechtliche wie technische Datenschutzstandard auch nach dem "Outsourcing" gesichert bleibt. Selbstverständlich sind diese "Datenschutz-Kosten" auch bei der Angebots- Kalkulation und dem Vergleich mit dem Kostenaufwand der bisherigen bearbeitenden Stelle - sei es die Behörde selbst oder der Eigenbetrieb - zu berücksichtigen.

2.2.3. Drohende Kontrolldefizite

Ein zweiter Aspekt betrifft meine Kontrollmöglichkeiten. Während meine Kontrollbefugnisse nach der Umwandlung eines Amtes in einen Eigenbetrieb untangiert bleiben, da es sich auch bei einem Eigenbetrieb um eine bremische öffentliche Stelle i.S.v. § 1 Abs. 2 BrDSG handelt, verschlechtern sich meine Überwachungsmöglichkeiten bei der Auftragsvergabe an eine Privatfirma erheblich. Zwar sieht § 8 Abs. 1 Satz 3 BrDSG in diesen Fällen vor, daß das Unternehmen die Bestimmungen des Bremischen Datenschutzgesetzes zu beachten hat und sich der Kontrolle des Bremischen Landesbeauftragten unterwerfen muß. In der Praxis lassen sich diese Kontrollrechte jedoch aus Kapazitäts- wie finanziellen Gründen nur schwer realisieren, wenn der externe Verarbeiter seinen Sitz in anderen Bundesländern hat oder - wie dies bei großen Systemhäusern der Fall sein kann - die DV-Produktion an wechselnden Orten je nach freien Kapazitäten in unterschiedlichen unternehmenseigenen oder sogar von Unterauftragnehmern betriebenen Rechenzentren erfolgt. Aktuellstes Beispiel für ein solches "Outsourcing"-Vorhaben ist die geplante Verarbeitung der Beschäftigtendaten der städtischen Krankenhäuser durch ein kirchliches Rechenzentrum in Nordrhein - Westfalen.

Das Bremische Datenschutzrecht bildet kein prinzipielles Hindernis für eine Privatisierung behördlicher Datenverarbeitung. Es verlangt jedoch eine "Bestandssicherung", sowohl was die materielle Wahrung des Persönlichkeitsrechts als auch was den organisatorisch-technischen Schutzstandard angeht. Wird eine Vergabe an Dritte ins Auge gefaßt,

ist der Landesbeauftragte für den Datenschutz frühzeitig zu beteiligen. Nur dann lassen sich rechtzeitig die datenschutzrechtlichen Vorgaben feststellen und ggf. in die mit den Auftragnehmern abzuschließenden Verträge aufnehmen. Die für die zukünftige IuK-Struktur in Bremen von der SKP angekündigte Gesamtkonzeption (vgl. dazu Ziff. 2.3.2.1.) muß auch den Rahmen für Inhalt und Umfang der Privatisierung von DV-Dienstleistungen festlegen.

2.3. Entwicklung der Informations- und Kommunikationstechnik

2.3.1. Abhörrisiken bei Mobiltelefonen und im Funkverkehr

Die zu diesem Thema bereits im letzten Berichtszeitraum von mir ergriffenen Aktivitäten (vgl. 15. Jahresbericht Ziff. 2.2.3.) habe ich fortgeführt.

2.3.1.1. Mobiltelefone

In Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz Niedersachsen und dem Hamburgischen Datenschutzbeauftragten habe ich im Auftrag der Konferenz der Datenschutzbeauftragten einen Bericht zur Netzsicherheit im Mobilfunk erstellt, der die datenschutzrechtlichen Risiken und Problemfelder zusammenfassend darstellt. Hierzu zählen insbesondere

- Abhörrisiken auf Luftschnittstellen;

- die Geheimhaltung der Verschlüsselungsalgorithmen der digitalisierten Netze (D1- und D2-Netz) für Mobiltelefone. Deren Sicherheit ist nur solange gegeben, wie die Verfahren tatsächlich geheim bleiben, im Gegensatz zu offengelegten - und trotzdem sicheren - Verschlüsselungsverfahren, bei denen die Sicherheit alleine durch die Geheimhaltung der Schlüssel erreicht wird;

- die Möglichkeit, über die Verbindungsdaten ein Bewegungsmuster zu erstellen, sowie

- die große Anzahl der Diensteanbieter, die Dienstleistungen bei den Netzbetreibern einkaufen und an die Benutzer und Benutzerinnen von Mobiltelefonen weiterverkaufen (sog. Service-Provider); sie verarbeiten zu Abrechnungszwecken die Verbindungs- und Stammdaten ihrer Kunden und Kundinnen.

Bei der Satellitenkommunikation kommen noch zwei weitere Punkte hinzu:

- die große Fläche, die im Sendebereich eines Satelliten liegt (zumeist große Teile Europas). In diesem sogenannten Abstrahlbereich des Satelliten kann das Signal empfangen werden. Nur durch eine Kennung in der Hardware des satellitengestützten Mobiltelefones erkennt ein Gerät, welche Signale für dieses Gerät bestimmt sind. Hier bestehen Manipulationsmöglichkeiten an der Hard- und oder Software;

- die multinationalen Eigentumsverhältnisse, denen kein multinationales Datenschutzrecht gegenüber steht.

Dieser Bericht mündete in eine Entschließung der Konferenz der Datenschutzbeauftragten (vgl. Ziff. 15.3). In dieser wird gefordert, daß

- Hersteller und Betreiber mobiler Kommunikationsdienste den Gefahren für das Fernmeldegeheimnis und den Datenschutz durch entsprechende Gestaltung entgegenwirken und technische Vorkehrungen für eine sichere Kommunikation treffen,

- Teilnehmer und Teilnehmerinnen mobiler Kommunkationsdienste umfassend über die mit der Nutzung verbundenen Risiken und das erreichte Sicherheitsniveau aufgeklärt werden,

- die realisierten Sicherheitsmerkmale bei bestimmten Diensten - z.B. den digitalen D-Netzen - für die Aufsichts- und Kontrollorgane nachprüfbar sind und

- internationale Regelungen getroffen werden, die den Datenschutz bei mobiler Kommunikation gewährleisten.

2.3.1.2. Funkverkehr der Behörden und Organisationen mit Sicherheitsaufgaben (BOS)

Der im September 1992 gegründete Ad-hoc-Ausschuß "Sicherung des Funkverkehrs" der Technischen Kommission des AK II der Konferenz der Innenminister des Bundes und der Länder (vgl. 15. Jahresbericht, Ziff. 2.2.3.4.) empfahl der Technischen Kommission die bundesweite Einführung der Sprachverschleierung (Invertierung). Dadurch sollte erreicht werden, daß das Abhören des Funkverkehrs im Bereich der Behörden und Organisationen mit Sicherheitsaufgaben (BOS-Funkverkehr) erschwert würde.

Das Verfahren der Sprachverschleierung wurde vom Arbeitskreis Technik der Datenschutzbeauftragten-Konferenz als nicht brauchbar bezeichnet. Die Invertierung kann mit einfachen Inverterschaltungen, die bei manchen Frequenz-Scannern sogar schon zur Standardausrüstung gehören, wieder rückgängig gemacht werden. Durch Aktivierung der Inverterschaltung am Scanner sind nur noch die invertierten Nachrichten verständlich. Dies führt dazu, daß dann nur die Funksprüche, die von Dritten gerade nicht mitgehört werden sollen, verständlich sind, es also Unbefugten wesentlich einfacher gemacht wird, sensible Funksprüche "herauszufiltern" und abzuhören.

Der Vorsitzende der Konferenz der Datenschutzbeauftragten hat der Technischen Kommission diese Bedenken übermittelt. Diese hat von der Empfehlung, die Sprachverschleierung durch Invertierung bundesweit einzuführen, abgesehen und einen Ad-hoc-Ausschuß gebildet, der weitere technologisch und wirtschaftlich in Frage kommende Übergangssysteme auf ihre Einsatztauglichkeit hin untersuchen soll.

Dieser Sachstand ist unbefriedigend. Es bleibt zu hoffen, daß die grundsätzlich beschlossene Normung eines digitalisierten BOS-Funks, der dann auch wirksam verschlüsselt werden kann, durch die entsprechenden Stellen zügig vorangetrieben wird. Für die Übergangszeit ist weiter nach einer einigermaßen sicheren Lösung zu suchen. Diese hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (vgl. Ziff. 15.4) gefordert.

Für den Bremer Bereich ist zu bedauern, daß aus Kostengründen bei der Neugestaltung der Feuerwehrleitstelle davon abgesehen wurde, auf die abhörsicherere digitale Funktechnik umzusteigen.

2.3.2. Technikunterstützte Informationsverarbeitung (TuI) in Bremen

Hier läßt sich zwischen den organisatorischen und den technischen Entwicklungen unterscheiden.

2.3.2.1. Organisatorische Veränderungen

Bereits im letzten Berichtszeitraum deuteten sich Umstrukturierungen im Bereich technikunterstützter Informationsverarbeitung (TuI) an (vgl. 15. Jahresbericht Ziff. 2.2.1.). Eine Überarbeitung der gesamten Regelungen zur Planung und zum Einsatz von ADV in der bremischen Verwaltung ist beabsichtigt, wurde aber immer wieder verschoben. Der zuletzt von der SKP genannte Termin, bis zu dem der Entwurf eines TuI-Regelwerkes vorliegen soll, ist Ende Juni 1994. Ich erwarte, frühzeitig an der Gestaltung dieses Regelwerkes beteiligt zu werden. Insbesondere ist sicherzustellen, daß Verfahrensvereinfachungen nicht zu Informationsverlusten über die Planung und Beschaffung von ADV-Systemen führen, die meine Beratungs- und Kontrollbefugnisse beeinträchtigen.

Unter dieser Prämisse stehe ich Verfahrenserleichterungen - insbesondere im Bereich der Beschaffung von nichtvernetzten Arbeitsplatzrechnern - aufgeschlossen gegenüber.

2.3.2.2. Technische Entwicklungen

Im Bereich der Technik ist vor allem eine Ausbreitung der PC-Netze zu erwarten (s.u. Ziff. 2.3.4.).

FAX-Modems - Wählmodems mit FAX-Option

Des weiteren werden in immer mehr Bereichen statt eigenständiger FAX-Geräte **PC´s mit FAX-Modems** genutzt. Da inzwischen Modems, mit denen nur gefaxt werden kann, teurer sind als solche, die daneben auch zur sonstigen **Datenfernübertragung (DFÜ)** eingesetzt werden können (Modem mit FAX-Option), werden letztere verstärkt genutzt. Dabei ist bisher nicht berücksichtigt worden, daß diese Modems durch das Ermöglichen der DFÜ den Regelungen für die ADV-Beschaffung unterliegen und nicht nur den Regelungen für Geräte der "Telekommunikation". Daher ist das ADV-Antragsverfahren obligatorisch einzuleiten.

Die BreKom (Bremer Kommunikationstechnik, vormals FTA) ist im Februar 1994 auf Bitte des Gesamtpersonlrates zum Thema Wählmodems und **ISDN-Karten** an mich herangetreten mit dem Wunsch, mich an der Erarbeitung eines erforderlichen Datenschutzkonzeptes zu beteiligen.

Der Einsatz von **Wählmodems** bedeutet faktisch eine Vernetzung **aller** Arbeitsplatzrechner, die mit diesen Modems ausgestattet sind. Sind sie an halb oder voll amtsberechtigten Anschlüssen angeschaltet, können sie auch mit nicht zur bremischen Verwaltung gehörenden Rechnern vernetzt werden.

Vorbehaltlich einer ausführlicheren Stellungnahme habe ich die BremKom auf einige wesentliche Punkte hingewiesen, die beim Einsatz von Wählmodems und ISDN-Karten zu berücksichtigen sind:

- Nach § 4 Abs. 3 der "Dienstvereinbarung über den Betrieb und die Nutzung von Telekommunikationsanlagen (Fernsprechanlagen)" vom 15. Mai 1991 (Brem. ABl. S. 395) ist eine Nutzungserweiterung zur Datenübertragung nur im Rahmen genehmigter ADV-Verfahren zulässig.

- Nach § 6 Abs. 1 Nr. 6 BrDSG ist zu gewährleisten, daß "überprüft und festgestellt werden kann, an wen wann welche personenbezogenen Daten durch Einrichtungen zur Datenübertragung übermittelt worden sind" (Übermittlungskontrolle). Dies bedingt, daß alle mit Wählmodems oder ISDN-Karten versehenen Arbeitsplatzrechner, auf denen personenbezogene Daten verarbeitet werden, mit einer geeigneten Protokollierungssoftware ausgestattet sein müssen.

- Die Regelungen der §§ 13 bis 15, 17 und 18 BrDSG für die Zulässigkeit von Datenübermittlungen sind zu beachten.

Außer in genehmigten ADV-Verfahren, bei denen eine Datenübermittlung per MODEM ausdrücklich vorgesehen ist, dürfen keine weiteren Wählmodems (mit oder ohne FAX-Option) bzw. ISDN-Karten in Arbeitsplatzrechnern installiert werden, bevor die datenschutzrechtlichen Fragen grundsätzlich geklärt sind. Eine positive Stellungnahme im Einzelfall behalte ich mir vor.

Sprachserver

Seitens des Fernmeldetechnischen Amtes (FTA), jetzt Bremer Kommunikationstechnik (BreKom), war der Piloteinsatz eines **zentralen Sprachservers** geplant, um der raschen und unkontrollierten Ausbreitung von dezentralen Anrufbeantwortern entgegenzuwirken

und diese Funktion sowie Ansagedienste der bremischen Verwaltung konzentriert an einer Stelle zur Verfügung zu stellen. Drei Dienststellen sind für den Piloteinsatz vorgesehen, nämlich die Senatskommission für das Personalwesen, das FTA (jetzt BreKom) selbst und das Hauptgesundheitsamt.

Gegenüber dem FTA habe ich meine Bereitschaft erklärt, dieses Projekt zu begleiten, das vom Eigenbetrieb BreKom weiterbetrieben wird.

Der Wortlaut der §§ 5 Nr. 5 und 10 der geltenden "Dienstvereinbarung über den Betrieb und die Nutzung von Telekommunikationsanlagen (Fernsprechanlagen)" vom 15. Mai 1991, wonach die zentrale digitale Speicherung des gesprochenen Wortes unzulässig ist bzw. Inhaltsdaten weder zentral erfaßt noch gespeichert werden, läßt vermuten, daß die Nutzung der Anrufbeantworterfunktion eines zentralen Sprachservers hiermit nicht zu vereinbaren ist. Diese Bestimmungen werden von den Vertragsparteien aber nicht restriktiv ausgelegt, so daß die für die Speicherung vorgesehenen Ansagetexte und die von den Anrufenden auf dem Sprachspeicher hinterlassenen Nachrichten von diesen Regelungen nicht erfaßt werden.

Unabhängig davon sind u.a. folgende Mindestanforderungen zum Datenschutz zu beachten:

Bei der Nutzung des Sprachservers als Anrufbeantworter muß nach dem allgemeinen akustischen Hinweis immer ein individueller Ansagetext kommen, in dem die Dienststelle sowie die Durchwahlnummer des Inhabers bzw. der Inhaberin der Sprachbox genannt werden, damit die anrufende Person vor dem Aufsprechen einer Nachricht feststellen kann, ob sie sich verwählt hat.

Bei der Installation von Sprachservern muß der Betreiber zudem darauf achten, daß

- alle vorinstallierten Sicherheitscodes verändert werden,
- prinzipiell ein Abhören von Meldungen nur nach Eingabe eines individuellen Paßwortes (PIN) in ausreichender Länge (nicht unter vier Stellen) ermöglicht wird,
- die Besitzer und Besitzerinnen von Sprachboxen über die Mißbrauchsrisiken informiert und zu einem risikominimierenden Verhalten angehalten werden,
- die Anlage in kurzen Abständen auf Unregelmäßigkeiten untersucht wird. Hierzu gehört auch das Registrieren von unberechtigten Eindringversuchen.

Mit der BreKom wurde vereinbart, daß ein zentrales Datenschutzkonzept erstellt und mit mir abgestimmt wird, in dem die allgemeinen Regelungen aufgenommen werden. Des weiteren ist es erforderlich, für die jeweiligen Bereiche - insbesondere für die sensiblen Bereiche wie z.B. das Hauptgesundheitsamt - spezifische Datenschutzkonzepte zu erstellen, die auch mit mir abzustimmen sind, bevor die Anrufbeantworterfunktion in diesen Bereichen eingeführt wird. Weitere Gespräche mit der BreKom und den betroffenen Bereichen sind vorgesehen.

2.3.2.3. Entwicklungen im nicht-öffentlichen Bereich

Auch außerhalb der öffentlichen Verwaltung gibt es eine Reihe von Entwicklungen bei den Informations- und Kommunikationstechniken, die einer intensiveren Beobachtung bedürfen. Hierzu gehört insbesondere die Ausbreitung von Mail- und Sprachboxen.

Mailboxen

Im Bundesland Bremen ist die Anzahl der Betreiber nichtkommerzieller Mailboxen in den letzten Jahren deutlich gestiegen. Über PC und Modem kann grundsätzlich jede/r Zugang zu den Mailboxen finden. Im allgemeinen ist jedoch eine Anmeldung als "User" erforder-

lich, um eine Berechtigung zu erhalten, Nachrichten über die verschiedenen Mailbox-Netze zu verbreiten.

Beim Betrieb eines Mailboxsystems fallen verschiedenartige Daten an. Neben den Stammdaten der Benutzer und Benutzerinnen fallen auch vielfältige Verbindungsdaten an. In manchen Netzen gibt es zudem für die Betreiber bzw. Betreiberinnen der Mailboxen die Möglichkeit, selbst die Nachrichten zu lesen, die nicht für sie bestimmt sind, sondern von den Benutzern und Benutzerinnen geschrieben bzw. an diese gerichtet sind.

Ich beabsichtige, möglichst bald in Zusammenarbeit mit den anderen Aufsichtsbehörden die datenschutzrechtlichen Vorgaben für den Betrieb von Mailboxsystemen zu definieren, um verbreitete Rechtsunsicherheiten auszuräumen.

Sprachboxen

Im Grunde funktionieren die Sprachboxen nach dem gleichen Prinzip wie der oben erwähnte Sprachserver. Schon bisher gab es solche Boxen, die ihren Standort zumeist in Übersee hatten. Ein Sprachserver, mit dem mehrere Sprachboxen realisiert werden, wurde jetzt auch in Bremen in Betrieb genommen.

Zu unterscheiden ist zwischen allgemein zugänglichen - öffentlichen - Boxen und privaten, die die Eingabe eines Zugangscodes voraussetzen.

Im Prinzip läßt sich ein solches System mit einem Kleinanzeigenblatt vergleichen: Eine Person gibt eine Kleinanzeige auf, in der auch ihre Telefonnummer genannt ist, Interessenten bzw. Interessentinnen können sich direkt melden oder es wird eine Chiffreanzeige aufgegeben; in diesem Fall schicken die Interessenten und Interessentinnen die Antworten unter Angabe der Chiffrenummer an den Verlag, der sie dem Inserenten bzw. der Inserentin zusendet.

Bei privaten Sprachboxen kann sich jemand eine private Box einrichten lassen, mit einer anzuwählenden Telefonnummer und einem Zugangscode. Wer die - z.B. in einer gedruckten Kleinanzeige eines Anzeigenblattes - angegebene Rufnummer wählt, hört die gesprochene Anzeige und hat die Möglichkeit, eine Antwort in der dazugehörigen Sprachbox zu hinterlassen. Die inserierende Person kann unter Angabe ihres Zugangscodes (entweder über ein Telefon mit Tonwahlverfahren oder über einen Tongeber, wie er auch für Anrufbeantworter eingesetzt wird) die eingegangenen Nachrichten abhören.

Bei den öffentlichen Boxen dieses Sprachservers läuft der Vorgang etwas anders ab. Hier gibt es die gesprochenen Anzeigen nur in der allgemein zugänglichen Box. Den Inserenten und Inserentinnen bleibt es dabei freigestellt, für Antworten ihre eigene Telefonnummer anzugeben oder ein Kennwort zu nennen. In diesem Fall können Antwortende ihren Text unter Nennung dieses Kennwortes in eine Box sprechen, die wiederum von allen abgehört werden kann.

Bei den öffentlich zugänglichen Boxen gibt es aber einen wesentlichen Unterschied zu einem Kleinanzeigenblatt. Während dieses nach dem Presserecht verpflichtet ist, sich Name und Anschrift der Inserenten und Inserentinnen angeben zu lassen, ist dort die anonyme Aufgabe von Anzeigen möglich. Dies hat zur Folge, daß nicht kontrolliert werden kann, ob Angaben enthalten sind, die nicht von der aufsprechenden Person stammen.

Solche Fälle der Belästigung aufgrund der von anonymen Dritten aufgegebenen Annoncen sind - zumindest bei den Sprachboxen mit Standort in Übersee - schon vorgekommen.

Die Entwicklung in Bremen werde ich weiter verfolgen. Allerdings beschränkt das BDSG im nichtöffentlichen Bereich seine Anwendbarkeit auf Dateien, ist also in diesen Fällen nur anwendbar, wenn die Speicherung in einer Form - insbesondere digitalisiert - erfolgt, die eine automatisierte Auswertung der in der Sprachbox enthaltenen Texte ermöglicht.

Unabhängig davon ist das Vorliegen der Voraussetzungen des § 15 Teledienstunternehmen-Datenschutzverordnung (UDSV) zu prüfen.

2.3.3. Erste Erfahrungen mit tragbaren PC´s (Laptops, Notebooks, etc.)

Sowohl in der Finanzverwaltung als auch im Gesundheitsressort wurde die Beschaffung von tragbaren PC´s ausgeschrieben. In beiden Fällen wurde ich an der Ausschreibung beteiligt. Die in meinem 15. Jahresbericht genannten Forderungen (vgl. dort 2.2.1.2 Laptops und Notebooks) wurden weitgehend berücksichtigt.

2.3.3.1. Finanzressort

Im Bereich des Senators für Finanzen wurde mir zugesichert, daß ich auch bei der Auswahl der zu beschaffenden Geräte beteiligt werde.

Im übrigen wird bei den zu erstellenden Datenschutzkonzepten festzulegen sein, wie den Erfordernissen des § 150 Abs. 6 Abgabenordnung entsprochen werden kann. Denn die genannte gesetzliche Vorschrift verlangt bei der Datenübermittlung auf maschinell verwertbaren Datenträgern oder bei Datenfernübertragung die Festlegung der Datenübermittlungsfälle in einer Rechtsverordnung und die freie Entscheidung des übermittelnden Steuerpflichtigen für diese Form der Datenübermittlung. Durch die Verwendung der tragbaren PC´s im Rahmen der Betriebsprüfung, Steuerfahndung oder Zollfahndung darf diese Vorschrift nicht unterlaufen werden. Deshalb sind entsprechende Sicherungen einzubauen.

2.3.3.2. Sozialbereich

Der Senator für Gesundheit, Jugend und Soziales hält den Einsatz von tragbaren PC´s auf Dienstreisen, bei Deputationssitzungen, Dienstgesprächen etc. für erforderlich. Es sollen mit ihrer Hilfe Protokollnotizen bzw. Protokolle, Pressemitteilungen, Redebeiträge, Briefe, Notizen usw. erstellt werden.

Grundsätzlich dürfen auf diesen mobilen Geräten keine durch § 65 Kinder- und Jugendhilfegesetz (KJHG), § 35 SGB I oder § 203 StGB geschützten Klientendaten verarbeitet werden.

Die folgenden technischen und organisatorischen Vorkehrungen (nach § 6 BrDSG bzw. § 9 BDSG) sind vor diesem Hintergrund zu sehen:

- Die tragbaren PC´s werden unter Verschluß im Abschnitt 400-102 (ADV-Angelegenheiten) aufbewahrt.

- Die Entleihung eines Gerätes wird in einer Entleihungsliste mit Datum, Organisationskennziffer, geplanter Rückgabe und Rückgabedatum, Datum der Geräteprüfung und Unterschrift des Ausleihers/ der Ausleiherin dokumentiert.

- Bei Rückgabe wird das Gerät durch die Mitarbeiter/-innen des Abschnitts 102 auf einwandfreien Zustand hin überprüft und alle Daten (außer Betriebssystem und Anwendungsprogramme), die sich nach Rückgabe auf der Festplatte befinden, werden gelöscht.

- Auf allen tragbaren PC´s soll die Datenschutzsoftware "Safeguard" installiert werden.

- Parallele und serielle Schnittstellen werden gesperrt.

- Bei Ausleihung wird eine Dienstanweisung (deren Empfang zu dokumentieren ist) ausgehändigt. Sie regelt im wesentlichen die vorübergehende Nutzung (zeitliche Begrenzung, Verpflichtung der zugriffssicheren Aufbewahrung für die Zeit der Ent-

leihung, Kopierverbot, zeitliche Beschränkung der Speicherung von Dateien auf der Festplatte), die zu installierende Standardsoftware (verbindliche Festlegung) sowie die Definition der Datenart, die verarbeitet werden darf (personenbezogene Daten nur im Zusammenhang mit Sitzungsprotokollen und Gesprächsnotizen, d. h. Name, Vorname, Dienst- oder Funktionsbezeichnung, Telefonnummer).

2.3.4. Pilotprojekt Netze

Die Pilotprojekte für eine "abteilungsbezogene Datenhaltung auf PC-Netzen" (vgl. 15. Jahresbericht, Ziff. 2.2.1.1) sind inzwischen abgeschlossen. Die Anwendungen im Aus- und Fortbildungszentrum (AFZ) der SKP sowie beim Amtsgericht Bremen sind eingeführt worden.

Die von der SKP verteilte Zusammenfassung der Ergebnisse wurde nicht mit mir abgestimmt. so daß das Kapitel über den Datenschutz zumindest mißverständliche Passagen enthält.

Die SKP plant, für den Einsatz von Netzen eine Reihe von Handlungshilfen zu verschiedenen Themen herauszugeben und hat mir zugesagt, die datenschutzrelevanten Teile dieser Handlungshilfen mit mir abzustimmen.

Die Ergebnisse der Pilotprojekte ermöglichen zwar einige grundsätzliche Aussagen auch zum Datenschutz, z.B. ist in sensibleren Bereichen der Einsatz von WINDOWS NT wegen des fehlenden Vier-Augen-Prinzips für die Systemverwaltung als Netzbetriebssystem nicht ausreichend.

Es ist erforderlich, bei der Einführung von Netzen jeweils im Einzelfall die Umsetzung der datenschutzrechtlichen Anforderungen zu prüfen. Es zeigt sich schon jetzt, daß eine intensive Schulung der für die Netzverwaltung zuständigen Personen unverzichtbar ist und daß die Netzverwaltung keine Aufgabe ist, die die Systemkoordinatoren und Systemkoordinatorinnen nebenbei ausüben können.

Es ist damit zu rechnen, daß die bremischen Behörden nach Abschluß der Pilotprojekte vermehrt Anträge zur Beschaffung von Netzen stellen werden. Der Beratungsbedarf wird daher auch - aber nicht nur im Bereich des Datenschutzes - stark steigen. Es wird Aufgabe der SKP sein, sowohl das Tul-Regelwerk so zu fassen als auch ausreichende Kapazität zur Verfügung zu stellen, um die Einhaltung der in den Pilotprojekten entwickelten technischen und organisatorischen Vorgaben zu gewährleisten. Mit meinen beschränkten Ressourcen kann ich nur ergänzende Hilfestellung geben.

2.3.5. Protokollierung bei SAFEGuard - Stand des Verfahrens

Entgegen ursprünglichen Aussagen der Herstellerfirma von SAFEGuard ist die in meinem letzten Jahresbericht (vgl. Ziff. 2.2.1.3.) erwähnte Windows-Version von SAFEGuard noch nicht verfügbar. Auch kann kein Markteinführungstermin verbindlich genannt werden. Daher muß ich verlangen, daß bei Neuanschaffungen in Bereichen, in denen die Protokollierung der Benutzer- und Benutzerinnen-Aktivitäten erforderlich ist, die aktuelle DOS-Version dieser Software eingesetzt wird. Bei vorhandenen Arbeitsplatzrechnern muß enstprechend nachgerüstet werden.

Ich habe zwischenzeitlich generelle Standards zur Protokollierung entwickelt und der Senatskommission für das Personalwesen sowie dem Gesamtpersonalrat zugeleitet. Zu diesen Standards gehören folgende Grundsätze:

1. Protokollierungen sollten im jeweiligen Anwendungsverfahren selbst erfolgen, nur so sind ausreichende Differenzierungen nach Daten, Feldern, Masken, Auswertungen, Ausdrucken o.ä. vorzunehmen.

Wo dies nicht möglich ist, ist auf die Protokollierung durch eine entsprechende Sicherheitssoftware zurückzugreifen.

2. Grundsätzlich ist jeder schreibende Zugriff aufzuzeichnen, evtl. mit Inhalt des neu eingegebenen oder geänderten bzw. gelöschten Datzensatzes; bei sensitiven Daten sollten jedoch nur Feldbezeichnungen protokolliert werden. Darüber hinaus sollten lesende Zugrife sensibler Anwendungen, alle lesenden Zugriffe durch Dritte (auch durch den Systemverwalter) sowie per Dialog veranlaßte Übermittlungen aufgezeichnet werden.

3. Für jede aufzuzeichnende Aktivität sollten mindestens Terminal-Nr. (sofern vorhanden: SAFEGuard bietet allerdings die Möglichkeit, für jeden PC eine individuelle Rechner-Nr. zu vergeben; diese sollte genutzt werden), Datum und bei sehr sensiblen Anwendungen auch Uhrzeit, Benutzer bzw. Benutzerin, Anwendungsprogramm und evtl. Grund sowie Ordnungsnr. des Datensatzes festgehalten werden. Protokolle sind untauglich, die lediglich das Starten und Beenden des Betriebssystems oder eines Datenbanksystems enthalten. Bei Massenprotokollierungen kann in weniger sensiblen Bereichen eine Stichproben-Aufzeichnung bzw. -Auswertung in Frage kommen.

4. Da die Protokolldateien sehr umfangreich sind, ist eine automatisierte Auswertung zur zeitnahen und effizienten Kontrolle erforderlich.

Zusätzlich sind die Zweckbindung der Protokolldateien und die Mitbestimmungsrechte der Personalräte zu beachten sowie Löschungsfristen festzulegen.

2.3.6. Kontrollergebnisse

Bei mehreren Datenschutzkontrollen im PC-Bereich habe ich Sicherheitsmängel festgestellt, die vermutlich auch bei anderen Behörden anzutreffen sein dürften.

Zum einem bestätigt sich immer wieder, daß das Konzept der dezentralen Systemkoordinierung ohne die Ausbildung und laufende Weiterbildung der Systemkoordinatoren und Systemkoordinatorinnen nicht funktionieren kann.

Es ist zu unterscheiden zwischen PC´s mit SAFEGuard und solchen ohne dieses Zugriffsschutzprogramm, bei denen die hardwareseitigen Mechanismen genutzt werden.

2.3.6.1. PC´s ohne SAFEGuard

Bei bestimmten PC´s (z.B. der Marke ICL) bietet die Hardware die Möglichkeit, ein System- und ein Benutzer- bzw. Benutzerinnen-Paßwort einzurichten sowie das "Booten" (also das Starten des PC´s und Laden des Betriebssystems) vom Diskettenlaufwerk zu unterbinden. Diese Vorkehrungen sollten genutzt werden. Dabei darf das Systempaßwort nicht für alle PC´s einer Behörde gleich sein. Sonst erstreckt sich, wenn es durch Ausspähen oder Ausprobieren bekannt wird, die unbefugte Zugangsmöglichkeit ebenfalls auf alle diese Arbeitsplatzrechner dieser Behörde, dann ist - zumindest bei einigen Modellen - auch ein Zugriff auf die dort gespeicherten Daten möglich.

Wird die Oberfläche Windows eingesetzt, sollten die automatische Aktivierung des Bildschirmschoners sowie ein Kennwortschutz eingerichtet sein.

2.3.6.2. PC´s mit SAFEGuard

Alle PC´s, die mit SAFEGuard ausgestattet geliefert werden, sind mit einer Grundkonfiguration versehen worden. Es ist zwingend erforderlich, diese Grundkonfiguration zu ändern, damit die Sicherheitsmechanismen von SAFEGuard greifen können. Zu den notwendigen Änderungen gehören:

- Das Systempaßwort muß geändert werden, auch hier dürfen nicht alle PC´s einer Behörde mit dem gleichem Systempaßwort versehen werden.

- Die Option, daß die Paßwörter nach einer bestimmten Zeit ungültig werden, sollte eingerichtet werden. Ein Zeitraum von 90 Tagen ist hierbei im allgemeinen sinnvoll. Danach können sich die Benutzer und Benutzerinnen zwar noch mit dem alten Paßwort einloggen, aber nur, um ein neues Paßwort einzugeben.

- Für alle zugriffsberechtigten Benutzer und Benutzerinnen sind eigene Kennungen mit eigenen Anfangspaßwörtern, die beim ersten Login geändert werden müssen, zu vergeben.

- Nach der ersten Einrichtung der Benutzer- und Benutzerinnen-Kennungen sind die Standardkennungen DEMO und BETON zu löschen, da auch diese mit Standardpaßwörtern versehen sind und damit keinen Zugriffsschutz bieten.

- Beim "offenen System" ist der Menüpunkt "Dienstprogramme" dahingehend zu ändern, daß die "Menü-/Benutzerorganisation" für die Benutzer und Benutzerinnen nicht verfügbar ist.

Werden diese Maßnahmen nicht getroffen, können Unbefugte, die Zugang zum PC haben, sich ohne Schwierigkeiten unter Verwendung von Standardpaßwörtern Zugriff auf die gespeicherten Daten verschaffen.

Bei zukünftigen Datenschutzkontrollen im PC-Bereich werde ich verstärkt auch auf diese Anforderungen achten.

2.3.7. PC-Anträge

Ein weiterer Arbeitsschwerpunkt ist nach wie vor die datenschutzrechtliche Beurteilung von ADV-Anträgen zur PC-Beschaffung. So sind in meiner Dienststelle weit über hundert Beschaffungsanträge mit einer Gesamtzahl von weit über 500 PC´s durchgelaufen. Dabei waren ca. zehn Netze, in denen zusammen deutlich über 150 PC´s angeschlossen werden sollen, geplant (das unter Punkt 2.3.3.1 erwähnte Netz im Finanzressort mit ca. 250 tragbaren PC´s nicht mitgerechnet).

Nach einer (sicher nicht ganz vollständigen) Aufstellung der SKP als Antwort des Senats vom 21. Dezember 1993 (Drucksache 13/797) auf eine Kleine Anfrage der Fraktion DIE GRÜNEN existieren in der bremischen Verwaltung 3377 Arbeitsplatzrechner, von denen 112 vernetzt sind (die Server nicht mitgerechnet) und 904 einen Großrechneranschluß haben. Weiter sind in der Aufstellung 534 Terminals mit Großrechneranschluß und 76 Terminals mit Anschluß an UNIX-Servern enthalten.

2.3.7.1. PC-Antrags-Formular

Die SKP beabsichtigt, unabhängig von der Überarbeitung des Tul-Regelwerkes (s.o.) die Anträge für den Einsatz von Hard- und Software nach der Beschaffungsliste zu vereinfachen. Ich schlug daher vor, dem neuen Antragsformular eine Anlage "Datenschutzkonzept" beizufügen, die zumindest folgende Informationen enthalten sollte:

- Art der zu verarbeitenden Daten (bei Datenbankanwendungen in der Form, wie sie im Rahmen des Pilotprojektes Netze (s.o.) beim Beratungszentrum für die Anwendung im AFZ entwickelt wurde),

- Rechtsgrundlage für die zu verarbeitenden Daten,

- Anwendungen, mit denen die Daten verarbeitet werden sollen,

- Beschreibung der Datenschutz- und -sicherungsmaßnahmen (bei SAFEGuard-Einsatz auch eine Kurzbeschreibung der Konfiguration),

- Protokollierungsmaßnahmen,

- wer auf die Protokolle zugreifen darf

sowie bei Netzanwendungen zusätzlich

- auf welche Daten mit welchen Anwendungen gemeinsam zugegriffen werden soll

- Begründung, warum ein gemeinsamer Datenzugriff erforderlich ist und

- welche Zugriffsrechte vorgesehen sind.

Ohne diese Angaben ist keine Abstimmung zwischen der beschaffenden Stelle und mir möglich.

Die SKP hat mir zugesichert, daß ich an der Erstellung dieses Formulars beteiligt werde. Dabei gehe ich davon aus, daß diese Abstimmung vor dem Zeitpunkt erfolgt, zu dem der Entwurf den senatorischen Behörden zur abschließenden Stellungnahme vorgelegt oder zur Senatsvorlage wird.

2.3.7.2. Formular für Stellungnahmen

Unabhängig von diesem Formular wurde in meiner Dienststelle ein Formblatt für die Erteilung von Stellungnahmen entwickelt, das zu einer noch rationelleren und effizienteren Bearbeitung der PC-Beschaffungsanträge in meiner Dienststelle führen wird.

2.4. Internationaler Datenschutz

2.4.1. Datenschutzrichtlinie der Europäischen Union

Auch unter der belgischen Präsidentschaft im zweiten Halbjahr 1993 konnten die Beratungen über die Datenschutz-Richtlinie der Europäischen Union (EU) nicht abgeschlossen werden. Die Diskussionen über den von der Kommission am 15. Oktober 1992 vorgelegten Geänderten Vorschlag für eine Direktive "zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" (Amtsblatt der EG Nr. C 311, S. 3o ff.) kreisen nach wie vor um die gleichen Themen, die im letzten Jahresbericht eingehend dargestellt wurden (vgl. 15. Jahresbericht, Ziff. 2.3.2). Umstritten oder jedenfalls nicht in einen konsentierten Text gefaßt sind immer noch u.a. die Fragen des Anwendungsbereichs, des anwendbaren Rechts bei grenzüberschreitenden Sachverhalten, der Möglichkeit eines einzelstaatlich höheren Schutzniveaus, des Umfangs der Meldepflicht für Dateien und der ausdrücklichen Absicherung des deutschen Kontrollmodells mit seiner Besonderheit der Institution eines innerbetrieblichen Beauftragten für den Datenschutz.

Die verbreitet festzustellende Europamüdigkeit in den Mitgliedstaaten, verbunden mit einer verschärften Prüfung aller Regelungsvorhaben der Kommission unter dem Gesichtspunkt der "Subsidiarität", wirkt sich auch bei diesem Richtlinienprojekt - zusätzlich zu der ohnehin vorhandenen Komplexität der EG-weit zu harmonisierenden Materie Datenschutz - verzögernd aus. Ich habe mich auch in diesem Berichtsjahr als einer der Vertreter der deutschen Datenschutzbeauftragten in mehreren Sitzungen intensiv an der von den EG- Gremien erwarteten Meinungsbildung der Konferenz der Datenschutz-Kontrollinstitutionen in der Europäischen Union beteiligt. Der im ersten Halbjahr 1994 amtierende griechische Vorsitzende der die Richtlinie beratenden Arbeitsgruppe des EU-Ministerrats drängt nachhaltig auf den Abschluß der seit dreieinhalb Jahren laufenden Diskussionen. Falls dies nicht gelingt, hat die im zweiten Halbjahr 1994 anschließende deutsche Präsidentschaft die Chance, den Gemeinsamen Standpunkt des Ministerrats zustande zu brin-

gen. Die Zeit drängt, und die Ziele der Richtlinie, die Freiheit des grenzüberschreitenden Datenverkehrs im europäischen Binnenmarkt zu kombinieren mit einem gemeinschaftsweiten Schutz des Persönlichkeitsrechts auf hohem Niveau, bleiben unverändert aktuell.

2.4.2. "Checkliste" für grenzüberschreitende Datenübermittlungen

Solange die einzelstaatlichen Datenschutzrechte nicht auf der Ebene der Europäischen Union harmonisiert sind, bleibt es bei national unterschiedlichen Rechtslagen, was die Beurteilung grenzüberschreitender Datentransfers angeht. Für den nicht-öffentlichen Bereich (Privatwirtschaft) enthält das Bundesdatenschutzgesetz (BDSG) dazu keine spezielle Vorschrift; vielmehr sind die allgemeinen Übermittlungsvoraussetzungen zu prüfen. Dazu gehören insbesondere die Fragen, ob im Zielland eine dem deutschen Standard entsprechende Datenschutzgesetzgebung besteht und inwieweit beim ausländischen Datenempfänger tatsächlich ausreichende Datenschutz- und Datensicherungsvorkehrungen getroffen sind.

Ein Arbeitskreis des "Düsseldorfer Kreises", dem Abstimmungsgremium der obersten Aufsichtsbehörden, hat dazu eine Checkliste erarbeitet und einer Reihe von Wirtschaftsverbänden zur Information und Stellungnahme zugeleitet. Die Checkliste enthält Hinweise auf notwendige vertragliche Vereinbarungen zwischen dem inländischen Datenabsender und dem Empfänger im Ausland; sie schließen das Kontrollrecht vor Ort durch die deutsche übermittelnde Stelle ein. Den Aufsichtsbehörden kann diese Liste als gemeinsame Orientierung für die Prüfung der Zulässigkeit internationaler Datentransfers nach dem BDSG dienen. Dies gilt jedenfalls bis zur Harmonisierung der Übermittlungsvoraussetzungen in den Mitgliedsstaaten der Europäischen Union durch die geplante Richtlinie (vgl. o. Ziff. 2.4.1.). Nach dem Inkrafttreten sind Anwendungsbereich und Kriterienkatalog der "Checkliste" zu überprüfen und zu aktualisieren.

2.4.3. Internationale polizeiliche Zusammenarbeit

2.4.3.1. Wasserschutzpolizei

Im Zuge der europäischen Integration wird auch der Datenaustausch verschiedener Polizeibehörden mit entsprechenden ausländischen Dienststellen intensiver. So kommuniziert z. B. die Wasserschutzpolizei, die im Lande Bremen die grenzpolizeilichen Aufgaben wahrnimmt, mit den Hafenpolizeien benachbarter Häfen, wie z. B. Amsterdam und Rotterdam. Der Datenaustausch bezieht sich u. a. auf Mannschafts- und Passagierlisten mit personenbezogenen Daten, die den Behörden des vom Schiff angesteuerten nächsten Hafens übermittelt werden. Das Verfahren habe ich datenschutzrechtlich begleitet.

2.4.3.2. EUROPOL

Weiter wird zur Umsetzung der Maastrichter Verträge von den Mitgliedstaaten angestrebt, zur Institutionalisierung der polizeilichen Arbeit auf europäischer Ebene eine Zentralstelle (EUROPOL) zu schaffen. Als erster Schritt soll im Bereich der Drogenkriminalität die Möglichkeit des Informationsaustausches geschaffen werden. Dazu ist eine EUROPOL-Drogenstelle (EDU) in Den Haag eingerichtet worden; wohin zunächst seitens der Mitgliedstaaten Verbindungsbeamten entsendet wurden. Die Verbindungsbeamten haben Zugriff auf ihre jeweiligen nationalen polizeilichen Informationssysteme. Der Kooperationsstab in der EDU-Zentralstelle (European Drug Unit) soll nicht berechtigt sein, eigene Dateien mit personenbezogenen Daten zu führen. Ob hingegen die Verbindungsbeamten unmittelbar Daten austauschen oder aber nur Kontakte zu den einspeichernden Dienststellen herstellen sollen, ist streitig. Eine ausdrückliche Rechtsvorschrift für die Zusammenarbeit gibt es bisher noch nicht. Bis zur Schaffung einer solchen Regelung stützt sich die Zusammenarbeit in der EDU-Zentrale auf eine Vereinbarung der zuständigen Minister vom April 1993, die keine eigenständige Rechtsgrundlage für Übermittlungen darstellen kann. Ich trete dafür ein, die Rechtsgrundlagen für eine EUROPOL-Zentrale unter parlamentarischer Verantwortung zu schaffen, d. h. z. B. in Form einer völkerrechtlich verbindlichen und ratifizierungsbedürftigen Konvention mit Regelungen über

den Datenschutz. Da in großem Maße auch Daten aus den Bundesländern in den EUROPOL-Bereich hineinfließen, müssen deren Interessen in diesem Verfahren ausreichend Berücksichtigung finden.

2.4.3.3. Schengener Informationssystem (SIS)

Im Zuge des Abbaus der Binnengrenzen zwischen den Vertragsstaaten und der Koordinierung der Kontrollen an den Außengrenzen ist das Schengener Übereinkommen verabschiedet und auch für die Bundesrepublik in Kraft gesetzt worden. Das Schengener Informationssystem (SIS) soll Ausschreibungen zur Fahndung nach Personen und Sachen dienen und für polizeiliche Überprüfungen an den Außengrenzen der Vertragsstaaten und im Landesinneren zur Verfügung stehen. Jede Vertragspartei bezeichnet eine eigene Kontrollinstanz, deren Aufgabe darin bestehen soll, nach Maßgabe des jeweiligen einzelstaatlichen Rechts den Datenbestand des nationalen Teils des Schengener Informationssystems (N.SIS) zu überwachen und zu prüfen, ob die Verarbeitung und Nutzung der im SIS gespeicherten Informationen die Datenschutzrechte der Betroffenen nicht verletzt. Daneben gibt es eine gemeinsame Kontrollinstanz, die die Einhaltung der Datenschutzbestimmungen im zentralen Schengener Informationssystem (C.SIS) überwachen soll. Ursprünglich war beabsichtigt, das Schengener Informationssystem Anfang 1994 in Betrieb zu nehmen. Aufgrund technischer Probleme verzögert sich dieser Termin um einige Zeit. Ich habe mich bei der Polizei in Bremen über die getroffenen Vorbereitungen informiert.

3. Senatskanzlei

3.1. Kein Verdienstorden ohne den Verfassungsschutz

Die Senatskanzlei hat mir auf Anfrage mitgeteilt, daß sie sich wegen der Überprüfung einer für die Ordensverleihung vorgeschlagenen Person an den Senator für Inneres wendet mit der ganz allgemein gehaltenen Bitte um Mitteilung, ob über die betreffende Person "Nachteiliges bekanntgeworden ist". Nach meinen Recherchen fragt die Innenbehörde daraufhin beim Staatsarchiv Bremen an, ob Informationen über die betroffene Person vorliegen. Gleichzeitig leitet sie das Auskunftsersuchen an die Staatsschutzabteilung der Polizei sowie an das Landesamt für Verfassungsschutz (LfV) weiter. Das LfV läßt sich zusätzlich zu den eigenen Erkenntnissen eine unbeschränkte Auskunft aus dem Bundeszentralregister geben und richtet bei den Geburtsjahrgängen vor 1926 eine Anfrage an das Document Center in Berlin.

Dieser Vorgang stellt einen tiefen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Personen dar, denen eigentlich ja eine Ehrung zugedacht ist, ohne daß sie häufig davon wissen. Da eine Einwilligung nicht vorliegt, bedürfte es zur Legitimation dieser Datenerhebung und -weitergabe wegen der Eingriffstiefe einer normenklaren Rechtsvorschrift.

Das Gesetz über Titel, Orden und Ehrenzeichen aus dem Jahre 1957 enthält jedoch keine Datenverarbeitungsregelungen.

Zwar enthalten die Ausführungsbestimmungen zum "Statut des Verdienstordens der Bundesrepublik Deutschland" allgemeine Grundsätze für die Vergabe, etwa den Ausschluß der Auszeichnung bei früherer Bestrafung wegen eines Verbrechens. Außerdem ist festgelegt, unter welchen Voraussetzungen eine Auszeichnung trotz einer Verurteilung wegen eines Vergehens möglich sein soll, daß Verurteilungen wegen einer Übertretung einer Ehrung grundsätzlich nicht entgegenstehen und daß Vorstrafen stets in der Vorschlagsbegründung zu erwähnen sind.

Daß zur Feststellung dieser Voraussetzungen in gewissem Umfang Ermittlungen erforderlich sind, ist unstreitig. Doch stellen bloße Ausführungsbestimmungen, die zudem die beteiligten Instanzen, den Umfang der bei diesen zu erhebenden Angaben und die Übermittlungswege nicht näher vorgeben, keine ausreichende verfassungsgemäße Rechtsgrundlage dar, die die in Bremen und anderen Bundesländern geübte Verfahrensweise rechtfer-

tigen könnte. Das Bundeszentralregistergesetz (BZRG) und das Bundesarchivgesetz (BArchG) regeln allenfalls Teilfacetten dieser komplexen Recherchen im Vorleben der Betroffenen.

Wegen der fehlenden Rechtsgrundlagen habe ich die Senatskanzlei gebeten, auf Bundesebene auf die Schaffung präziser und abschließender Datenverarbeitungsregelungen im Gesetz über Titel, Orden und Ehrenzeichen hinzuwirken. Unabhängig davon ist die Senatskanzlei bereits jetzt gehalten, ihr Informationsersuchen an den Innensenator präziser, d. h. konkret auf die gesetzlichen Voraussetzungen bezogen, zu formulieren.

4. Personalwesen

4.1. Zwei Fälle: Verkürzung des Akteneinsichtsrechts

Die Behörde des Senators für Bildung und Wissenschaft beachtete in zwei Beschwerdefällen nicht, daß neben dem Recht auf Einsicht in die Personalakten das Bremische Datenschutzgesetz ein allgemeines Akteneinsichtsrecht gewährt, das nur unter den gesetzlich ausdrücklich vorgesehenen Voraussetzungen beschränkt oder verweigert werden kann (§ 19 BrDSG). So hatte ein ehemaliger Lehrbeauftragter der Universität Bremen Einsicht in eine bei der senatorischen Dienststelle geführte "Sachakte" beantragt, die Korrespondenz im Zusammenhang mit seiner Ernennung zum Lehrbeauftragten und mit der Beendigung dieser Tätigkeit, die bereits ca. 10 Jahre zurückliegt, enthielt.

Die Behörde hatte entschieden, die Überlassung einzelner Schriftstücke sei für den vom Betroffenen dargelegten Grund seines Einsichtswunsches ausreichend. Eine weitere, insbesondere rechtliche Begründung dieser Einschränkung ist nicht dargelegt worden.

Aufgrund der Eingabe des Betroffenen habe ich den Vorgang überprüft und bin zu dem Ergebnis gekommen, daß gesetzliche Hinderungsgründe nicht bestehen und dem Bürger das vollständige Akteneinsichtsrecht zusteht. Außerdem habe ich festgestellt, daß die Sachakte Unterlagen enthielt, die unmittelbar das Dienstverhältnis betreffen und demzufolge nur Bestandteil der Personalakte sein dürfen. Ich habe daher gefordert, diese Schriftstücke aus der Sachakte herauszunehmen und zur Personalakte des Betroffenen zu geben. Der Senator für Bildung und Wissenschaft hat mir dies zugesagt und wird im übrigen dem vollständigen Akteneinsichtsrecht des Bürgers entsprechen.

In einem anderen Fall wurde einem Lehrer die Einsicht in die Sachakte im Schulsekretariat verwehrt.

Meine Überprüfung hat ergeben, daß dort über jeden Lehrer ein Vorgang geführt wird, der allgemeine und personenbezogene Daten enthält, die den sog. "Geschäftsverkehr" betreffen, z. B. über Freistellung und Vertretung eines Lehrers bei Fortbildung, sowie Angaben über sonstige besondere Vorkommnisse, z. B. Elternbeschwerden. Auch in diesen Sachakten fanden sich Dokumente, die nur in der Personalakte aufzubewahren sind, z. B. Sonderurlaubsanträge.

Die Schulleitung hat zugesagt, die Sachakten der Lehrer durchzuarbeiten und die Personalaktendaten beinhaltenden Unterlagen in die bei der senatorischen Behörde geführten Personalakten zu geben. Außerdem wird auch sie künftig den Einsichts- und Auskunftsanspruch der Lehrer nach dem BrDSG beachten und nur dann versagen, wenn gesetzliche Hinderungsgründe (z. B. Rechte Dritter) vorliegen. Vom Bildungssenator erwarte ich, daß er dieses Thema generell aufgreift und die Schulleitungen entsprechend informiert.

4.2. Mitteilung von Schwangerschaften an den Betriebsarzt

Nach dem Mutterschutzgesetz (MuSchG, § 5 Abs. 1) sollen werdende Mütter dem Arbeitgeber ihre Schwangerschaft und den mutmaßlichen Zeitpunkt der Entbindung mitteilen, sobald ihnen ihr Zustand bekannt ist. Darüber hinaus sollen sie auf Verlangen des Arbeitgebers das Zeugnis eines Arztes oder einer Hebamme vorlegen. Aufgrund dieser

Mitteilung obliegt es dem Arbeitgeber, unverzüglich die Aufsichtsbehörde zu benachrichtigen. Sein Wissen darf er Dritten nicht unbefugt bekanntgeben.

In einem Bremer Krankenhaus leitete die Personalabteilung die Mitteilung der schwangeren Arbeitnehmerinnen darüber hinaus in jedem Fall an den Betriebsarzt weiter. Das Krankenhaus hält diese Datenweitergabe zur Erfüllung der Aufgaben des Betriebsarztes nach dem Arbeitssicherheitsgesetz (ASiG) für erforderlich. Das zuständige Gewerbeaufsichtsamt als Aufsichtsbehörde teilt diese Auffassung. Bei Fehlen einer ausdrücklichen Erlaubnis der Betroffenen könnte der Arbeitgeber im Rahmen der betrieblichen Erfordernisse von deren "stillschweigender Einwilligung" in die Information des Arbeitsmediziners ausgehen.

Ich habe sowohl dem Krankenhaus als auch dem zuständigen Gewerbeaufsichtsamt meine gegenteilige Auffassung dargelegt, wonach für die routinemäßige Unterrichtung weder eine ausreichende Rechtsgrundlage besteht noch eine "stillschweigende Einwilligung" der Schwangeren als Legitimation herangezogen werden kann.

Neben den Beratungs- und Mitwirkungsaufgaben nach § 3 ASiG obliegt es dem Betriebsarzt zwar auch, die Arbeitnehmerinnen zu untersuchen, arbeitsmedizinisch zu beurteilen und zu beraten sowie die Untersuchungsergebnisse zu erfassen und auszuwerten. Dieser abschließende Aufgabenkatalog enthält jedoch keine Befugnis oder gar Verpflichtung des Arbeitgebers, den Betriebsarzt regelmäßig und ohne Einzelfallprüfung über Schwangerschaften von Belegschaftsangehörigen zu unterrichten.

Um dieser Rechtslage Rechnung zu tragen und Kriterien dafür zu erarbeiten, unter welchen Voraussetzungen die Personalabteilung in Fällen der Schwangerschaft doch den Betriebsarzt einschalten darf bzw. soll, haben alle Beteiligten, d. h. die Krankenhausleitung, das Gewerbeaufsichtsamt, der Landesgewerbearzt, der Personalrat und die Frauenbeauftragte mit mir die Gesamtproblematik eingehend erörtert.

Übereinstimmung wurde darüber erzielt, daß der Arbeitgeber im Rahmen der im Mutterschutzgesetz definierten Pflichten zu entscheiden hat, ob und welche Maßnahmen er zum Schutze der werdenden Mutter zu treffen hat. Selbstverständlich kann er jederzeit ohne Namensnennung den Rat des Betriebsarztes einholen, insbesondere wenn, wie etwa in den ärztlichen Abteilungen der Krankenhäuser, die mutterschutzrechtlichen Konsequenzen komplexerer Natur sein können. Im Einzelfall kann zusätzlich zur Angabe des Arbeitsplatzes auch die Offenlegung der Identität der Schwangeren geboten oder unvermeidlich sein.

Um beiden Schutzgütern, dem Anspruch auf Mutterschutz einschließlich ggf. betriebsärztlicher Betreuung ebenso wie dem Persönlichkeitsrecht der Schwangeren Rechnung zu tragen, soll ein Informationsblatt für die weiblichen Beschäftigten erarbeitet werden, aus dem sich insbesondere die Modalitäten des Datenflusses zwischen dem Arbeitgeber und dem Betriebsarzt ergeben. Den betroffenen Mitarbeiterinnen soll bei der Meldung eine Einwilligungserklärung vorgelegt werden, damit sie für den Regelfall selbst entscheiden können, ob sie einer personenbezogenen Datenweitergabe an den Betriebsarzt zustimmen möchten.

4.3. Neues Personalaktenrecht

Das Gesetz zur Änderung dienstrechtlicher Vorschriften ist im Februar 1994 von der Bürgerschaft in erster Lesung behandelt worden (vgl. Drs. 13/723). Nach der Novellierung des Beamtenrechtsrahmengesetzes (BRRG) war auch der bremische Gesetzgeber gehalten, im Bremischen Beamtengesetz (BremBG) die datenschutzrechtlichen Anforderungen an die bundesrechtlichen Vorgaben anzupassen (vgl. dazu 15. JB, Ziff. 4.3).

In der Vorbereitung der Novellierung ging es mir vor allem darum,

- landesrechtliche Regelungsspielräume zugunsten einer Intensivierung des Arbeitnehmerdatenschutzes zu nutzen, und

- das vergleichweise hohe bestehende Datenschutzniveau in § 22 Bremisches Datenschutzgesetz (BrDSG) aufrecht zu erhalten.

Dies ist im wesentlichen gelungen.

Nunmehr wird in § 93 BremBG präzise geregelt, zu welchen Zwecken im Rahmen der Personalverwaltung und -wirtschaft personenbezogene Daten über Bewerber, Beamte und ehemalige Beamte verarbeitet werden dürfen. Insbesondere aus Gründen der Normenklarheit und der Transparenz ist der SKP als oberster Dienstbehörde auferlegt worden, Inhalt und Umfang dieser Datenerhebung, auch hinsichtlich medizinischer und psychologischer Untersuchungen, im Detail in Verwaltungsvorschriften zu regeln. Fragebogen, mit denen Angaben von Beschäftigten erhoben werden, bedürfen dann ihrer Genehmigung.

Des weiteren stellt die Neuregelung klar, daß auch die in Dateien gespeicherten und automatisiert verarbeiteten personenbezogenen Daten "Personalaktendaten" und damit auch vom Akteneinsichtsanspruch erfaßt sind.

Die sog. Sicherheitsakten nehmen das BRRG und dementsprechend auch das Landesgesetz aus dem Personalakteneinsichtsrecht aus. Der Senat verweist hierzu in der Begründung auf das allgemeine Auskunfts- und Einsichtsrecht nach § 19 BrDSG. Meinem Vorschlag, diesen Verweis in den Gesetzestext aufzunehmen, wurde allerdings nicht gefolgt. Bei der anstehenden Vorbereitung eines Sicherheitsüberprüfungsgesetzes für die Landesbediensteten werde ich erneut darauf drängen, daß der Inhalt von Sicherheitsakten grundsätzlich auch dem Bediensteten auf Antrag offengelegt wird.

Neu ist auch, daß bei erstmaliger Speicherung dem Beamten die Art der über ihn gespeicherten Daten mitzuteilen ist; bei wesentlichen Änderungen ist er zu benachrichtigen. Außerdem sind die Verarbeitungsformen automatisierter Personalverwaltungsverfahren zu dokumentieren; sie sind einschließlich des jeweiligen Verwendungszwecks sowie der regelmäßigen Empfänger und des Inhalts automatisierter Übermittlungen allgemein bekanntzugeben.

Das bisher in Bremen bestehende Verbot, dienst- und arbeitsrechtliche Beurteilungen sowie medizinische und psychologische Befunde des Beschäftigten automatisiert zu verarbeiten, ist insoweit beachtet worden, als im novellierten BremBG festgelegt ist, daß von ärztlichen oder psychologischen Untersuchungen und Tests im Rahmen der Personalverwaltung nur die Ergebnisse automatisiert verarbeitet werden dürfen und dies auch nur, soweit sie die Eignung betreffen und ihre Verarbeitung dem Schutz der Beamten dient.

Durch eine entsprechende Änderung des § 22 BrDSG ist sichergestellt, daß die neuen Regelungen für den Umgang mit Personaldaten nicht nur für die Beamten, sondern auch für die Angestellten und Arbeiter im bremischen öffentlichen Dienst in gleichem Maße gelten.

4.4. Datenschutz auch bei den Personalräten

Die Senatskommission für das Personalwesen hat mir den Entwurf einer Änderung des Bremischen Personalvertretungsgesetzes (BremPersVG) mit der Bitte um Stellungnahme vorgelegt. Den Personalräten obliegt eine Reihe gesetzlicher Aufgaben, die sie gegenüber den Dienstherren bzw. Arbeitgebern ohne Kenntnis zahlreicher persönlicher Informationen über die Beschäftigten nicht effizient wahrnehmen könnten. Die in sämtlichen Personalvertretungsgesetzen enthaltenen allgemeinen Informationsrechte und Auskunftsansprüche der Personalräte erfüllen jedoch nicht die verfassungsrechtlichen Anforderungen an

eine normenklare Regelung der Erhebung, Weitergabe oder sonstigen Nutzung von Arbeitnehmerdaten.

Ich halte es daher für unabdingbar, anläßlich der jetzt anstehenden Novellierung des BremPersVG die Datenverarbeitung durch den Personalrat möglichst präzise zu normieren.

Das BremPersVG erlegt der Dienststelle und dem Personalrat die Pflicht auf, darüber zu wachen, daß alle in der Dienststelle tätigen Personen nach "Recht und Billigkeit" behandelt werden. Der zur Erreichung dieser Zielnorm beispielhaft aufgeführte Katalog sollte um die Verpflichtung, das informationelle Selbstbestimmungsrecht der Beschäftigten zu gewährleisten, erweitert werden. Außerdem habe ich angeregt, im Gesetzestext klarzustellen, daß auch die Datenschutzvorschriften zu den Bestimmungen gehören, über deren Einhaltung die Personalvertretung zu wachen hat.

Hinzu kommt, daß sowohl aufgrund divergierender Gerichtsentscheidungen u. a. des Bundesarbeitsgerichts und des Bundesverwaltungsgerichts als auch wegen zahlreicher in der Praxis der Personalvertretungen aufgetretener Streitfragen festgelegt werden muß, in welchem Umfang, für welchen Zweck und für welche Dauer Personalräte ihnen übermittelte Daten der Beschäftigten verarbeiten dürfen.

Das allgemeine Informationsrecht des Personalrats gegenüber der Dienststelle sollte konkretisiert werden, was Umfang und Form der Vorlage in Dateien gespeicherter Angaben oder listenmäßig aufgeführter Personaldaten angeht.

Außerdem muß festgelegt werden, daß dem Personalrat anläßlich eines Mitbestimmungsverfahrens zugänglich gemachte personenbezogene Daten nach Abschluß des Verfahrens zu löschen bzw. - wie etwa Bewerbungsunterlagen - zurückzugeben sind, soweit sie nicht zur Erfüllung anderer gesetzlicher Aufgaben - etwa für die Beurteilung von Vergleichsfällen - später noch erforderlich sind.

4.5. Personaldaten: On-line-Anschluß ohne Rechtsgrundlage

Die Senatskommission für das Personalwesen (SKP) hat mir auf Anfrage mitgeteilt, daß in der PAADIS-Dienstvereinbarung vom 08. September 1992 zwar vorgesehen sei, bei Bedarf unständige Bezüge, Bestandteile von bzw. nebenamtliche Vergütungen von den Beschäftigungsdienststellen direkt in PAADIS (Personalabrechnungs- und Änderungsdienst) einzugeben bzw. dort abzurufen. Gebrauch gemacht worden sei hiervon bisher noch nicht.

Meinen Hinweis auf § 14 Bremisches Datenschutzgesetz (BrDSG), wonach die Einrichtung eines automatisierten Abrufverfahrens nur aufgrund Bundes- oder Landesrecht zulässig ist (Abs. 1) und nur durch Rechtsverordnung eingeführt werden darf (Abs. 2), hält die SKP für unbeachtlich. Nach ihrer Auffassung erübrigt es sich nach der Novellierung des Bremischen Beamtengesetzes (vgl. o. Ziff. 4.3), eine Rechtsverordnung nach § 14 Abs. 2 BrDSG zu erlassen, weil nach dem neuen Recht der Datenfluß zwischen Teilen der Personalakte keine Übermittlung darstelle. Datenabrufe der Personalstellen aus den Datenbeständen der Bezüge zahlenden Stellen hätten den gleichen rechtlichen Charakter.

Diese Auffassung ist nicht zutreffend. Weil für einzelne Aufgabenbereiche bzw. Bearbeitungsvorgänge im Rahmen der Personalverwaltung und -wirtschaft mehrere Behörden zuständig sind, haben diese nach dem Personalaktenrecht die Befugnis, die für ihre jeweiligen (Teil-)Zwecke erforderlichen Personalaktendaten zu verarbeiten, wozu nach dem neuen § 93a Abs. 1 BremBG auch die in (automatisierten) Dateien gespeicherten Angaben gehören. Gerade wegen dieser aufgeteilten Verarbeitungszuständigkeiten ist mit § 93 g Abs. 1 BremBG die Rechtsgrundlage für die Übermittlung von Personaldaten zwischen den personalverwaltenden Behörden geschaffen worden. Jede dieser Dienststellen bleibt im Rahmen ihrer jeweiligen Zuständigkeit "speichernde Stelle" im Sinne des BrDSG, der Datenaustausch zwischen ihnen folglich eine "Übermittlung" i. S. d. BrDSG.

Insofern bleibt es dabei, daß für die Einführung eines automatisierten Abrufverfahrens eine Rechtsverordnung nach § 14 Abs. 2 BrDSG notwendig ist, was der Senat im übrigen in der Begründung zu § 93 g Abs. 1 BremBG ausdrücklich anerkannt hat (vgl. Drs. 13/723, zu § 93 g).

Inzwischen hat mir das Justizvollzugsamt mitgeteilt, es sei nunmehr an PAADIS angeschlossen mit dem Zweck, sog. "unständige Leistungen" einzugeben. Ich habe daher die SKP aufgefordert, umgehend für den Erlaß der bisher fehlenden Rechtsverordnung zu sorgen, um den Verstoß gegen § 14 BrDSG zu beseitigen. Außerdem habe ich den Senator für Justiz und Verfassung über diesen rechtswidrigen Anschluß informiert und ihn gebeten, in seinem Geschäftsbereich entsprechend tätig zu werden.

4.6. Automatisierte Arbeitszeiterfassung

In meinem 15. Tätigkeitsbericht habe ich ausführlich über die Regelungen und DV-technischen Planungen zur Einführung der automatisierten Arbeitszeiterfassung (zunächst) in der Finanzverwaltung informiert (15. Jahresbericht, Ziffer 4.1.1). Die dort erhobenen Forderungen zur technischen Ausgestaltung wurden in einem mit mir abgestimmten Konzept zunächst weitgehend berücksichtigt. Nur auf den zentralen Server könne aus technischen Gründen nicht verzichtet werden. Es bestand jedoch Einigkeit darüber, daß die Arbeitszeitdaten in der jeweiligen Dienststelle, also dezentral, gespeichert würden.

Für mich und offensichtlich auch die Personalräte überraschend änderte der Finanzsenator gegen Jahresbeginn sein Konzept und wollte künftig doch eine zentrale Speicherung und Verarbeitung der Arbeitszeitdaten aller Beschäftigten der Dienststellen im Haus des Reiches auf einem entsprechend größer dimensionierten Server vorsehen.

Ich habe daraufhin eine umgehende "Nachbesserung" der Datensicherungsmaßnahmen verlangt. In einem Gespräch, in dem neben dem Senator für Finanzen und meiner Dienststelle auch die Firma, die die Hard- und Software für die Arbeitszeiterfassung liefern soll, vertreten war, wurde eine einvernehmliche Lösung unter Berücksichtigung der zentralen Datenspeicherung gefunden. Durch die Teilnahme des Firmenvertreters war auch sichergestellt, daß sich die gefundene Lösung technisch umsetzen läßt.

Wichtige Merkmale dieser Lösung sind, daß

- zwischen den Arbeitsplatzrechnern in den Dienststellen, auf denen die Arbeitszeitkonten verwaltet werden, und dem Zentralserver keine Wählleitungen, sondern Standleitungen geschaltet werden,

- der Server nicht von außen anwählbar ist, sondern von sich aus die Zeiterfassungsterminals anwählt,

- der/die Gleitzeitbeauftragte in der Dienststelle nur Zugriff auf die Daten der Mitarbeiter und Mitarbeiterinnen seiner Dienststelle hat,

- die erforderlichen Sicherungen (Backups) zentral gesteuert werden, aber dabei (durch Menüsteuerung) sichergestellt wird, daß eine Einsicht in die Daten nicht möglich ist,

- der Ausdruck der monatlichen Journale auf einem zentralen Drucker mit verdecktem Druck erfolgt, so daß eine unautorisierte Einsichtnahme in das Journal zumindest festzustellen ist (der Umschlag muß hierzu geöffnet werden) und

- der Ausdruck von dem/der Gleitzeitbeauftragten der jeweiligen Dienststelle "angestoßen" wird.

Es wurde ein mit mir abgestimmtes Organisations- und Datensicherungskonzept erstellt, so daß einem (Probe)-Betrieb - nach Abschluß der erforderlichen Mitbestimmungsverfah-

ren bzw. Inkrafttreten der notwendigen Regelungen - aus meiner Sicht nichts entgegensteht.

5. Inneres

5.1. Polizei

5.1.1. Informationssystem ISA-D ohne ausreichenden Datenschutzstandard

5.1.1.1. Stand der Vernetzung

Im Dezember 1993 wurde das DV-System ISA-D (Informationssystem Anzeigen - Dezentral) als besonders nutzerfreundliches Informationssystem der Polizei der Öffentlichkeit vorgestellt. Bereits im Herbst 1993 war mit der Installation der PC-Netze begonnen worden. Insgesamt ist geplant, ca. 140 PC in den Polizeirevieren und Dienststellen der Bremer Kriminalpolizei zu installieren. Damit wird es den dort beschäftigten Polizeibeamten möglich, sich mit verschiedenen Informationssystemen des Bundes und des Landes in Verbindung zu setzen und online Daten abzufragen. Aus folgenden Datenbeständen sind Abrufe geplant:

- Kfz.- und Halterinformationssystem des Bundes (ZEVIS) und des Landes Bremen (FAZID)
- Einwohnermeldedatenbank des Landes (EDAS/DEMOS)
- Polizeiliches Informationssystem über Straftatverdächtige und Täter, Anzeigeerstatter, Hinweisgeber und Geschädigte im Lande Bremen (ISA)
- Polizeiliche Zentral- und Verbunddatei beim Bundeskriminalamt (INPOL)
- Ausländerzentralregister beim Bundesverwaltungsamt (AZR).

Ungeachtet der prinzipiellen rechtlichen Bedenken, die ich gegenüber der Einführung von ISA-D - insbesondere wegen fehlender bereichsspezifischer bundesrechtlicher Datenschutzvorschriften - geäußert habe (vgl. zuletzt 13. JB, S. 21; 14. JB, S. 19), habe ich dieses Verfahren weiter begleitet. In einer Reihe von Gesprächen mit Vertretern des Senators für Inneres und Sport habe ich die erforderlichen Datenschutzmaßnahmen dargelegt; zum Teil habe ich mich an ihrer Erarbeitung beteiligt.

5.1.1.2. Datenschutzkonzept nicht realisiert

In diesem Zusammenhang habe ich immer deutlich gemacht, daß bereits bei der Einführung von ISA-D ein aus folgenden Eckpunkten bestehendes Datenschutzkonzept verwirklicht sein muß:

- Rechtsverordnung gem. § 14 Abs. 2 BrDSG

  Bereits in meinem 11. Jahresbericht (vgl. S. 55) habe ich auf die Notwendigkeit hingewiesen, daß eine Rechtsverordnung gem. § 14 Abs. 2 BrDSG vom Senator für Inneres und Sport erlassen wird. Diese Regelung ist gerade deshalb in das bremische Datenschutzrecht aufgenommen worden, weil online-Abrufverfahren besonders schnell und einfach, insbesondere aber ohne vorherige Prüfmöglichkeit der speichernden Stelle, eine Datenübermittlung ermöglichen. ISA-D mit seiner einheitlichen Benutzeroberfläche läßt aufgrund seiner besonderen technischen Ausgestaltung einen problemlosen Wechsel zwischen den o. a. Informationssystemen des Bundes und des Landes zu. Ein solches Abrufsystem darf nur betrieben werden, wenn durch eine Rechtsverordnung ergänzende Datenschutzregelungen getroffen worden sind. Für ISA-D gibt es aber derzeit keine solche Regelung.

- Datenschutzkonzept

  Bisher liegt mir nur der Entwurf eines Datenschutzkonzeptes vom Januar 1993 vor. Auf einer Besprechung mit Vertretern des Senators für Inneres und Sport im Dezember 1993 wurde mir ein neuer Entwurf präsentiert, zu dem ich ergänzende Vorschläge unterbreitet habe. Sie beziehen sich u. a. auf die Frage der Berechtigungsverwaltung und die Zugriffsmöglichkeiten auf die Datenschutzprotokollierung. Weiter habe ich die Übertragung der Daten in unverschlüsselter Form, insbesondere im Hinblick auf die Kennungen und Paßwörter, kritisiert. Auf die Darstellung weiterer, mehr technischer Kritikpunkte wird an dieser Stelle verzichtet.

- Dienstanweisungen

  Ergänzend zum Datenschutzkonzept ist vorgesehen, Dienstanweisungen zur Benutzung von ISA-D zu erlassen. Darin wären u. a. die Nutzung und Verwahrung der Magnetkarte wie auch der Umgang mit Ausdrucken etc. zu regeln. Diese Dienstanweisungen waren anläßlich der Besprechung im Dezember 1993 noch nicht fertiggestellt. Es wurde zwar zugesichert, mir die fertigen Entwurfstexte zur Verfügung zu stellen, bis zum Redaktionsschluß lagen sie mir jedoch noch nicht vor.

- Magnetkarten oder Chipkarten

  Bereits in meinem 13. Jahresbericht (vgl. S. 16) habe ich darauf hingewiesen, daß bei der technischen Ausgestaltung von ISA-D alle abfrageberechtigten Polizisten Chip- oder Magnetkarten erhalten müssen, um die Abwehr unberechtigter Benutzer sicherzustellen. Daraus ergibt sich, daß ich die Verwendung von Magnetkarten nicht grundsätzlich ausgeschlossen habe. Gleichwohl haben sich sowohl aufgrund der technischen Weiterentwicklung und wegen nachlassender Preise der Chipkartensysteme als auch wegen der tatsächlichen Ausgestaltung der Einführung der Magnetkarte in den Kartenleser von ISA-D Bedenken gegen das jetzige Verfahren ergeben, die ich dem Senator für Inneres und Sport im Juni 1993 vorgetragen habe. Auf der Besprechung im Dezember 1993 habe ich die Risiken der Verwendung von Karten mit Magnetstreifen statt mit Chips noch einmal konkretisiert. Eine Antwort des Senators für Inneres und Sport insbesondere zu den Manipulationsmöglichkeiten steht noch aus.

Ingesamt wird das neue ISA-D noch ohne die erforderlichen Regelungen und Datenschutz- bzw. Datensicherungsmaßnahmen betrieben. Von einer förmlichen Beanstandung habe ich bisher noch abgesehen im Hinblick auf die Zusagen der senatorischen Behörde, die rechtlichen wie technischen Defizite alsbald zu beheben.

5.1.1.3. Fehlende Bereinigung der Datenbestände

In den Besprechungen des letzten Jahres habe ich ebenso wie in meinen Jahresberichten (vgl. 13. und 14. Jahresbericht) immer wieder mit Nachdruck darauf aufmerksam gemacht, daß die Datenbestände in ISA (alt) bereinigt und aktualisiert werden müssen. In diesem Zusammenhang hatte ich vor Einführung von ISA vorgeschlagen, den Altbestand von ISA mit ADV-technischer Unterstützung nach Datenschutzschwerpunkten qualifiziert zu untersuchen und zu bereinigen. Meine in den Jahren aufgrund von Eingaben und Beschwerden von Bürgern durchgeführten Einzelfallprüfungen haben in einer Vielzahl von Fällen u. a. zu Änderungen der Datenspeicherung oder der Löschfristen, zu Berichtigungen oder aber auch zu Löschungen gesamter Datensätze geführt. Die Mängel des alten ISA-Verfahrens setzen sich - soweit es zu weiteren Speicherungen in der Folgezeit gekommen ist - immer weiter fort. Es war und ist unerläßlich sicherzustellen, daß das polizeiliche Informationssystem nur solche Daten enthält, deren Speicherung rechtmäßig und aktuell erforderlich sind. Dieser Rechtspflicht ist nach wie vor nicht Rechnung getragen worden. Das dringend notwendige aktualisierte Datenschutzkonzept müßte z. B. eine Trennung zwischen Vorgangs- und Kriminalaktennachweissystem ebenso vorsehen wie

eine Trennung zwischen Tätern und Tatverdächtigen auf der einen und sogenannten Dritten (z. B. Geschädigte, Anzeigeerstatter) auf der anderen Seite.

5.1.1.4. Keine Rechercheprogramme für die Datenschutzkontrolle

Wiederholt habe ich darauf hingewiesen, daß es nicht ausreichend ist, die einzelnen Datenabfragen zu protokollieren. Vielmehr müssen für die Kontrolle durch den Landesbeauftragten für den Datenschutz auch Auswertungsprogramme zur Verfügung gestellt werden, die eine gezielte Datenrecherche ermöglichen. Meine Vorschläge habe ich im Berichtsjahr gegenüber dem Senator für Inneres und Sport konkretisiert, bisher allerdings ohne Reaktion.

5.1.2. Erfolgskontrolle der erweiterten Fahndungsbefugnisse

Angesichts der in Politik und Medien stark in den Vordergrund gerückten Entwicklung steigender Kriminalität in der Bundesrepublik Deutschland stellen sich auch die Datenschutzbeauftragten der öffentlichen Debatte, ob und in welchem Umfang eine Ausweitung polizeilicher Befugnisse geeignet ist, die Prävention und die Aufklärungsquote von Straftaten tatsächlich entscheidend zu verbessern.

In den letzten Jahren - zuletzt vor allem durch das 1992 verabschiedete Gesetz zur Bekämpfung der organisierten Kriminalität (OrgKG) - sind die Befugnisse der Polizei besonders im technischen Bereich zu Lasten des Rechts auf informationelle Selbstbestimmung, des Fernmeldegeheimnisses nach Art. 10 GG und des Rechts auf Unverletzlichkeit der Wohnung nach Art. 13 GG erheblich ausgeweitet worden (vgl. 15. JB, Ziff. 1.1). Hierzu gehören die neu geregelten Methoden wie Rasterfahndung, Einsatz verdeckter Ermittler und technischer Mittel zur Strafverfolgung und Gefahrenabwehr ebenso wie die Weiterentwicklung bestehender Instrumente zur automatisierten Datenverarbeitung (z. B. das automatisierte Fingerabdrucksystem AFIS, vgl. dazu Ziff. 5.1.3). Dabei ist der Kreis der von diesen Maßnahmen Betroffenen immer weiter ausgedehnt worden, und zwar auch auf Nichtverdächtige, Kontakt- und Begleitpersonen und sonstige Unbeteiligte.

In der Diskussion über grundrechtsrelevante Maßnahmen zur Verbesserung der inneren Sicherheit wird Bedenken gegen die Verhältnismäßigkeit der drohenden Grundrechtseingriffe vielfach mit der pauschalen Behauptung begegnet, erweiterte Ermittlungs- und Fahndungsbefugnisse seien unverzichtbar. Diese Linie zeichnet sich auch wieder bei der aktuellen Diskussion um die Einführung des sogenannten Großen Lauschangriffs ab.

Die Datenschutzbeauftragten fordern daher seit langem, zunächst die vorhandenen Möglichkeiten im Bereich der Gefahrenabwehr und der Strafverfolgung effektiv zu nutzen und ihre Wirksamkeit zu bewerten, bevor weitere, mit tieferen Eingriffen in Grundrechte verbundene Befugnisse eingeführt werden. Bezeichnend ist, daß bundesweit verifizierbare Zahlen über den Einsatz und den Erfolg z. B. der neuen Ermittlungsmethoden nach dem OrgKG nach meiner Kenntnis bisher nicht vorliegen.

Meine Kollegen und ich haben deshalb verabredet, das jeweilige Innenministerium um Mitteilung der vorhandenen Informationen über die Evaluation der erweiterten polizeilichen Befugnisse zu bitten. Führen beispielsweise Maßnahmen in vielen Fällen zu Eingriffen in das Recht auf informationelle Selbstbestimmung unbeteiligter Dritter, ohne daß sie in einer relevanten Zahl von Fällen den vom Gesetzgeber angestrebten Erfolg erreichen, fehlt es an der verfassungsrechtlich gebotenen Verhältnismäßigkeit der Mittel.

Zur Aufbereitung dieser Fragestellung habe ich den Senator für Inneres und Sport um die Beantwortung folgender Fragen gebeten:

- Welche praktischen Möglichkeiten bestehen, um gesetzlich vorgesehene Befugnisse und einzelne Instrumente der Strafverfolgung, der Gefahrenabwehr und der vorbeugenden Straftatenbekämpfung - vor allem im technischen Bereich - auf ihre Geeignetheit und Wirksamkeit zu untersuchen?

- Sind diese Maßnahmen nach den bisherigen Erfahrungen tatsächlich unabdingbar oder könnten einzelne wenigstens zeitweise oder gebietsweise ausgesetzt werden, ohne daß sich Nachteile für die Aufgabenerfüllung zum Schutz der inneren Sicherheit ergäben?

- Wie wird für vorhandene und künftige Regelungen sichergestellt werden, daß Unbeteiligte von den Maßnahmen zur Straftatenbekämpfung so wenig wie möglich betroffen werden, damit schwerwiegende Eingriffe in ihre Grundrechte vermieden werden?

- Welche rechtlichen und praktischen Schritte kommen insoweit in Betracht?

- Könnten diese Schritte zeitweise oder gebietsweise erprobt werden, um eine realistische Überprüfung der Notwendigkeit für diese schwerwiegenden Eingriffe zu erreichen?

Ich habe dabei deutlich gemacht, daß es nicht darum geht, ob die bestehenden Befugnisse bei untypischen Ausnahmefällen weiterhelfen, sondern um die ohnehin begrenzte Anwendung im Sinne der jeweiligen Regelungen, d. h. um den Regelfall. In diesem Zusammenhang habe ich auch an den Beschluß der Innenministerkonferenz vom 18./19.01.1990 zu den INPOL-Grundsätzen erinnert, der für dieses polizeiliche Informationssystem eine derartige Erfolgskontrolle vorsieht. Da ich erst vor kurzem diese Anfrage an den Senator für Inneres und Sport gerichtet habe, liegt mir derzeit noch keine Antwort vor.

5.1.3. Automatisiertes Fingerabdruckinformationssystem (AFIS)

Mit großen Schlagzeilen, wie z. B. "Mit AFIS auf Ganovenjagd", wurde die Inbetriebnahme des automatisierten Fingerabdruckidentifizierungssystems (AFIS) im letzten Jahr gefeiert. Auch das Land Bremen beteiligt sich an AFIS, in dem Fingerabdrücke von Asylbewerbern, von anderen Ausländern und von Personen, die von der Polizei erkennungsdienstlich behandelt wurden, gespeichert sind (vgl. 15. JB, Ziff. 5.2.1.1). Das System wurde allerdings in Betrieb genommen, ohne daß die erforderlichen datenschutzrechtlichen Voraussetzungen getroffen worden sind.

AFIS ermöglicht es, an Bremer Tatorten festgestellte Fingerabdruckspuren über den BKA-Zentralrechner mit den derzeit dort gespeicherten rund 1,9 Mio. Fingerabdrucksätzen abzugleichen. Kurz nach dem Einlesen liefert das System - soweit vorhanden - den "Treffer". Anschließend wird noch einmal überprüft, ob tatsächliche Identität mit einem der angelieferten Fingerabdrücke besteht. Mit der zugehörigen Nummer kann dann im INPOL-System der Name der betreffenden Person recherchiert werden.

AFIS ist bei der bereits jetzt für die erkennungsdienstliche Behandlung zuständigen Organisationseinheit des Kriminaltechnischen Dienstes beim Polizeipräsidium Bremen installiert. Es soll dabei als LKA-Funktion wahrgenommen werden. Die Fingerabdrücke von erkennungsdienstlich behandelten Personen werden in dem bisher üblichen Verfahren in Papierform erhoben und an das BKA zur Erfassung übersandt. Ein besonderes Bremer "Fenster", d.h. ein separierter Datenbestand ortsgebundener Spuren, zu dem nur bremische Polizeidienststellen zugreifen dürften, ist in AFIS nicht vorgesehen. Alle von Bremen eingestellten Datensätze können daher von allen an AFIS angeschlossenen Stellen abgerufen werden. Bremen kann das System allerdings lediglich zur Recherche, d.h. als Identifizierungs- und Spurensuch-System, nutzen. Eine direkte Einspeicherung auf elektronischem Wege durch Bremer Polizeidienststellen ist nicht vorgesehen.

Auf der Grundlage der mir auszugsweise zur Verfügung gestellten Unterlagen der Lieferfirma habe ich im Mai des letzten Jahres ein Gespräch über den Einsatz mit Vertretern des Senators für Inneres und Sport geführt.

Nach Klarstellung einiger offener Punkte habe ich mich im September erneut an das Innenressort gewandt und folgende Forderungen erhoben:

1. Berechtigung

   Es ist zu klären und festzulegen, wer aus welchem Anlaß aus Bremen und Bremerhaven berechtigt ist, eine Recherche in AFIS durchzuführen.

2. Dokumentation

   An AFIS soll nur ein begrenzter Personenkreis arbeiten. Da diese Bediensteten aber häufig im Auftrag anderer Polizeibeamter tätig werden, ist festzulegen, wie die Abfrage für andere Abteilungen dokumentiert wird, um nachprüfen zu können, ob ordnungsgemäße Aufträge erteilt wurden.

3. Automatisierte Protokollierung

   Es ist zu klären, in welchem Umfang Bremer Zugriffe im AFIS-System automatisiert protokolliert werden und welche Auswertungsprogramme für die Protokolldaten zur Verfügung stehen. Gleiches gilt für die Frage, ob bei der Recherche nur eine Protokollierung der Treffer oder aller Anfragen vorgesehen ist. Ich habe deshalb um die Mitteilung des Datensatzes gebeten.

4. Datenschutzkonzept

   Bei dem Gespräch ging ich davon aus, daß vor Einführung von AFIS eine Errichtungsanordnung erforderlich ist. Das Polizeipräsidium sicherte in diesem Zusammenhang zu, daß entsprechende Datenschutzregelungen in der Errichtungsanordnung mit eingearbeitet werden sollen. Der Polizeiführungsstab hat mit Schreiben vom 08.02.1994 mitgeteilt, daß der Bundesbeauftragten für den Datenschutz dem AFIS-Projekt zugestimmt hat, ein anwendungsspezifisches Datenschutzkonzept werde für das Gesamtprojekt beim BKA erstellt. Dieses Konzept liegt mir noch nicht vor.

5. Rechtsverordnung

   Bei AFIS handelt es sich um ein online-Abrufsystem. Gem. § 14 Abs. 2 BrDSG ist die Einrichtung eines automatisierten Abrufverfahrens durch Rechtsverordnung einzuführen. Ein solches Verfahren darf nur eingerichtet werden, soweit dies unter Berücksichtigung des informationellen Selbstbestimmungsrechts des betroffenen Personenkreises und der Aufgaben der beteiligten Stellen angemessen ist. Die Datenempfänger, die Datenart und der Zweck des Abrufs sind festzulegen. Der Landesbeauftragte für den Datenschutz ist vorher zu beteiligen. Die Zweckbindungsgrundsätze nach § 12 BrDSG sollten dabei Berücksichtigung finden. Ich habe deshalb um Mitteilung gebeten, wie weit die Vorarbeiten an der Rechtsverordnung gediehen sind.

Darüber hinaus hat mir auf Anfrage das Polizeipräsidium im Februar 1994 mitgeteilt, die Datei AFIS werde vom BKA als Zentralstelle für den elektronischen Datenverbund gem. den Dateienrichtlinien für das BKA als Verbunddatei beim BKA geführt. Danach seien die Verbundteilnehmer verpflichtet, Daten auf Stromwegen anzuliefern. Deshalb sei eine Errichtungsanordnung vom BKA und nicht von den einzelnen Ländern zu erstellen. Eine Errichtungsanordnung für AFIS auf Bundesebene befinde sich aber noch im Abstimmungsprozeß beim BKA und in den zu beteiligenden Gremien. Das Genehmigungsverfahren beim Bundesminister des Innern schließe sich dann an. Das Abstimmungsverfahren finde zur Zeit im AK II der Innenministerkonferenz statt. Das Ergebnis bleibe abzuwarten. Sobald aber eine verabschiedete und genehmigte Fassung der Errichtungsanordnung vorliege, würden dann noch evtl. von Bremen zu treffende Datenschutzmaßnahmen eingearbeitet.

Folgende grundsätzliche Probleme blieben bisher ungelöst:

Ich bin der Meinung, daß das AFIS in der bestehenden Doppelfunktion sowohl für erkennungsdienstliche Dateien der Polizei- und Strafverfolgungsbehörden als auch für Ausländ-

derbehörden gegen das verfassungsrechtliche Zweckbindungsgebot, wie es das Bundesverfassungsgericht entwickelt hat, verstößt. Danach dürfen Daten grundsätzlich nur für den jeweiligen Erhebungszweck (Asylbewerberdaten für ausländerrechtliche Maßnahmen bzw. erkennungsdienstliche Daten, die nach der Strafprozeßordnung oder nach polizeirechtlichen Normen erhoben wurden, nur für diese Zwecke), genutzt werden, es sei denn, die Zweckänderung ist ausnahmsweise ausdrücklich erlaubt. Eine solche Befugnis liegt nach meiner Rechtsauffassung für die Vorratsspeicherung der erkennungdienstlichen Asylbewerberdaten bei der Polizei nicht vor und wäre auch unverhältnismäßig. Deshalb trete ich auch für eine Trennung der Suchläufe ein. Klärungsbedürftig ist deshalb, ob bei einer Abfrage durch die Polizei bei der Recherche im Datenbestand des BKA nur auf die von der Polizei eingestellten Daten oder auch auf die von den Ausländerbehörden eingestellten Daten im AFIS zugegriffen werden darf.

Ich muß feststellen, daß dieses System einer rechtlichen Prüfung unter Berücksichtigung der Kriterien des Volkszählungsurteils nicht standhalten würde. Weiter ist festzustellen, daß bisher nicht einmal die nach allgemeinem Datenschutzrecht erforderlichen Voraussetzungen geschaffen wurden. Das System wird dennoch nach der Devise betrieben: "Der Datenschutz kann warten!"

5.2. Ausländer

5.2.1. Fall: Voreilige Ermittlungen wegen angeblicher Scheinehe

Eine Aufenthaltserlaubnis mit zunächst einer Befristung von drei Jahren wird einem Ausländer erteilt, der mit einem deutschen Partner verheiratet ist (§ 23 Ausländergesetz). In dem einer Eingabe zugrunde liegenden Fall sah sich der zuständige Sachbearbeiter des Ausländeramtes wegen zweier geringfügiger Verfahren veranlaßt, das Polizeipräsidium Bremen im Wege der Amtshilfe ermitteln zu lassen, ob es sich bei dieser Ehe um eine "Scheinehe" handele. Ein Schutzpolizeibeamter des zuständigen Reviers erkundigte sich daraufhin in der Nachbarschaft mit dem Ergebnis, daß eine eheliche Lebensgemeinschaft tatsächlich besteht. Von diesen Ermittlungen erfuhr der deutsche Ehepartner und war zu Recht sehr betroffen. Ich wurde erst eingeschaltet, nachdem eine Dienstaufsichtsbeschwerde abgeschlossen war. Das Ausländeramt hatte schon selbst erkannt, die Überprüfung zu früh eingeleitet zu haben. Es wird zukünftig solche Amtshilfeersuchen zur Feststellung einer Scheinehe erst dann stellen, wenn dafür konkrete Anhaltspunkte vorliegen. Der Katalog dieser Anhaltspunkte ist durch eine hausinterne Anweisung entsprechend eingeschränkt worden. Der Fall zeigt, daß gelegentlich vorschnell "durchermittelt" wird und dabei auch sensible Daten erhoben werden, ohne das Gewicht von Hinweisen oder Verdachtsmomenten vorher sorgfältig zu prüfen.

5.2.2. Unterbringung von Asylbewerbern

5.2.2.1. Bremische Gesellschaft

Kurz vor Ende des Jahres 1993 erhielt ich zunächst aus der Presse und dann durch eine Mitteilung der Bremischen Gesellschaft für Stadterneuerung, Stadtentwicklung und Wohnungsbau mbH (Bremische) die Information, daß sie zukünftig allein zuständig für die Unterbringung von Aussiedlern, Asylbewerbern, Emigranten, Kriegs- und Bürgerkriegsflüchtlingen und Obdachlosen in der Stadtgemeinde Bremen sein soll. Ich bin dankbar dafür, daß die Mitarbeiter der Bremischen - offensichtlich aufgrund von Erfahrungen aus früheren Projekten - mich unverzüglich eingeschaltet haben. So konnte in einem ersten Schritt gemeinsam ein Fragebogen für die Bewohner der Unterkünfte entworfen und sein Umfang auf den für die Abwicklung der Unterbringung erforderlichen Umfang begrenzt werden. Die ausgefüllten Fragebögen dienen als Datenbasis für ein DV-System, wobei großer Wert darauf gelegt wurde, daß die Datenverarbeitung für diesen Personenkreis vollkommen abgeschottet von dem privatrechtlichen Geschäftsbereich als Wohnungsbaugesellschaft erfolgt. Zu den Daten über Aussiedler, Asylbewerber, Obdachlose usw. wer-

den nur die mit dieser Aufgabe unmittelbar betrauten Mitarbeiter der Bremischen Zugriff haben . Das Datenschutzkonzept, in dem Zugriffe, Sperr- und Löschfristen zu regeln sein werden, wird zur Zeit erarbeitet.

5.2.2.2. Asylschiff

Aufgrund von Hinweisen auf und Veröffentlichungen über eine angeblich umfassende Überwachung der auf dem Asylschiff "EMBRICA-MARCEL" untergebrachten Asylbewerber sah ich mich veranlaßt, dort eine unangemeldete Datenschutzprüfung vorzunehmen.

Mich interessierten im Rahmen der vertraglichen Festlegungen durch die Freie Hansestadt Bremen zur Unterbringung und Betreuung von Asylbewerbern insbesondere die Pflichten zur Datenerhebung und -speicherung sowie zur Mitteilung an andere Stellen. Dazu gehören auch Informationsverpflichtungen gegenüber der Wohnungshilfe des Amtes für soziale Dienste. So ist die Wohnungshilfe zu unterrichten, wenn ein Asylbewerber länger als drei Tage abwesend ist oder es zu Problemen mit einem bestimmten Bewohner gekommen ist.

Die Daten über die Bewohner werden fast ausnahmslos von der sog. Rezeption des Schiffes erhoben und verwaltet. Erstellt werden u. a. Bewohner-, Belegungs- und Abmeldelisten; letztere werden regelmäßig an die Wohnungshilfe übermittelt.

Der eingesetzte PC ist zusätzlich mit Lesegeräten, die an den Eingangs- und Ausgangsschleusen des Schiffes angebracht sind, verbunden. Jeder Bewohner erhält einen solchen elektronischen Chipschlüssel, mit dem er diese Türen betätigt; dies wird auf dem PC registriert. Wird festgestellt, daß ein Bewohner länger als drei Tage nicht auf das Schiff zurückgekehrt ist, erfolgt eine besondere Signalisierung für die Abmeldeliste. Er ist damit automatisch abgemeldet und bedarf bei einer Rückkehr einer erneuten Zuweisung durch die Wohnungshilfe. Dieses Verfahren ist insoweit korrekt, als nur die aktuellen Daten gespeichert bzw. vorhandene Angaben stets mit dem neuesten Datum des Betretens bzw. Verlassens des Schiffes überschrieben werden. Ich habe allerdings angeregt, Daten von Bewohnern, die mehr als zwei Wochen nicht zurückgekehrt sind, zu löschen.

Des weiteren wird ein Wachbuch in Loseblattform geführt, in dem jedes "besondere Vorkommnis" eingetragen wird. Ich konnte feststellen, daß dort z.B. auch Auskünfte oder Informationen von Sicherheitsbehörden vermerkt wurden, wenn diese für andere Mitarbeiter in der Rezeption wichtig sind oder eine Handlung dokumentierten.

Ein besonderes Augenmerk habe ich auf die Videoanlage gelegt. Es sind acht Videokameras auf dem Schiff installiert, davon sechs in den drei Fluren, eine im Aufenthaltsraum und eine vor der Außentür. Einwände habe ich gegen die optische Überwachung im Aufenthaltsraum; Gründe für ihre Notwendigkeit konnten nicht vorgebracht wurden. Die Aufnahmegeräte sind nach Auskunft des Kapitäns nicht an Videorecorder angeschlossen, die eine Aufzeichnung vornehmen könnten.

Der o. g. Chipschlüssel dient neben der Ein-und Ausgangskontrolle auch der Bedienung eines Lesegerätes an der Essensausgabe. Eine Datenspeicherung über die Essensausgabezeit hinaus erfolgt nicht.

Die Organisation der Datenverarbeitung auf dem Schiff entspricht nach meinen Kontrollergebnissen - von den genannten Einschränkungen abgesehen - den Vorgaben des Datenschutzrechts.

5.3. Straßenverkehr

5.3.1. Zentrale Register für Kraftfahrer

5.3.1.1. Zentrales Führerscheinregister

Der Senator für Inneres und Sport hat mir den Referentenentwurf des Bundesverkehrsministeriums für ein Gesetz zur Änderung des Straßenverkehrsgesetzes mit der Bitte um Stellungnahme vorgelegt.

Der Entwurf enthält eine Vielzahl neuer Datenverarbeitungsregelungen, die das informationelle Selbstbestimmungsrecht der Kraftfahrerinnen und Kraftfahrer nachhaltig tangieren. Insbesondere ist beabsichtigt, zusätzlich zu den ohnehin örtlich bestehenden Dateien ein zentrales Führerscheinregister beim Kraftfahrtbundesamt aufzubauen, in dem dann Fahrerlaubnisdaten von über 50 Millionen Bürgerinnen und Bürgern zentral gespeichert werden sollen. Der Referentenentwurf begründet dessen Notwendigkeit mit der vollständigen Aufhebung der Kontrollen an den Binnengrenzen der Europäischen Union (EU), mit dem Wegfall der Umtauschpflicht für die in einem EG-Mitgliedstaat ausgestellten Führerscheine sowie generell mit der weitgehenden Harmonisierung des Fahrerlaubnisrechts in der EU durch die sog. Führerschein-Richtlinie. Die dort enthaltene Verpflichtung zu einem effektiven gegenseitigen Informationsaustausch über die bestehenden Fahrerlaubnisse und ausgestellten Führerscheine könne wirksam nur durch Errichtung eines zentralen Fahrerlaubnisregisters in Deutschland erfüllt werden.

Diese Gründe sind nicht überzeugend. Sämtliche im Entwurf genannten Zwecke sollen sowohl von den örtlichen als auch von dem neuen zentralen Fahrerlaubnisregister erfüllt werden. Allein diese Doppelzuständigkeit läßt erkennen, daß eine bundesweite Führerscheindatei überflüssig ist.

5.3.1.2. Verkehrszentralregister

Einen weiteren tiefen Eingriff in das Persönlichkeitsrecht der Betroffenen stellen die im Entwurf enthaltenen Vorschriften über das Verkehrszentralregister dar. Zum einen sollen mehr Daten gespeichert werden als bisher. Zum anderen soll das Verkehrszentralregister für weitere Zwecke verwendet werden.

So soll z. B. die Einstellung eines strafgerichtlichen Hauptverfahrens nach Erfüllung von Auflagen bzw. wegen Fehlens des öffentlichen Interesses im Verkehrszentralregister über Jahre gespeichert werden. Auch die Speicherung des freiwilligen Verzichts auf die Fahrerlaubnis ist unverhältnismäßig. Wenn insbesondere ältere Personen aufgrund eigener Überzeugung ihren Führerschein abgeben und auf die Fahrerlaubnis verzichten, halte ich es für unabdingbar, daß deren Daten so gelöscht werden, daß sie nicht mehr als Führerscheinbesitzer in Erscheinung treten. Auch die Anordnung und die Teilnahme an einer Nachschulung müssen nicht eingetragen werden, weil diese Tätigkeiten ausschließlich den örtlichen Führerscheinstellen obliegen.

Alle im Verkehrszentralregister gespeicherten Daten sollen nach dem Entwurf für erheblich erweiterte Zwecke genutzt werden können. Damit soll eine unverhältnismäßige Perfektionierung des Verkehrszentralregisters zu einem Auskunfts- und Überwachungssystem erreicht werden. Insbesondere wird im Gegensatz zu den bisherigen Regelungen nicht präzise festgelegt, welche personenbezogenen Daten an welche Stellen übermittelt werden dürfen.

Eine neue Dimension des Datenschutzrückschritts entsteht, wenn erstmalig ausdrücklich erlaubt werden soll, Protokolldaten, d. h. Aufzeichnungen über die erfolgten Datenzugriffe, für die Verfolgung schwerer Straftaten zuzulassen. Selbst die Bundesregierung räumt in ihrem Erfahrungsbericht über das Zentrale Verkehrsinformationssystem (ZEVIS) ein, daß eine solche Notwendigkeit offensichtlich bisher nicht vorgelegen hat.

Vor allem aber verletzt diese beabsichtigte Verwendung den im Bundesdatenschutzgesetz (BDSG), in den Landesdatenschutzgesetzen sowie in der Fahrzeugregisterverordnung (FRV) enthaltenen Grundsatz, wonach personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle gespeichert werden, nur für diesen Zweck genutzt werden dürfen. Für ein bereichsspezifisches Abweichen von diesem Grundsatz gibt es keinerlei Veranlassung.

Abzulehnen ist auch die vorgesehene Einschränkung des Auskunftsanspruchs des/der Betroffenen gegenüber dem Kraftfahrtbundesamt. Entgegen der bisherigen Regelung im Bundesdatenschutzgesetz soll er Herkunft oder Empfänger der Daten nicht einschließen. Erschwerend kommt hinzu, daß die Auskunft gebühren- oder kostenpflichtig sein soll.

Ich habe gegenüber dem Senator für Inneres und Sport meine Bedenken und Anregungen dargelegt. Er hat meine Stellungnahme in den zuständigen Bund-Länder-Facharbeitskreis zur Beratung eingebracht; sie stieß jedoch dort auf Ablehnung. Nach letzten Informationen besteht allerdings die Aussicht, daß die Novellierung des Straßenverkehrsgesetzes in dieser Legislaturperiode nicht mehr realisiert wird.

5.4. Standesamt

5.4.1. Fall: Der Standesbeamte als unberechtigter Bevölkerungsstatistiker

Ein junger Vater beklagte sich im Berichtsjahr bei mir darüber, daß das Standesamt Bremen-Mitte sich weigere, die Geburt seines Kindes zu beurkunden. Der zuständige Standesbeamte hatte seine Weigerung damit begründet, daß der Vater nicht bereit sei, ihm die für die Bevölkerungsstatistik benötigten Angaben zu machen.

Ich habe dem Eingeber daraufhin mitgeteilt, daß das Standesamt die Bekanntgabe von Angaben, die es ausschließlich für die amtliche Statistik erhebt und nicht für seine sich aus dem Personenstandsrecht ergebenden Aufgaben benötigt, nicht zur Voraussetzung der Beurkundung machen darf. Diese Auffassung teilt der Senator für Inneres und Sport. Er gestand ein, daß dem Standesbeamten ein Fehler unterlaufen sei; das Kind wurde nachträglich auch ohne die Mitteilung der Statistikdaten registriert.

Dieser Fall zeigt plastisch, wohin die von mir mehrfach kritisierte Verquickung von Verwaltungsvollzug und amtlicher Statistik führen kann (vgl. 12 JB, Ziff. 2.2.5.2; 15. JB, Ziff. 5.5.1). Die strikte Trennung der Datenverarbeitung dieser beiden Bereiche ist die Kernaussage des Volkszählungsurteils des Bundesverfassungsgerichts von 1983. Es ist daher aus verfassungsrechtlichen Gründen nicht mehr hinnehmbar, daß Daten, die für Verwaltungszwecke nicht benötigt werden, durch die Verwaltung, in diesem Fall den Standesbeamten, sogar mit Auskunftspflicht für Zwecke der Bevölkerungsstatistik erhoben werden. Für die Zählung der Lebend- und Totgeburten zur Durchführung der Statistik der natürlichen Bevölkerungsbewegung werden zusätzlich zu den Angaben nach dem Personenstandsrecht auch das Körpergewicht, die Körperlänge und die erkennbaren Fehlbildungen des Kindes sowie die Erwerbstätigkeit der Mutter registriert. Der Standesbeamte erhält auf diesem Wege Kenntnis von ggf. sensiblen Daten, die er weder für die Beurkundung der Geburt noch für die Wahrnehmung anderer amtlicher Aufgaben benötigt.

Die von mir mehrfach angemahnte Novellierung des Bevölkerungsstatistikgesetzes läßt aber weiterhin auf sich warten. Auch in dieser Legislaturperiode kann nicht mehr mit der Verabschiedung einer datenschutzrechtlichen Anforderungen entsprechenden Regelung gerechnet werden.

Durch die Eingabe habe ich auch erfahren, daß die für die Lebend- und Totgeburten auszufüllenden Zählkarten, die vom Statistischen Landesamt stammen, nicht den Bestimmungen des Bevölkerungsstatistikgesetzes entsprechen. Dort wird nicht nur, wie nach dem Gesetz vorgesehen, nach Wohngemeinde und Alter der Eltern, sondern auch nach der Straße und Hausnummer der Hauptwohnung der Mutter sowie nach den exakten Ge-

burtsdaten der Eltern gefragt. Ich habe das Statistische Landesamt um die schnellstmögliche Anpassung der Kartenvordrucke an die Rechtslage und die Löschung der dort gespeicherten "überschießenden" Angaben gebeten. Eine Reaktion auf meine Kritik steht derzeit noch aus.

5.5. Ortsämter

5.5.1. Konzentration und Dezentralisierung von Verwaltungsaufgaben: Bürgerfreundlichkeit ohne Mehrfachspeicherung

In der bremischen Verwaltung wird seit längerer Zeit die Frage diskutiert, inwieweit durch Umorganisation oder Zusammenlegung von Aufgaben eine bürgerfreundlichere Verwaltung erreicht werden kann. In der Bundesrepublik gibt es bereits verschiedene Modelle, z. B. das Amt für Bürgerberatung der Stadt Bielefeld, wo bislang auf verschiedene Dienststellen der Stadtverwaltung verteilte Aufgaben an einer Stelle erledigt werden.

Das Stadtamt Bremen beabsichtigt, es den Bürgern zu ermöglichen, bei Aufsuchen der Meldebehörde aufgrund eines Wohnungswechsels innerhalb der Stadtgemeinde auch gleichzeitig ihren Kfz.-Schein dort aktualisieren zu lassen. Damit sollen den Bürgern unnötige Wege und Wartezeiten erspart werden.

Diese neue Aufgabe soll zunächst einer Meldestelle als Pilotanwendung übertragen werden, um den Aufwand für die Organsation und die Umsetzung der Maßnahme so gering wie möglich zu halten und um Erkenntnisse für die weitere Vorgehensweise sammeln zu können. Hierzu bietet sich aus der Sicht des Stadtamtes die Meldestelle des Ortsamtes Vegesack an, weil diesem Amt bereits Aufgaben der Straßenverkehrsbehörde Bremen als Außenstelle übertragen worden sind.

Das Datenschutzrecht geht prinzipiell aus von der klaren Trennung von Behördenfunktionen sowie einer strikten Zuordnung und Zweckbindung der für die jeweilige Funktion erhobenen und genutzten Datenbestände. Die Zulässigkeit der Bündelung unterschiedlicher gesetzlicher Aufgaben in einer Behörde bedarf daher im Einzelfall sorgfältiger Prüfung. Ein entscheidendes Kriterium für diese Beurteilung ist, ob dem Antragsteller die Wahlmöglichkeit offen bleibt: Er muß entscheiden können, ob er das zentrale Bearbeitungsangebot annimmt mit dem Risiko, daß in seinem Ortsamt Angaben aus unterschiedlichen Lebensbereichen bekannt werden, oder ob er nach wie vor das zentrale Amt in Anspruch nimmt. Für den Betroffenen darf es m. a. W. keinen Zwang geben, sich der Mithilfe der Meldebehörde bei der Änderung der Anschrift im Kfz.-Schein zu bedienen. Es muß ihm freigestellt bleiben, diesen Vorgang auch bei der Kfz.-Zulassungsstelle abzuwickeln. Im ersten Falle darf die Meldestelle im Ortsamt kein Doppel der Berichtigung in den Meldeunterlagen aufbewahren und auch sonstige Informationen aus diesem Vorgang nicht speichern, die ihr aufgrund ihrer Tätigkeit als Meldebehörde nicht zugänglich wären. Nur so läßt sich verhindern, daß Bürgerfreundlichkeit durch "kurze Wege" gleichzeitig zu einer Redundanz und Streuung von Datenspeicherungen führt.

Nach Angaben des Stadtamtes werden die vorgenannten Kriterien im Pilotprojekt uneingeschränkt beachtet. Die Behörde hält weiterhin die Einsichtnahme in die Kfz.-Zulassungsdatei für erforderlich, um rechtlich unzulässige Anschriftenänderungen zu vermeiden, z. B. bei Vorliegen einer vollziehbaren Stillegungsverfügung wegen fehlendem Haftpflichtversicherungsschutz oder einer vollziehbaren Betriebsuntersagung nach der Straßenverkehrszulassungsordnung (StVZO). Dazu soll ein online-Anschluß an die bei der Kfz.-Zulassungsstelle geführte automatisierte Datei FAZID eingerichtet werden.

Für die Zulässigkeitsvoraussetzungen ist maßgeblich, ob die Meldestelle durch Übernahme der Teilaufgabe "Anschriftenänderung auf dem Kfz.-Schein" insoweit funktional Teil der zentralen Straßenverkehrsbehörde wird oder nicht. Da in dem Vegesacker Modell die Meldestelle lediglich eine Hilfsfunktion für die Kfz.-Zulassungsstelle wahrnimmt, dem Bürger aber die Möglichkeit bleibt, die Adreßkorrektur auch dort vornehmen zu las-

sen, findet eine vollständige Übertragung der Aufgaben nicht statt. Beide Dienststellen bleiben daher funktional getrennte datenverarbeitende Stellen.

Die Einsichtnahme des Meldeamtes in die Kfz.-Zulassungsdatei FAZID stellt konsequenterweise eine Datenübermittlung dar. Für das automatisierte Abrufverfahren bedarf es daher der erforderlichen Rechtsgrundlagen nach § 14 Bremisches Datenschutzgesetz (BrDSG), die derzeit noch nicht vorliegen.

5.6. Meldewesen

5.6.1. Fall: Wählerdaten aus dem Melderegister?

Eine Bremerhavener Bürgerin beklagte sich darüber, daß sie seit der letzten Bürgerschaftswahl mehrfach von einer Partei und deren Bürgerschaftsfraktion zu Veranstaltungen in Bremerhaven und Bremen eingeladen worden sei, ohne Mitglied dieser Partei zu sein und ohne um Aufnahme in eine Einladungsdatei gebeten zu haben. Eine Erklärungsmöglichkeit war, daß die Bremerhavener Meldestelle zur letzten Bürgerschaftswahl an die örtliche Organisation der Partei Meldedaten übermittelt hatte und diese verwendet wurden, obwohl seit der letzten Bürgerschaftswahl bereits ca. zwei Jahre vergangen waren.

Gem. § 33 Abs.1 Bremisches Meldegesetz(BremMeldG) 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. Sortierkriterium darf dabei ausschließlich das Lebensalter der Betroffenen sein, z. B. für den Ausdruck von Jungwählerlisten. Den Betroffenen steht dabei ein Widerspruchsrecht zu. Die Parteien und Wählergruppen dürfen die Angaben nach § 32 Abs.4 BremMeldG nur strikt zweckgebunden und nur selbst im Rahmen der jeweils anstehenden Wahl nutzen. Die Verwendung für andere Zwecke, z. B. für Einladungen zu Parteiveranstaltungen, die mit der Wahl in keinem Zusammenhang stehen, ist ebenso unzulässig wie die Weitergabe der Wählerlisten an Dritte einschließlich der eigenen Parlamentsfraktion und der weitere Gebrauch der Adreßdatensätze nach der Wahl. Die Nichteinhaltung dieser Zweckbindung stellt nach § 35 Abs.2 Nr. 4 BremMeldG eine bußgeldbewehrte Ordnungswidrigkeit dar. In meinem 14. Jahresbericht (Ziff. 2.2.3.3) habe ich ausführlich über dieses Problem berichtet. Der Senat hat hierzu Durchführungsbestimmungen angekündigt, die bis heute nicht erlassen sind.

Woher das Adreßmaterial stammte, mit dem die Bremerhavenerin zu den Veranstaltungen der Partei und deren Bürgerschaftsfraktion eingeladen wurde, war im nachhinein nicht mehr präzise feststellbar.

Ich habe die Eingabe aber im Vorfeld der in diesem Jahr stattfindenden Wahlen zum Europäischen Parlament und zum Deutschen Bundestag zum Anlaß genommen, den Meldebehörden zu empfehlen, zur Sicherung der Zweckbindung, d. h. der Einladungsmöglichkeit zu Wahlveranstaltungen, den Parteien möglichst nur aus dem Melderegister erstellte Adreßaufkleber zu übersenden. Auch habe ich darum gebeten, die Datenempfänger auf ihre Verpflichtungen zur Einhaltung der wahlbezogenen Zweckbindung und zur Löschung der übermittelten Daten bzw. zur Vernichtung von Wählerlisten spätestens unmittelbar nach der Wahl hinzuweisen.

Unmittelbar vor Redaktionsschluß hat sich die Rechtslage durch Änderung des Melderechtsrahmengesetztes geändert bzw. konkretisiert. Neben dem in Bremen schon lange eingeführten Widerspruchsrecht für die Betroffenen wurde die Übermittlungsmöglichkeit der Parteien ausdrücklich auf Daten von Gruppen von Wahlberechtigten eingeschränkt, was die Übermittlung der Adreßdaten aller Wahlberechtigten ausdrücklich ausschließt. Außerdem werden die Parteien oder ihre Auftragnehmer verpflichtet, die Daten spätestens einen Monat nach der Wahl zu löschen. So kann verhindert werden, daß mit der Zeit ein Duplikat des Melderegisters/Wählerverzeichnisses bei den Parteien entsteht. Weitergehende Vorschläge zur Sicherung der informationellen Selbstbestimmung der Betroffenen

- wie z. B. Vorgabe der Art der Datenträger, Zustimmungslösung anstelle der Widerspruchslösung - wurden nicht realisiert.

Das Land Bremen muß jetzt sein Melderecht im Hinblick auf die Änderung des Melderechtsrahmengesetzes überprüfen.

5.6.2. Meldedaten für den Rundfunkgebühreneinzug

Die Konferenz der Innenminister des Bundes und der Länder(IMK) hat in ihrer Sitzung am 26.11.1993 beschlossen, den Ländern - soweit noch nicht erfolgt - eine Änderung ihrer Meldedatenübermittlungsverordnungen zu empfehlen: Die Meldebehörden sollen der zuständigen Landesrundfunkanstalt bzw. der GEZ zum Zwecke der Erhebung und des Einzugs der Rundfunkgebühren im Falle der Anmeldung, Abmeldung oder des Todes regelmäßig den Familiennamen (jetziger und früherer Name mit Namensbestandteilen), den Vornamen, ggf. den Doktorgrad, den Tag der Geburt, gegenwärtige und frühere Anschriften, den Tag des Ein- und Auszugs, den Familienstand sowie ggf. den Sterbetag volljähriger Einwohner übermitteln. Dieser Beschluß ist auf eine bereits seit längerer Zeit bestehende Forderung der öffentlich-rechtlichen Rundfunkanstalten -auch Radio Bremen hält dies für wünschenswert- zurückzuführen, für die regelmäßige Übermittlung von Meldedaten aller Einwohner an die GEZ bundesweit Rechtsgrundlagen zu schaffen. Bislang sahen dies nur die Meldedatenübermittlungsverordnungen einiger Länder vor. Die Rundfunkanstalten versprechen sich durch einen Abgleich mit den eigenen Datenbeständen eine wesentlich höhere Erfolgsquote bei der Ermittlung von Personen, die ihrer Gebührenpflicht bislang nicht nachgekommen sind.

An dem Beschluß der IMK ist zum einen zu kritisieren, daß nicht alle vorgesehenen Meldedaten für die Feststellung der Gebührenpflicht erforderlich erscheinen, z. B. die früheren Anschriften. Entscheidender Einwand aber ist, daß auch die Daten der weit überwiegenden Zahl derjenigen Einwohner der Bundesrepublik weitergegeben werden müßten, die ihre Gebühren immer korrekt bezahlt haben. Im Ergebnis könnte zumindest temporär ein Register aller Volljährigen entstehen. Die GEZ kann aus ihrer Feststellung, daß ein ihr gemeldeter Einwohner in ihrem Datenbestand bislang nicht verzeichnet war, auch keineswegs automatisch den Schluß ziehen, dieser habe seine Rundfunkgebührenpflicht verletzt. Es besteht durchaus die Möglichkeit, daß eine Gebührenpflicht schon deshalb nicht besteht, weil kein Radio vorhanden ist.

Auch wenn der automatisierte Datenabgleich nicht eingeführt wird, bleibt es bei der Regelung des geltenden Rundfunkgebührenstaatsvertrages, daß die Landesrundfunkanstalten im Einzelfall, d. h. bei tatsächlichen Anhaltspunkten für die Verletzung der Gebührenpflicht und soweit die Erhebung beim Betroffenen nicht möglich ist oder einen unverhältnismäßigen Aufwand erfordern würde, Auskünfte bei den Meldebehörden einholen dürfen.

Die von der IMK empfohlene Änderung der Meldedatenübermittlungsverordnungen der Länder ist von der Konferenz der Datenschutzbeauftragten in einer Entschließung abgelehnt worden (vgl. Ziff. 15.6). Ich habe dem Senator für Inneres und Sport diesen Beschluß zugeleitet. Offensichtlich will er gleichwohl die Bremische Meldedatenübermittlungsverordnung im Sinne des IMK-Beschlusses ändern. Sollte ein Entwurfstext vorgelegt werden, werde ich ihn kritisch kommentieren.

5.7. Personenstandswesen

5.7.1. Fall: Späte Heirat - Forschungsobjekt wider Willen

Ein Ehepaar beschwerte sich bei mir darüber, daß das Standesamt Bremen-Mitte ohne seine Kenntnis oder Einwilligung personenbezogene Daten an den Sonderforschungsbereich 186 der Universität Bremen weitergegeben habe. Die Prüfung des Vorgangs ergab daraufhin, daß das Amt zur Durchführung eines Forschungsprojekts "Ehe und Partnerschaft" die Namen, Anschriften, Berufe sowie die Geburts- und Heiratsdaten derjenigen

Personen übermittelt hatte, die 1991 oder 1992 geheiratet haben und zum Zeitpunkt der Eheschließung zwischen 45 und 55 Jahren alt waren. Die Übermittlung war erfolgt, indem Mitarbeiterinnen des Forschungsprojektes Einsicht in die Heiratsbücher der Jahre 1991 und 1992 gewährt wurde.

Der zuständige Standesbeamte rechtfertigte die Zulässigkeit der Einsichtnahme mit § 61 Abs. 1 Personenstandsgesetz (PStG), der "Behörden" diese Möglichkeit eröffnet, wenn sie sich dabei im Rahmen ihrer Zuständigkeit halten und den Zweck der Einsichtnahme angeben. § 86 Abs. 1 der Dienstanweisung für die Standesbeamten zähle zu den Behörden auch "Universitätsinstitute". Der Senator für Inneres und Sport teilte die Auffassung des Standesbeamten und berief sich auf die Bindungswirkung der Dienstanweisung, die eine Verwaltungsvorschrift im Sinne des Art. 84 Abs. 2 Grundgesetz darstelle.

Diese Rechtsauffassung zur Übermittlung von standesamtlichen Daten zu Forschungszwecken halte ich nach wie vor für unzutreffend. Das dringend novellierungsbedürftige Personenstandsgesetz sieht hierfür an keiner Stelle explizit eine Befugnis vor. Die Dienstanweisung für die Standesbeamten kann als Allgemeine Verwaltungsvorschrift gesetzliche Bestimmungen nur erläutern, nicht aber ändern oder erweitern. Hinzu kommt, daß unter "Einsichtnahme" typischerweise der Einblick in Einzelfällen, nicht aber wie bei diesem Projekt in bezug auf ganze Personengruppen zu verstehen ist.

Das allgemeine Datenschutzrecht trennt strikt zwischen der Datenübermittlung zu Verwaltungs- und der zu Forschungszwecken (vgl. §§ 13, 21 BrDSG; §§ 15, 14 Abs. 2 Nr. 9 BDSG). Im Verwaltungsverfahrensrecht ist der Begriff der "Behörde" eindeutig definiert und umfaßt zwar die Universitätsverwaltung, nicht aber Forschungseinrichtungen.

Für das Forschungsinteresse gerade an den Daten der Standesämter gibt es gute und anerkennenswerte Argumente. Es ist höchste Zeit, endlich die Novellierung des PStG, die die Datenschutzbeauftragten zum wiederholten Male gefordert haben (vgl. u.a. 15. Jahresbericht, Ziff. 5.6.1) anzugehen und dabei auch den Datenumgang für wissenschaftliche Zwecke zu regeln. Solange dies nicht der Fall ist, der Bundesgesetzgeber also eine Regelungslücke läßt und dem ebenfalls grundrechtlich abgestützten Informationsanspruch der Forschung (vgl. Art. 5 Abs. 3 GG) keine Rechnung trägt, muß dieses Defizit mit den einschlägigen Sonderbestimmungen des Landesdatenschutzrechts kompensiert werden.

Der Standesbeamte hat mit anderen Worten bei der Gewährung der Einsicht an die Mitarbeiter von Forschungsprojekten die Vorgaben des § 21 BrDSG, der die Datenverarbeitung zum Zwecke wissenschaftlicher Forschung regelt, zu berücksichtigen. Dazu gehören der Vorrang der Einwilligung der Betroffenen, bei Absehen von der Einwilligung die Prüfung der entgegenstehenden schutzwürdigen Belange, die Zweckbindung der erhobenen Daten und die frühzeitige Anonymisierung durch Abtrennung der Personalien von den übrigen Angaben.

Ich möchte erreichen, daß zwar der legitime Datenbedarf der Wissenschaft auch im Personenstandswesen gedeckt werden kann, dies aber unter den gleichen Bedingungen geschieht wie bei allen übrigen Datenbeständen der Verwaltung, für die keine speziellen Forschungsbestimmungen existieren.

6. Justiz

6.1. Prüfung der Justizvollzugsanstalt Oslebshausen

6.1.1. Der Anlaß: Aktenfunde

Im Jahr 1993 tauchte eine ganze Reihe von amtlichen Schriftstücken und Aktenteilen aus dem Bereich des Strafvollzuges in den Händen von Gefangenen oder in der Öffentlichkeit auf. In der lokalen Presse wurde ausführlich über diese Aktenfunde berichtet. Bei den Unterlagen handelte es sich z. B. um einen siebenseitigen Strafverfahrens-Registerausdruck, vier Aufnahmemitteilungen, zwei Beschlüsse von Strafvollstreckungskammern, ei-

nen Haftbefehl, eine Hausakte, zwei Gefangenen-Personalakten, Karteiakten und Vorführlisten sowie eine Polamydon-Ausgabeliste mit den Namen, Geburtsdaten und Ausgabemengen von ca. 70 Gefangenen.

Ich habe dies zum Anlaß genommen, eine eingehende Datenschutzprüfung in der Justizvollzugsanstalt Oslebshausen durchzuführen. Für die Prüfung wurden überwiegend Bereiche ausgewählt, die Zentral- oder Schnittstellen der Datenverarbeitung bilden. Nach Durchführung dieser Querschnittsprüfung wie auch der Untersuchung der Funde der Unterlagen und Akten haben sich folgende prinzipielle Vorgaben als unverzichtbar für einen korrekten Datenumgang im Strafvollzug herausgestellt:

6.1.2. Wesentliche Rahmenbedingungen

Erforderlich sind bereichsspezifische Regelungen für die automatisierte Datenverarbeitung wie für die Datenverarbeitung in Akten und manuellen Dateien, die den besonderen Verhältnissen im Strafvollzug Rechnung tragen (vgl. auch unten Ziff. 6.2). Im Rahmen eines umfassenden Datenschutzkonzeptes muß das Ziel verfolgt werden, daß nur der - möglichst kleine - Kreis von Berechtigten auf die für jeden einzelnen jeweils erforderlichen Daten Zugriff hat. Um dem Resozialisierungsgedanken und dem "Recht auf Vergessen" Rechnung zu tragen, sind für die Zeit nach der Entlassung der Gefangenen für deren Daten und Akten differenzierte Sperrungs- und Löschungsvorschriften vorzusehen.

Bei automatisierter Datenverarbeitung sind auch und gerade im Strafvollzug die im § 6 BrDSG vorgeschriebenen technischen und organisatorischen Maßnahmen zu treffen. Dies gilt insbesondere für das neue ADIV-Verfahren (vgl. Ziff. 6.2). Dort ist vorzusehen, daß alle relevanten Datenverarbeitungsvorgänge protokolliert werden. Differenzierte Löschungs- und Zugriffsregelungen sind zu erlassen. Nach Ausscheiden des Gefangenen aus dem Strafvollzug sind seine Daten im automatisierten Verfahren zu löschen. Ein Ausdruck - auch ein auszugsweiser Ausdruck - der zuletzt gespeicherten Daten kann zur Personalakte genommen werden, soweit die weitere Aufbewahrung dieser Daten erforderlich ist. Soweit es erforderlich sein sollte, kann darüber hinaus ein nur dem Auffinden dieser ausgesonderten Akten dienendes spezielles Nachweissystem mit besonderer Zugriffsberechtigung in automatisierter Form aufgebaut werden.

Mit Zunahme der ADV in der Gefangenenverwaltung wird die Bedeutung der verschiedenen Karteien und Buchwerke abnehmen. In vielen Fällen kann dann auf eine manuelle Datenhaltung ganz verzichtet werden. Durch geeignete Sicherungsvorkehrungen ist in jedem Fall zu gewährleisten, daß Gefangene keinen Zugang zu Datenverarbeitungsanlagen mit personenbezogenen Daten haben. Bei dem dezentralen Einsatz von Terminals ist sicherzustellen, daß Gefangene keine Einsichtsmöglichkeiten auf Bildschirme bekommen.

Die Prüfung der JVA Oslebshausen hat deutlich gemacht, daß die Datenverarbeitung in den Strafanstalten in einigen Bereichen gravierend geändert werden muß. Das Erforderlichkeitsprinzip, die Bindung der Nutzung der Daten an den Erhebungszweck sowie die rechtliche Begrenzung der Verwendung für andere Zwecke sind verfassungsrechtlich vorgegebene datenschutzrechtliche Prinzipien, die auch im Strafvollzug Geltung beanspruchen.

Die gesamte Datennutzung innerhalb der Anstalt ist zur Zeit so organisiert, daß mit Ausnahme der ärztlichen Unterlagen alle Daten, die einmal erhoben worden sind, intern frei verfügbar sind. Es kann aber nicht dabei bleiben, daß jeder Bedienstete innerhalb der Vollzugsanstalt über jeden Gefangenen "alles" erfahren kann und zwar unabhängig davon, ob er es für seine Aufgabenerfüllung braucht ob er überhaupt mit dem Gefangenen zu tun hat.

6.1.3. Konkrete Maßnahmen

In meinem Prüfbericht habe ich eine ganze Reihe von Maßnahmen zur Verbesserung des Datenschutzes angeregt. Einige Vorschläge sind nicht ohne eine Änderung der organisa-

torischen und räumlichen Situation zu verwirklichen. Details müssen "vor Ort" und in Kenntnis auch der personellen und finanziellen Möglichkeiten festgelegt werden. Empfehlungen habe ich u. a. für folgende Schwerpunktbereiche gegeben:

- Die Verwaltung aller personenbezogener Daten über Gefangene in Papierform sollte noch stärker bei der Vollzugsgeschäftsstelle konzentriert werden. Bisher wird von der Vollzugsgeschäftsstelle im Zuge des Aufnahmeverfahrens eine ganze Reihe von Datenträgern erstellt und anstaltsintern und -extern verteilt. Daß diese Papiere in der Anstalt bleiben, erscheint sowohl während der Haftzeit als auch nach Ausscheiden des Gefangenen aus dem Vollzug nicht gesichert. Die Übermittlung des vervielfältigten Aufnahmebogens mit allen seinen Daten u.a. an das Polizeipräsidium (LKA-INPOL), an die Ausländerbehörde oder den Senator für Justiz und Verfassung führt dazu, daß diesen Stellen weit mehr Daten zur Verfügung gestellt werden, als sie für ihre Aufgabenerfüllung benötigen.

- Der unmittelbare Zugang einer Vielzahl von Beschäftigten zur Vollzugsgeschäftsstelle ist nicht erforderlich. Gleiches gilt für die Poststelle und die Ordonnanz. Es empfiehlt sich, abgeschottete Bereiche mit klaren Zugangsberechtigungen zu bilden. Die Herausgabe und die Dokumentation des Verbleibs von Akten und sonstigen Datenträgern sind zu verbessern. Die Gefangenenpersonalakte ist nach der Entlassung umgehend zu vervollständigen (d. h. Zusammenführung mit sonstigen Unterlagen über den Gefangenen aus der JVA) und sicher zu archivieren.

- Die vielfältige Streuung der Veränderungsmeldungen (Umlaufpläne) sollte durch eine differenziertere Darstellung bei der Aufstellung der Pläne sowie durch eine Überprüfung des Empfängerkreises reduziert werden.

- Nicht nur wegen der datenschutzrechtlich bedenklichen Redundanz, sondern auch aus Gründen der Verwaltungsvereinfachung ist zu prüfen, wie die Vielzahl der Dateien, Karteien, Bücher und Sammelakten reduziert werden kann.

  Sie sollten durch solche Formen der Dokumentation ersetzt werden, die es ermöglichen, in regelmäßigen Abständen die Unterlagen zu archivieren und in den für den täglichen Dienstbetrieb bestimmten Papieren nur noch aktuelle Maßnahmen oder Daten zu registrieren.

- Es ist anzustreben, daß der ärztliche Bereich mit seinen Informationen über den Gesundheitszustand der Häftlinge gegenüber dem Vollzug noch weiter abgeschottet wird. Im Einzelfall sollte z. B. dem Gefangenen ermöglicht werden, daß verordnete Medikamente ihm durch ärztliches Personal und nicht durch Vollzugsbedienstete ausgehändigt werden.

- Es müssen mehr Aktenvernichter eingesetzt werden, die der einschlägigen DIN-Norm (32757, Stufe 4) entsprechen und leicht zugänglich sind.

- Es sind klare, für die verschiedenen Akten und Unterlagen differenzierte Aufbewahrungsbestimmungen zu erlassen. Eigenständige Verantwortung für die Führung der verschiedenen Archive, die Kenntnis der jeweils geltenden Aufbewahrungsbestimmungen sowie ein geordnetes Verfahren zur Vernichtung der Datenträger sind notwendig.

- In Kernbereichen personenbezogener Datenverarbeitung innerhalb der Anstalt, wie z. B. in der Vollzugsgeschäftsstelle, der Poststelle oder dem Lazarett ist der Einsatz von Gefangenen auszuschließen. Dies gilt für jedwede Arbeiten in diesen Bereichen, auch für die Reinigung. Es muß immer davon ausgegangen werden, daß einzelne Häftlinge die Gelegenheit nutzen könnten, um an amtliche Datenträger zu gelangen. Weiter ist zu berücksichtigen, daß mir von allen Befragten zu verstehen gegeben wurde, daß es jederzeit möglich sei, einzelne Schriftstücke oder auch ganze Akten in die oder aus der JVA zu bringen. Nur mit einer extrem hohen Kontrolldichte, die

weder personell leistbar noch in der Sache gerechtfertigt sei, könnte dieses Risiko eingeschränkt bzw. verhindert werden.

Daraus ergibt sich, daß nicht darauf vertraut werden kann, daß einmal entwendete Datenträger in der Anstalt schon deshalb wieder auftauchen werden, weil man sich in mit hohen Mauern umgebenen und bewachten Räumlichkeiten befindet. Vielmehr ist bei der Aktenhaltung und der Dokumentation der Verwaltungsabläufe von vornherein in Rechnung zu stellen, daß - anders als in anderen Verwaltungsbereichen - jeder Datenträger, der nicht sorgfältig verwahrt und verschlossen ist, den Weg zu unbefugten Dritten oder in die Öffentlichkeit finden kann. Wie alle in der JVA Beschäftigten beim Durchschreiten verschiedener Bereiche gewohnt sind, die Türen und Tore vor sich auf- und hinter sich abzuschließen, müßten sie es sich zur Gewohnheit werden lassen, alle Datenträger besonders gesichert aufzubewahren und innerhalb der Anstalt zu transportieren.

- Die umfangreiche Kontrollprozedur für die Besucher der Haftanstalt darf anders als bisher nicht mehr ohne deren Wissen und Einwilligung stattfinden.

- Um zu verhindern, daß im Einzelfall nicht erforderliche Daten innerhalb der Anstalt weitergegeben werden, bedarf es klarerer Geschäftsverteilungs- und Zuständigkeitsregelungen.

- Ausländische Gefangene sollten auf Wunsch die Gelegenheit erhalten, ohne Einschaltung von Mitgefangenen gleicher Nationalität bzw. Sprache als Dolmetscher mit der Anstaltsleitung, den Beratungseinrichtungen usw. zu kommunizieren.

Meinen rund 50 Seiten umfassenden Prüfbericht habe ich dem Senator für Justiz und Verfassung im Oktober 1993 zugestellt. Da einige der im Bericht aufgeführten Sicherungsmängel bzw. Rechtsverstöße gravierend waren, habe ich eine förmliche Beanstandung gegenüber dem Senator gem. § 29 BrDSG ausgesprochen.

6.1.4. Reaktionen

In Folge hat es mehrere Gespräche mit der im Justizressort zuständigen Abteilungsleitung und den Anstaltsleitern gegeben. Die Gespräche haben gezeigt, daß ein Teil der im Prüfbericht beanstandeten Datenverarbeitungsformen mit der Einführung automatisierter Datenverarbeitung korrigiert werden kann. Zur Zeit läuft in den Anstalten die erste Stufe der Inbetriebnahme, d. h. die Datenerfassung und -speicherung im System. Der Landesbeauftragte für den Datenschutz begleitet die Entwicklung und berät das Datenschutzkonzept. Eine Reihe von im Prüfbericht enthaltenen Empfehlungen und Anregungen lassen sich allerdings weder durch die geplanten Verfügungen (s. u.) noch durch die Einführung von ADIV erledigen. Hierzu ist aber der interne Meinungsaustausch zwischen Anstaltsleitern und Justizsenator noch nicht abgeschlossen. Als Reaktion auf meine Kontrollergebnisse haben der Justizsenator bzw. seine nachgeordneten Dienststellen folgende Unterlagen erarbeitet und mir zur Verfügung gestellt:

- Vorläufiges Datenschutzkonzept für ADIV

- Stellungnahme des Justizvollzugsamtes und der JVA Oslebshausen zu meinem Prüfbericht

- Entwurf des Justizsenators einer Allgemeinverfügung zur Anwendung der Vollzugsgeschäftsordnung (VGO) vom 03.11.1993, sowie

- Entwurf einer Allgemeinverfügung betreffend Aufbewahrung und Vernichtung von Akten mit personenbezogenen Daten und Auskunftserteilung über Gefangene, deren Angehörige und sonstige Kontaktpersonen, deren Vorlage an die Justizdeputation für Anfang März geplant ist.

Darüber hinaus will der Senator für Justiz und Verfassung Regelungen zur Führung der Gefangenen-Personalakten und der Hausakten in einer getrennten Geschäftsordnung erlassen.

Dem Datenschutzausschuß und der Justizdeputation wurde jeweils aktuell berichtet. Bei Redaktionsschluß dieses Berichts stand noch nicht fest, wann mit einer abschließenden Stellungnahme des Senators für Justiz und Verfassung zu meiner Beanstandung zu rechnen ist. Zwar wird ein Teil meiner Kritikpunkte und Vorschläge durch die erwähnte Allgemeinverfügung abgedeckt. Offensichtlich soll aber entgegen meinem dringenden Rat von der externen Reinigung wichtiger Funktionsräume und dem Einsatz leistungsfähigerer Shredder abgesehen werden. Ich gehe davon aus, daß sich die Justizdeputation mit der Umsetzung der weiteren erforderlichen Maßnahmen im laufenden Jahr befassen wird.

6.1.5. Gesetzesdefizite

Auch nach Umsetzung meiner konkreten Vorschläge bleibt die Situation im Strafvollzug angesichts der mangelnden rechtlichen Regelung der Datenverarbeitung weiter unbefriedigend. Das geltende Strafvollzugsgesetz bestimmt nur unzulänglich die vielfältigen Formen des Datenumgangs in den Haftanstalten. Die Vollzugsgeschäftsordnung (VGO) erscheint antiquiert; sie trägt modernen Möglichkeiten der Datenverarbeitung und entsprechenden Anforderungen der Verwaltung nicht ausreichend Rechnung. In dieser Situation fehlender bereichsspezifischer Gesetzgebung trotz verfassungsrechtlicher Gebotenheit hat sich die Datenverarbeitung im Strafvollzug auf das absolut notwendige Mindestmaß zu beschränken. Ein Ziel des Vollzugs ist es, den Gefangenen zu befähigen, künftig in sozialer Verantwortung ein Leben ohne Straftaten zu führen. Dieses Ziel der Resozialisierung muß auch Auswirkungen auf die Entscheidung haben, in welchem Umfang Informationen über die Gefangenen verarbeitet werden dürfen. Im Zweifel ist diejenige Form der Datenverarbeitung zu wählen, die dem Gefangenen die Rückkehr in die Gesellschaft erleichtert und nicht erschwert oder unmöglich macht. Daraus folgt eine restriktive Praxis der Übermittlung von Daten über Gefangene nach draußen, auch über die bloße Tatsache des Gefängnisaufenthaltes. Die Datenverarbeitung über Dritte, die im sozialen Umfeld des Gefangenen eine Rolle spielen, ist auf das unbedingt erforderliche Maß zu beschränken und so weit wie möglich mit deren Wissen und Einwilligung durchzuführen.

Auch wenn man in Rechnung stellt, daß der Entzug der Freiheit den gewichtigeren Eingriff für die Gefangenen darstellt, kann daraus nicht abgeleitet werden, daß wegen der Besonderheiten des Strafvollzugs der Verwirklichung des Rechts auf informationelle Selbstbestimmung dort von vornherein nur eine untergeordnete Bedeutung zukommt. Auch in Haftanstalten sind konsequent die allgemeinen datenschutzrechtlichen Grundsätze wie z. B. die Zweckbindung, die möglichst frühzeitige Sperrung oder Löschung zu beachten und die Maßnahmen zur Datensicherheit zu treffen.

Bereits 1991 hatte ich dem Senator für Justiz und Verfassung eine umfangreiche Stellungnahme zum Regelungsbedarf im Strafvollzugsgesetz zur Verfügung gestellt. Immer wieder habe ich gesetzliche Regelungen für diesen Bereich angemahnt (vgl. nur 7., 8. und 14. JB). Mir ist nicht bekannt, daß dies zu Initiativen auf Länderebene oder gegenüber dem Bundesminister der Justiz geführt hat. Anstatt zunächst die Datenverarbeitung im Strafvollzug präzise zu normieren und datenschutzgerecht auszugestalten sowie auf dieser Grundlage ADV einzuführen, wird hier der umgekehrte Weg gegangen. Daraus ergibt sich das Risiko, daß nach Erlaß der notwendigen gesetzlichen Regelungen für den Strafvollzug die eben eingeführte Technik später erneut angepaßt werden muß.

6.2. Automatisierte Datenverarbeitung in den Vollzugsgeschäftsstellen - Verfahren ADIV

Seit mehreren Jahren ist beabsichtigt, die Datenverarbeitung im Strafvollzug zu automatisieren (vgl. 9. JB, Ziff. 5.3.1.2). Auf Bundesebene war bereits im September 1986 eine Fachgruppe "ADV im Strafvollzug" gebildet worden. In verschiedenen Arbeitsgruppen wurden Projekte zu einzelnen Bereichen vorangetrieben. Das Land Bremen hat den

Schwerpunkt auf die Automation der Vollzugsgeschäftsstellen in den Haftanstalten gelegt. Für das Verfahren "Automatisation der Datenabläufe in den Vollzugsgeschäftsstellen (ADIV)" sind die technischen Voraussetzungen, die ich in diesem Beitrag noch näher darstelle, bereits geschaffen. Ende 1993 ist mit der Datenerfassung für ADIV begonnen worden.

Im September 1993 wurde mir auf Einladung des Justizvollzugsamtes der Stand der Einführung dieses Verfahrens dargelegt. Zu den Verfahrensteilen wurden mir anhand eines Soll-Konzeptes Erläuterungen gegeben. Die zur Anwendung kommenden Programme wurden federführend in Nordrhein-Westfalen unter Beteiligung der angeschlossenen Bundesländer erarbeitet. Der Einsatz der technisch unterstützten Datenverarbeitung am Arbeitsplatz kann zur Entlastung der Bediensteten von Routine- und Verwaltungsarbeiten einerseits sowie zur Gewinnung und zum Austausch von Informationen andererseits genutzt werden. Damit läßt sich auch der Datenfluß zwischen Vollzug und Verwaltung effektivieren, aktualisieren und auf das datenschutzrechtlich erforderliche Maß begrenzen, in dem die betroffenen Organisationseinheiten jeweils mit den auf ihre Tätigkeiten speziell zugeschnittenen Datensätzen versorgt werden. Der Einsatz zentraler Rechner im Geschäftsbereich des Justizvollzugsamtes und der angeschlossenen Justizvollzugsanstalten erfolgt in der Form, daß die Zugriffsmöglichkeiten aus dem Vollzugsbereich dem jeweiligen Zweck entsprechend ausgestaltet werden können. Nur lesende Zugriffe sollen zulässig sein; eine Verarbeitung, Fortschreibung und Änderung von Vollzugsdaten soll nur zentral im Bereich der Geschäftsstelle durchgeführt werden.

Zunächst ging ich mit dem Justizvollzugsamt davon aus, daß Nordrhein-Westfalen parallel zur Entwicklung von ADIV auch ein Datenschutzkonzept bereithalten würde. Dieses Konzept sollte auf der Grundlage der alle Bundesländer einheitlich bindenden Vorschriften erarbeitet werden. Ein solches Konzept lag aber auch Ende 1993 noch nicht einmal im Entwurf vor. Da ich darauf bestand, daß vor Inbetriebnahme des ADIV-Verfahrens ein solches Konzept zur Verfügung steht, wurde kurzfristig ein vorläufiges Datenschutzkonzept erstellt, das sich noch in der Abstimmung befindet.

Zwar verbinde ich mit der Einführung von ADIV die Hoffnung, daß die Führung einer Vielzahl von Büchern sowie die Weiterleitung einer Vielzahl von Meldungen in Papierform entfallen können (vgl. o. Ziff. 6.1.2). Doch gilt auch für dieses Automationsprojekt die prinzipielle Kritik am Gesetzgebungsdefizit im Strafvollzug (s. o. Ziff. 6.1.5).

6.3. Mitteilung von Bußgeldschuldnern an gemeinnützige Organisationen

Derzeit erfahren gemeinnützige Organisationen im Rahmen der Zuweisung von Geldauflagen aus Strafverfahren nicht nur die Höhe der Geldbuße, sondern auch den Namen des Zahlungspflichtigen, die Kontonummer und das gerichtliche Aktenzeichen. Ich sehe nach wie vor keine Notwendigkeit, die Empfänger von Geldbußen über die Identität des Schuldners zu informieren (vgl. 14. JB, Ziff. 2.3.6). Der Zahlungspflichtige könnte den fälligen Betrag an die Justizkasse bzw. Landeshauptkasse entrichten, diese wiederum könnte entweder unmittelbar oder in regelmäßigen Abständen die eingegangenen Zahlungen an die Adressaten weiterreichen.

Ich war der Auffassung, das von mir vorgeschlagene Verfahren läge auch im Interesse der Justiz, zumal es eine effektive und zeitnahe Kontrolle des Zahlungseingangs ermöglichen würde und darüber hinaus gewährleistet wäre, daß keine Spendenquittungen - mit der Möglichkeit steuerlicher Absetzbarkeit - ausgestellt würden. Anläßlich der Behandlung meines 14. Jahresberichts im Datenschutzausschuß im November 1992 berichtete ein Vertreter des Senators für Justiz und Verfassung, die Landeshauptkasse habe ein Verfahren angeboten, mit dem meinen Bedenken Rechnung getragen werden könne. Dieses Verfahren müsse noch mit der Staatsanwaltschaft und den Gerichten abgestimmt werden.

Der Justizsenator teilte dagegen Ende September 1993 mit, der Präsident des Hanseatischen Oberlandesgerichts Bremen habe erhebliche Bedenken gegen das von der Landeshauptkasse vorgeschlagene Verfahren erhoben. Es komme in der Praxis häufig vor, daß

Zahlungsbelege unvollständig ausgefüllt würden. Bei Zahlungen an die Landeshauptkasse könne außerdem bei dem Zahlungspflichtigen der Gedanke aufkommen, die Gelder seien nicht für die gerichtlich festgelegte gemeinnützige Einrichtung bestimmt. Der Generalstaatsanwalt habe gegen den Vorschlag eingewandt, daß bei der Vielzahl der als Empfänger in Betracht kommenden Einrichtungen die entsprechenden Überweisungsträger nicht bereitgehalten werden könnten. Außerdem sei die Empfängerliste der Landeshauptkasse nicht vollständig. Der Wunsch des Betroffenen, an eine bestimmte Einrichtung zu zahlen, sei zu respektieren.

Der Senator für Justiz und Verfassung hat wegen der geschilderten Bedenken geäußert, er wolle derzeit den Vorschlag der Landeshauptkasse nicht aufgreifen. Darüber hinaus sei ein Meinungsaustausch mit den Landesjustizverwaltungen über einen Vorschlag aus dem Bundesministerium der Justiz, das Überweisungsverfahren an gemeinnützige Einrichtungen in der Strafprozeßordnung (StPO) neu zu regeln, noch nicht abgeschlossen.

Diese Gegenargumente stellen vor allem den befürchteten Verwaltungsaufwand in den Vordergrund. Ich halte sie nicht für ausreichend, in das Persönlichkeitsrecht der Betroffenen derart weitgehend einzugreifen, daß ihre Identität gegenüber am Gerichts- und Bußgeldverfahren unbeteiligten Dritten ohne ihre Einwilligung offenbart wird. Das von mir bzw. der Landeshauptkasse vorgeschlagene Verfahren würde - dies vertrete ich nach wie vor - auf einfache Art und Weise den Staatsanwälten ohne Rückfragen bei gemeinnützigen Organisationen ermöglichen, ausbleibende Zahlungen bzw. die Höhe der von den Leistungspflichtigen entrichteten Beträge festzustellen. Das Thema sollte im Datenschutzausschuß noch einmal aufgegriffen werden.

7. Bildung und Wissenschaft

7.1. Forschungsprojekte in Schulen

Der Senator für Bildung und Wissenschaft unterrichtete mich über eine Reihe beabsichtigter, von ihm zum Teil schon genehmigter Forschungsvorhaben im Schulbereich. Sie dienten u. a. der Erforschung der Lesegewohnheiten von Schülerinnen der Klassen 5 bis 7, der "Gefühle Jugendlicher in Ost und West", der "Hoffnungslosigkeit, Depressivität und Ambiguitätstoleranz sowie von Verhaltensstörungen, Ängsten und Depressionen Jugendlicher", bestehender Gefährdungen im Hinblick auf den Umgang mit Rauschmitteln sowie des "sexuellen Mißbrauchs von Schülerinnen und Schülern". Mehrere Projekte betrafen sehr intime Lebensbereiche von auch minderjährigen Schülerinnen und Schülern. Verantwortlich für die Durchführung waren häufig Studentinnen und Studenten bremischer Hochschulen, die im Rahmen ihrer Diplomarbeiten derartige Vorhaben betrieben. Die Daten wurden in der Regel mittels eines in der Schule verteilten Fragebogens erhoben.

Für die Anwendung des einschlägigen § 13 des Gesetzes zum Datenschutz im Schulwesen (BremSchDSG) entscheidend ist die Frage, ob bei der Erhebung von den Betroffenen Angaben erfragt werden, mit denen ihre Identifizierung auch nach Ende ihrer Befragung möglich bleibt, sei es direkt durch die Angabe der Personalien, sei es indirekt aufgrund der geringen Klassengröße, der differenzierten Fragestellung o. ä.

Bei den erwähnten Befragungen wurde wiederholt übersehen, daß § 13 BremSchDSG ausgeht vom Grundsatz der Einwilligung der Schülerinnen und Schüler bzw. deren Erziehungsberechtigter in die Erhebung, Speicherung und Auswertung der von den Forschern gewünschten Daten. Ausnahmen nach § 13 Abs. 3 BremSchDSG bedürfen ausdrücklicher Begründung. In den mir zur Kenntnis übersandten Erhebungsunterlagen fehlten nicht selten Hinweise auf das Einwilligungserfordernis sowie auf die Freiwilligkeit der Auskunftserteilung. In mehreren Fällen wurde nicht ausreichend über den Zweck der Erhebung durch eine präzise Erläuterung des Forschungsvorhabens informiert. Die sich aus § 3 Abs. 2 BrDSG ergebenden formalen Anforderungen an die Einwilligung, vor allem die Schriftlichkeit, blieben mehrmals unberücksichtigt.

Nach § 13 Abs. 4 BremSchDSG haben im Schulbereich tätige Forscher bzw. forschende Stellen zu beachten, daß, sobald der Forschungszweck dies erlaubt, personenbeziehbare Merkmale gesondert zu speichern sind, d. h. eine möglichst frühzeitige Anonymisierung der Daten erfolgen muß. Auswertungen haben danach nur noch aus den nicht-personenbezogenen Datenbeständen zu erfolgen. Auf die personenbezogenen Angaben darf dann nur noch im Bedarfsfall und von ausdrücklich dazu ermächtigten Projektmitarbeitern zugegriffen werden. Sie sind spätestens dann zu löschen, wenn das Forschungsvorhaben beendet ist. Auch diese Vorkehrungen waren bei mehreren Vorhaben nicht gewährleistet bzw. in der Projektbeschreibung nicht enthalten.

Ich habe den Senator für Bildung und Wissenschaft jeweils auf die von mir festgestellten Mängel hingewiesen, um deren Beseitigung gebeten und Datensicherungsmaßnahmen empfohlen. Dies war in den Fällen nicht mehr möglich, in denen ich entgegen § 13 Abs. 6 BremSchDSG nicht rechtzeitig, d. h. vor Beginn des Vorhabens, unterrichtet worden war. Um künftig datenschutzrechtliche Defizite zu vermeiden, habe ich ein Merkblatt zu Forschungsprojekten im Schulbereich entwickelt. Es geht in Kürze dem Senator für Bildung und Wissenschaft zu und soll ihm als "Checkliste" für die Prüfung angemeldeter Erhebungen dienen.

8. Gesundheit, Jugend und Soziales

8.1. Der "Leistungsmißbrauch" und seine Kontrolle - wie ein Grundrecht ausgehöhlt wird

8.1.1. Die Folgen des "Solidarpakts"

In ihrem Entwurf für ein Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms (FKPG), auch Solidarpakt genannt, vom 25.04.1993 stellte die Bundesregierung in Aussicht, auf die darin vorgesehenen Senkungen der Lohnersatzleistungen nach dem Arbeitsförderungsgesetz zu verzichten, wenn rechtzeitig vor Abschluß des Gesetzgebungsverfahrens der Nachweis erbracht werde, daß durch Einführung von Meldepflichten für Arbeitslose und weitere Intensivierung der Bekämpfung von Mißbrauch und Leistungsmitnahme ein entsprechendes Einsparvolumen erbracht werde. Mir ist nicht bekannt, ob die hier in Aussicht gestellte Rechnung je aufgemacht wurde. Jedenfalls wurden inzwischen beide Alternativen realisiert: Das zum 01.07.1993 in Kraft getretene FKPG und die beiden folgenden Gesetze zur Umsetzung des Spar-, Konsolidierungs- und Wachstumsprogramms (1. und 2. SKWPG) kürzen Lohnersatzleistungen und Sozialhilfe, zugleich aber sollen deren Empfänger in einem bisher nicht gekannten Maße durch Datenabgleiche kontrolliert werden.

Schon deshalb erwies sich die Alternative, sich entweder für Einsparungen zu entscheiden, die die "ehrlichen" Leistungsempfänger treffen oder für Kontrollen, die die "unehrlichen" Doppelbezieher oder "Absahner" treffen, die in der Öffentlichkeit und in den parlamentarischen Gremien wirksam verkauft wurden, als bloßer Schein. Außerdem heißt Mißbrauchskontrolle, wie sie in diesen Gesetzen verstanden wird, Kontrolle aller Leistungsempfänger, also auch der "Ehrlichen" unter ihnen. Nicht um Einzelprüfung auf begründeten Verdacht hin geht es, sondern um "Rasterfahndung" in Form des Abgleichs der Daten, die unterschiedliche Stellen zwecks Erfüllung ihrer unterschiedlichen Aufgaben über Leistungsempfänger oder Klienten gesammelt haben.

Als mich jüngst ein Bürger anrief und mir die Frage stellte, ob denn die Behörden untereinander alle über ihn gespeicherten Daten austauschen dürften, mußte ich ihm sagen: "Im Prinzip nein, aber...". Zwar gilt weiterhin prinzipiell der Grundsatz der Zweckbindung. Das Bundesverfassungsgericht hat dies in seinem Volkszählungsurteil dem Gesetzgeber unmißverständlich mit den Worten vorgegeben: "Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt. Schon angesichts der Gefahren der automatischen Datenverarbeitung ist ein "amtshilfefester" Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote erforderlich." Gerade umgekehrt aber sieht es der

Gesetzgeber des Jahres 1993: Mittels automatisierter Datenabgleiche wird die Zweckbindung nach und nach aufgehoben.

8.1.2. Datenabgleich in der Sozialhilfe - der neue § 117 BSHG

Ein Beispiel, das auch die kommunalen Sozialhilfeträger im Lande Bremen unmittelbar betrifft, enthält der neue § 117 des Bundessozialhilfegesetzes (BSHG). Zwar wurde der ursprüngliche Entwurf nicht Gesetz, der die Träger der Sozialhilfe pauschal berechtigen sollte, Hilfeempfänger regelmäßig darauf zu überprüfen, inwieweit sie auch Leistungen der Arbeitslosenunterstützung oder der gesetzlichen Rentenversicherung beziehen. Es gelang aber auch nicht, die Datenabgleiche auf ein verfassungsrechtlich unbedenkliches Maß, d. h. auf konkrete Verdachtsfälle, zu reduzieren, obwohl der Bundesrat auf Initiative Bremens, Hamburgs und Hessens einen entsprechenden Beschluß faßte. Vielmehr sollen nach Erlaß einer Durchführungsverordnung und Schaffung einer aufwendigen zentralisierten technischen Infrastruktur über zentrale Vermittlungsstellen (Kopfstellen) alle Sozialhilfeempfänger im Wege automatisierter Datenabgleiche kontrolliert werden können, inwieweit sie Leistungen bei mehreren Sozialhilfeträgern, zusätzlich bei Arbeitsämtern oder bei Trägern der Unfall- bzw. Rentenversicherung bezogen haben.

In seinem dritten Absatz berechtigt § 117 BSHG nunmehr die Träger der Sozialhilfe - also vor allem die Kommunen - dazu, eine Reihe von Daten von Sozialhilfeempfängern bei anderen öffentlichen und nicht-öffentlichen Stellen ihrer Verwaltung abzurufen. Diese Stellen ihrerseits sind verpflichtet, die gewünschten Daten zur Verfügung zu stellen. Am interessantesten dürfte dabei die Anfrage bei der Kfz.-Zulassungsstelle sein, ob ein Hilfeempfänger Halter eines Kfz ist. Es ist bezeichnend, daß einzelne Großstädte (das Beispiel Aachen ging kürzlich durch die Presse) bereits versuchten, dies im Wege automatisierter Datenabgleiche umzusetzen. Demgegenüber ist festzuhalten, daß § 117 Abs. 3 BSHG - anders als es in den Absätzen 1 und 2 geregelt ist - lediglich Einzelanfragen gestattet. Erfreulicherweise sind es nicht nur Datenschutzbeauftragte, sondern auch Fachaufsichtsbehörden, die diese Auffassung vertreten - und durchsetzen, wie der Fall Aachen zeigt, wo der Abgleich abgeblasen wurde.

Ich habe dem Senator für Gesundheit, Jugend und Soziales meine Auffassung mitgeteilt und gebeten, diese in seiner noch ausstehenden Verwaltungsanweisung zu § 117 Abs. 3 BSHG zu berücksichtigen.

Derartige Abgleiche und Anfragen, gleich ob automatisiert oder nicht, schränken die Transparenz des Verwaltungsgeschehens für den einzelnen Betroffenen ein: Die Verwaltung ist nicht mehr auf ihn als "Datenlieferanten" angewiesen, die Sachbearbeiter/-innen geraten in Versuchung, sich nicht mehr mit ihren Klienten auseinanderzusetzen, sondern von vornherein auf andere Datenquellen zurückzugreifen. Dies widerspricht eindeutig den bisherigen Regelungen in § 60 SGB I, § 13 BDSG und § 10 BrDSG, die die Verwaltung grundsätzlich verpflichten, personenbezogene Daten nur beim Betroffenen mit seiner Kenntnis zu erheben.

Zumindest erwarte ich von den Sozialhilfeträgern im Lande Bremen, daß

- sie vor der Verwertung des Ergebnisses eines automatisierten Datenabgleichs nach § 117 Abs. 1, 2 BSHG zu seinen Lasten den Betroffenen dazu anhören, § 24 SGB X,

- sie vor einer Einzelanfrage bei einer anderen Stelle nach § 117 Abs. 3 BSHG dem Betroffenen Gelegenheit geben, selbst die gewünschte Auskunft zu erteilen, § 60 SGB I, § 13 BDSG, § 10 BrDSG.

Ich habe den Senator für Gesundheit, Jugend und Soziales angeschrieben und gebeten, mich am Zustimmungsverfahren im Bundesrat zu den Rechtsverordnungen und an den technischen Vorbereitungen für die Durchführung der automatisierten Datenabgleiche sowie an der Erarbeitung von Dienstanweisungen zu beteiligen. Angesichts der kritischen

Haltung, die er in Abstimmung mit mir in den Ausschüssen des Bundesrats eingenommen hat, gehe ich davon aus, daß er für eine strikte Beachtung des Gesetzeswortlauts und damit für eine Eingrenzung der Datenabgleiche Sorge tragen wird.

8.2. Neuregelung des Sozialgeheimnisses - Abschied von der Zweckbindung

8.2.1. Die neue Einheit der (Sozial)-Verwaltung im 2. SGB-Änderungsgesetz

Unabhängig von der Mißbrauchskontrolle (vgl. Ziffer 8.1) beobachte ich mit Sorge die Tendenz in der Gesetzgebung, Transparenz und Zweckbindung bei der Erhebung, Nutzung und Übermittlung von Sozialdaten einzuschränken. Im Vorblatt zum Entwurf der Bundesregierung zum 2. SGB-Änderungsgesetz (2. SGBÄndG), das im Januar 1994 den Bundestag passiert hat, werden zwar als Inhalte die Verstärkung der Zweckbindung bei der Verarbeitung und Nutzung von Sozialdaten sowie der Rechte der Betroffenen angekündigt. Das Gegenteil aber war Inhalt des Entwurfs und ist Gegenstand des Gesetzesbeschlusses geworden. Gegen den Widerstand von Vertretern von Datenschutzbeauftragten und Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich sowie der Opposition im Bundestag (vgl. den Änderungsantrag der SPD-Fraktion vom 01.12.1993) ist ein Gesetz verabschiedet worden, das im Interesse der großen Sozialversicherungsträger wie Rentenversicherungsanstalten, Bundesanstalt für Arbeit, Krankenkassen und Berufsgenossenschaften einen weitgehend ungehinderten Austausch von Sozialdaten untereinander erlaubt. Dies wird beschönigend so ausgedrückt: "Zweckänderungen unter dem Dach des Sozialgeheimnisses müssen ermöglicht werden, weil insoweit ein Bedürfnis in der Verwaltungspraxis besteht" (Gegenäußerung der Bundesregierung zur Stellungnahme des Bundesrates, Bundestags-Drucks. 12/5187 vom 18.06.1993, S. 64).

Das heißt im Klartext: Die Sozialleistungsträger brauchen untereinander das Sozialgeheimnis nicht zu wahren, weil sie ohnehin alle dem Sozialgeheimnis verpflichtet sind und es so schön praktisch ist. Die von der Bundesregierung dem Gesetzgebungsvorhaben vorangestellten grundrechts- und bürgerfreundlichen Ziele spielen hier keine Rolle mehr. Unabhängig von den neuen Möglichkeiten der Mißbrauchskontrolle muß ein Bürger, der einem Sozialleistungsträger in einem bestimmten Sachzusammenhang eine Tatsache mitteilt, gewärtig sein, daß ihm jederzeit ein anderer Träger diese Tatsache in einem ganz anderen Zusammenhang entgegenhalten kann.

Angesichts der enormen Größe und Ausdehnung des sozialen Sektors und der Heterogenität seiner Aufgaben erscheint es absurd, daß gerade im Bereich der Sozialverwaltung der Bürger mit der verfassungsrechtlich obsoleten "Einheit des Staates" konfrontiert wird. Oder sollte - gerechtfertigt durch die Zauberworte "Bedürfnisse der Praxis" und "Mißbrauchskontrolle" und ermöglicht durch die Automatisierung der Datenverarbeitung - die obrigkeitliche Staatsauffassung wieder an Boden gewinnen? Man darf gespannt darauf sein, ob, wann und wie das Bundesverfassungsgericht, das vor 10 Jahren in seinem Volkszählungsurteil in diesem Zusammenhang deutliche Worte gefunden und diese inzwischen mehrmals bestätigt hat, hierauf reagieren wird.

8.2.2. Sozialbehörden als Fahndungshelfer?

Im zweiten Durchgang des Gesetzentwurfs im Bundesrat versuchten einige Landesregierungen, das Sozialgeheimnis noch weiter auszuhöhlen. So sollten etwa nach einem der Länderanträge die Sozialbehörden der Polizei und den Staatsschutzbehörden auf Anfrage außer dem Wohnsitz auch den "tatsächlichen Aufenthalt" von Klienten mitteilen und damit ggf. auch, daß der Gesuchte sich gerade in der Dienststelle aufhält. Denkbar wäre es dann auch etwa, den Sozialämtern Listen von gesuchten Personen mitzuteilen, deren Besuch im Amt sofort gemeldet werden soll. Der Sozialhilfesachbearbeiter als Hilfsperson von Polizei und Nachrichtendienst, der erste Blick in Fahndungslisten bei Klientenbesuch oder das Sozialamt als "Polizeifalle" - erschreckende Vorstellungen.

Ein anderer Antrag ging dahin, der Polizei zur Bekämpfung von Schwarzarbeit den automatisierten Direktabruf von Klientendaten der Arbeitsämter zu erlauben. Beide Anträge

wurden damit legitimiert, daß man ja nur Rechtsbrecher fangen und Mißbrauch verhindern wolle. Man ließ völlig außer Acht, daß damit alle Sozialleistungsempfänger in ihrem Persönlichkeitsrecht betroffen würden und das Sozialgeheimnis geradezu in sein Gegenteil verkehrt würde: Wer auf Sozialleistungen angewiesen ist, muß auf Datenschutz verzichten - nicht nur, wie oben kritisiert gegenüber allen Sozialleistungsträgern (vgl. Ziffer 8.2.1), sondern auch gegenüber Polizei und Staatsschutz.

Der Bundesrat hat es glücklicherweise abgelehnt, zu diesen Anträgen den Vermittlungsausschuß anzurufen. Erleichterung stellt sich dennoch nur zaghaft ein, zu groß ist das Erschrecken darüber, daß derartigen Anträgen überhaupt Aussicht auf Erfolg zugesprochen wird. Immerhin war der erste Antrag im Innenausschuß des Bundesrates angenommen, der zweite nur bei Stimmengleichheit abgelehnt worden.

Dagegen hat der Bundesrat den Vermittlungsausschuß mit dem Ziel der Änderung des Gesetzbeschlusses des Bundestages in vier anderen Punkten angerufen. Auch mit diesen Anträgen versuchen die Länder, weitere Hindernisse für den freien Datenaustausch der Sozialleistungsträger untereinander beiseite zu räumen. Auch Bremen hat zugestimmt, obwohl ich die zuständigen Senatoren angeschrieben und um Ablehnung gebeten hatte. Der Vermittlungsausschuß selbst ist erst nach Redaktionsschluß zusammengetreten.

8.3. Gesundheitsdatenschutz in der Gesetzlichen Krankenversicherung

8.3.1. Chipkarten für "gläserne Patienten"

8.3.1.1. Rechtslage und Sachstand

Im 15. Jahresbericht (Ziff. 10.3) hatte ich Gefährdungen dargestellt, denen der Patientendatenschutz bzw. die ärztliche Schweigepflicht durch neue Abrechnungsverfahren, Gesetze und technische Entwicklungen in der gesetzlichen Krankenversicherung ausgesetzt sind. Inzwischen ist die Entwicklung zügig vorangeschritten - nicht zum Vorteil der Patientenrechte. Immerhin scheint die von mir seinerzeit als erforderlich bezeichnete Diskussion in der demokratischen Öffentlichkeit in Gang zu kommen. Ich habe sie u.a. dadurch anzuregen versucht, daß ich zusammen mit dem Institut für Informations- und Kommunikationsökologie (IKÖ) und dem Bremer Gesundheitsladen im Oktober 1993 eine Fachtagung zu dem Thema "Computerisierte Medizin - wo bleiben die PatientInnen?" veranstaltete. Teilnehmerinteresse, Verlauf und Medienecho waren ermutigend. Inzwischen ist auch in der Fachpresse, auf Kongressen aller Art, aber auch in politischen Printmedien die Debatte in Gang gekommen.

§ 291 SGB V i. d. F. des Gesundheitsstrukturgesetzes 93 ordnet an, daß spätestens bis zum 01.01.1995 die gesetzlichen Krankenkassen jedem Versicherten anstelle der Krankenscheine eine Krankenversichertenkarte austellen. Sie darf nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen der ärztlichen Versorgung sowie zur Abrechnung mit Leistungserbringern verwendet werden, und nur die hierfür erforderlichen Daten (im wesentlichen die Krankenkasse, die Identifikationsdaten des Versicherten einschließlich Krankenversichertennummer, Versichertenstatus, Beginn und ggf. Ende des Versichertenverhältnisses) dürfen auf ihr gespeichert werden.

Die Spitzenverbände der Krankenkassen und Ärzte haben sich für die Einführung der Krankenversichertenkarte als Chipkarte entschieden und die hierfür gesetzlich vorgesehenen vertraglichen Vereinbarungen getroffen. Die Karte wurde im April 1993 in einigen Modellregionen eingeführt; im Lande Bremen wird sie im dritten Quartal 1994 an die Versicherten ausgegeben werden. Stichtag soll der 01. Oktober 1994 sein.

Damit die gesetzlichen Vorgaben eingehalten werden, ist zu gewährleisten, daß

- die Speicherkapazität der Chipkarten selbst auf die gesetzlich zugelassenen Daten begrenzt wird,

- die bei den Beteiligten zu installierenden Lesegeräte nur die gesetzlich zugelassenen Daten lesen können und

- nur die Kassen, nicht aber z. B. die Ärzte, Daten auf der Chipkarte speichern können.

Andernfalls wäre zu befürchten, daß an dem Verfahren Beteiligte, etwa Ärzte oder Kassen, doch die technisch vielfältigen neuen, aber unzulässigen Möglichkeiten ausschöpfen.

Der Bundesbeauftragte für den Datenschutz versucht, in Verhandlungen mit den Spitzenverbänden die Umsetzung dieser Forderungen zu erreichen. Ich werde die Einführung der Krankenversichertenkarte im Lande Bremen und die Installation der damit verbundenen technischen Einrichtungen im Rahmen meiner Zuständigkeiten kritisch begleiten.

8.3.1.2. Weitergehende Interessen - Verlautbarungen und Hintergründe

Die Befürchtung, daß mit der Karte der "gläserne Patient" geschaffen werde, wird von seiten der Krankenkassen und Kassenärztlichen Vereinigungen immer wieder als gegenstandslos bezeichnet (vgl. etwa "Kurier am Sonntag" vom 22.08.1993). Man verweist dann regelmäßig darauf, daß auf der Karte nur die gesetzlich zugelassenen Daten gespeichert werden dürften. Mit der Karte werde der Startschuß für den Beginn einer rationelleren Abwicklung des Verwaltungsaufwandes bei den Kassen und Ärzten gegeben. Von seiten der Kassenärztlichen Vereinigung Hessen ist allerdings jüngst der in Aussicht gestellte Rationalisierungs- und Spareffekt der Einführung der Karte in Frage gestellt worden. Der Arzt habe keine Vorteile davon, sondern nur zusätzliche Kosten ("Weser-Kurier" vom 26.01.1994).

In der Fachpresse und auf Fachkongressen dagegen ist ganz anderes zu lesen und zu hören. Die Chipkarte wird als Durchbruch einer innovativen Technik gepriesen, sie werde einen neuen Kreislauf des Austauschs medizinischer Daten im Gesundheitswesen in Gang setzen. Die Rede ist von der Smart-Card, der intelligenten Karte mit Prozessor-Chip zwecks multifunktionaler Anwendung. Dem Bundesbeauftragten für den Datenschutz wird vorgeworfen, mit seiner Forderung nach funktionalen Restriktionen bei Lesegeräten zwecks Einhaltung der gesetzlichen Vorgaben die Entwicklung in eine Sackgasse führen zu wollen. Von dadurch später ggf. erforderlich werdenden Neuinvestitionen in Höhe von mehreren hundert Millionen DM ist die Rede.

Es wird in Aussicht gestellt, daß der Mensch mit Hilfe der neuen intelligenten Kartentechnik unabhängig von übergeordneten Informationssystemen werde. Er werde seine Gesundheitsdaten bei sich tragen und sie so nutzen, wie er es für richtig halte. Von Demokratie, informationeller Selbstbestimmung und Selbstverwirklichung ist die Rede. Die multifunktionale Gesundheitskarte werde verschiedene selbständige Module aufweisen. Der Zugang zu den Modulen, d. h. Eingabe und Lesen von Daten, könne je nach Art und Zweckbindung der gespeicherten Daten differenziert geregelt werden.

8.3.1.3. Automatisierter Datenfluß - Risiken der Versichertenkarte

Die Ärzte zeichnen zwecks Abrechnung und weiterer Behandlung die Gesundheitsdaten auf und speichern sie in ihrer Patientenkartei, z. T. bereits in automatisierter Form. Zwecks Abrechnung müssen die Diagnosen patientenbezogen an die Kassenärztliche Vereinigung, von dieser dann lediglich fallbezogen, aber nicht versichertenbezogen, an die Kassen übermittelt werden, § 295 Abs. 1, 2 SGB V. Diese Einschränkung hatte der Gesetzgeber im letzten Augenblick auf das gemeinsame Betreiben des Bundesbeauftragten für den Datenschutz und von mir in das Gesundheitsstrukturgesetz 1993 aufgenommen. Zwar sollen - nach dem mir zuletzt bekannten Stand der Verhandlungen über einen "Vertrag über den Datenaustausch auf Datenträgern" zwischen Ärzten, Kassenärztlichen Vereinigungen und Krankenkassen - letztere zwecks Prüfung ihrer Leistungspflicht gegenüber dem jeweiligen Versicherten auch personenbezogene Daten erhalten. Diese Daten sollten aber nicht mit den Abrechnungsdaten, die eben auch Gesundheitsdaten enthalten,

zusammengeführt werden dürfen. Ich habe mich dafür verwandt, dies zumindest durch ein striktes Zweckbindungsgebot für die versichertenbezogenen Daten zu ergänzen. Jedenfalls dürfte nach gegenwärtigem Recht die Kasse auf der Krankenversichertenkarte gespeicherte Gesundheitsdaten ihrer Versicherten nicht so ohne weiteres zur Kenntnis nehmen. Und dies mit gutem Recht:

- Zur inhaltlichen Überprüfung des Einzelfalls ist ggf. der Medizinische Dienst der Krankenkassen zuständig, nicht die Kasse selbst, § 275 SGB V.

- Für versichertenbezogene Prüfungen gibt es in §§ 106, 297 SGB V eigene enge Regelungen, die sich auf Stichproben beschränken.

Werden auf den Krankenversichertenkarten Gesundheitsdaten der Versicherten gespeichert, erhalten die Krankenkassen die technische Möglichkeit, genau das zu realisieren, was sie nach ihren eigenen Beteuerungen nicht wollen und auch nicht dürfen. Und damit würden sie dann lediglich das technische Potential der Chipkarte realisieren. Die Kassen könnten die Gesundheitsdaten ihrer Versicherten jederzeit abrufen und auswerten, für sie existierte der "Gläserne Patient" tatsächlich. Es wäre z. B. möglich, die Entscheidung, ob die Kosten einer teuren Therapie übernommen werden, vom Ausgang der Überprüfung abhängig zu machen, ob nach den vorliegenden Gesundheitsdaten die Behandlung hinreichend Aussicht auf Erfolg verspricht (Kosten-Nutzen-Analyse). Ganz neue Möglichkeiten der Kostendämpfung und der Kontrolle des Gesundheitsverhaltens der einzelnen Versicherten eröffneten sich. Alten, chronisch kranken, behinderten oder "unvernünftigen" Versicherten könnten kostspielige Behandlungen vorenthalten werden, es sei denn, sie trügen die Kosten aus eigener Tasche.

Und dies ist nur eine Möglichkeit. Auch Begehrlichkeiten von anderer Seite, etwa von Lebensversicherungen oder von Arbeitgebern wird die Gesundheitskarte wecken. Die Zusicherung, Gesundheitsdaten nur mit Einwilligung des Betroffenen auf der Karte zu speichern, erweist sich bei näherem Hinsehen als wertlos. Ganz abgesehen davon, daß der Wegfall dieser Hürde nur eine Frage der Zeit sein dürfte, wird eine intensive Öffentlichkeitsarbeit der Kassen den Betroffenen schmackhaft machen, daß ihre Gesundheitsdaten auf die Karte gehören. Die Freiheitssphäre, die die Gesundheitskarte dem Einzelnen angeblich eröffnen soll, wird eher eine Sphäre der Begehrlichkeiten von seiten vieler Institutionen sein. Bedenkt man dies, so sind die medizinischen Patientendaten in der Kartei des behandelnden Arztes, vorausgesetzt er nimmt seine Schweigepflicht ernst, doch sicherer.

8.3.2. Kontrolle einer "Randgruppe": NUB-Richtlinie und Methadon-Substitution

8.3.2.1. Reaktionen auf meine Initiative

Immer noch müssen die Ärzte, die Drogenabhängigen Methadon verabreichen, unabhängig vom normalen Abrechnungsverfahren dies der Kassenärztlichen Vereinigung und der Krankenkasse melden. Ich bemängele nach wie vor, daß es hierfür an der gesetzlichen Grundlage fehlt (vgl. die ausführliche Darstellung im 15. JB, Ziff. 10.3.1). Dem Bundesbeauftragten für den Datenschutz gegenüber, der sich meiner Auffassung angeschlossen hatte, hat der zuständige Bundesausschuß der Ärzte und Krankenkassen die Notwendigkeit der Meldung damit begründet, daß sie der Einhaltung der Höchstgrenze der Anzahl substituierter Patienten beim einzelnen Arzt, der Sicherstellung der psychosozialen Begleitbetreuung und der sicheren Vermeidung der mehrfachen Substitution ein und desselben Versicherten mit Methadon diene.

Meiner Forderung, sich wenigstens auf die Meldung an die Kassenärztliche Vereinigung zu beschränken - eine Prüfung durch zwei Stellen sei doch wohl nicht nötig - wurde damit begegnet, nur die Kassen könnten zuverlässig verhindern, daß einzelne Substituierte sich bei Ärzten aus mehreren Bundesländern Methadon verschaffen. Merkwürdig ist, daß für die AOK Bremen/Bremerhaven, bei der ich die Verarbeitung von Daten Methadon-Substi-

tuierter überprüfte, dieser Zweck der Meldung überhaupt keine praktische Bedeutung hat: Man nutzte die Meldungen zu denselben Zwecken wie die Kassenärztliche Vereinigung, vor allem aber dazu, festzustellen, ob der oder die Betreffende Mitglied der AOK ist. Letzteres aber, so sieht es das Gesetz vor, wird bei den durch Vertragsärzte erbrachten Leistungen erst bei der Abrechnung überprüft. Warum dies bei der Methadon-Substitution nicht ausreicht, ist mir bislang nicht dargelegt worden.

Ich habe meine Feststellungen und Bedenken dem Bundesbeauftragten für den Datenschutz und dem Senator für Arbeit und Frauen, letzterem in seiner Eigenschaft als Rechtsaufsichtsbehörde über die AOK Bremen/Bremerhaven und die Kassenärztliche Vereinigung Bremen, mitgeteilt in der Hoffnung, daß sie sich für eine Abschaffung der Meldung an die Kassen und für eine strikte Zweckbindung der Verarbeitung der Daten Methadon-Substituierter bei der Kassenärztlichen Vereinigung einsetzen.

Der Senator für Arbeit und Frauen hat inzwischen dem Datenschutzausschuß der Bremischen Bürgerschaft, der ihm gegenüber ebenfalls Bedenken geäußert hatte, mitgeteilt, er habe diese an den Bundesminister für Gesundheit herangetragen. Er wolle die Ergebnisse von dessen Beratungen mit den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung und die meiner Prüfung abwarten, bevor er entscheide, ob er als Aufsichtsbehörde tätig werde.

8.3.2.2. Neues Meldeverfahren mit Einwilligung

Nach Informationen des Bundesbeauftragten für den Datenschutz hat man sich inzwischen auf Bundesebene auf folgendes Verfahren geeinigt: Die Ärzte müssen weiterhin sowohl an Kassen und Kassenärztliche Vereinigungen melden, die Kassen sollen aber nur noch die Daten erhalten, die sie benötigen, um die Mehrfachsubstitution zu überprüfen. Dies und eine enge Zweckbindung beim Umgang mit den gemeldeten Daten wiederum sollen nicht in der einschlägigen Richtlinie der Spitzenverbände selbst, sondern in dem dieser als Anlage beigefügten Vordruck einer Einwilligungserklärung der Substituierten festgelegt werden. Obwohl rechtlich bedenklich ist, eine Schweigepflichtentbindung mit diesen Klauseln zu befrachten, obwohl die Notwendigkeit der Anzeigen an die Kassen und die Rechtsgrundlage für das gesamte Meldeverfahren nach wie vor zweifelhaft sind, wäre damit doch eine gewisse Verbesserung erreicht. Hinzu kommt, daß jetzt auch die Kassenärztliche Vereinigung Bremen mir zugesichert hat, den Postgang und die Löschung der bei ihr eingegangenen Meldungen datenschutzgerecht zu handhaben. Es bleibt vor allem abzuwarten, ob die AOK Bremen/Bremerhaven ihr Verfahren an die zu erwartenden Vorgaben ihres Spitzenverbandes und an meine Anforderungen anpaßt.

Kritisch ist anzumerken, daß es erst hartnäckiger Fragen, Prüfungen und Verhandlungen von seiten mehrerer Datenschutzbeauftragter und des Datenschutzausschusses der Bremischen Bürgerschaft bedurfte, um in kleinen Schritten ein etwas datenschutzgerechteres Verfahren bei der Methadon-Substitution zu erzwingen - ein Lehrbeispiel über dieses spezielle Verfahren hinaus dafür, wie schwierig es geworden ist, auch nur minimale Forderungen zum Schutz der Persönlichkeitsrechte Betroffener durchzusetzen.

8.3.3. Der Abrechnungsschein des ärztlichen Notfalldienstes im Krankenhaus

Im 15. Jahresbericht (Ziff. 10.3.1) hatte ich davon berichtet, daß für die Abrechnung des ärztlichen Notfalldienstes in den Krankenhäusern ein Formular benutzt wird, dessen für die Krankenkassen bestimmter Durchschlag identisch mit den für den nachbehandelnden Arzt und den Verbleib im Krankenhaus bestimmten Durchschlägen ist. Auf diese Weise erhalten die Kassen über das gesetzlich vorgesehene Maß hinaus Kenntnis von Patientendaten, die sie für die Honorarabrechnung nicht benötigen (z. B. Daten zum Unfallhergang und zur Therapie).

Ich habe deshalb im Oktober 1992 von der AOK Bremen/Bremerhaven und den anderen zuständigen Stellen im Lande Bremen verlangt, das Formular zu ändern. Mein Vorschlag

war, auf dem für die Kassen bestimmten Durchschlag nur die für sie bestimmten Daten vorzugeben.

Zunächst berief sich die AOK auf die bundeseinheitlich zwischen den Spitzenverbänden der gesetzlichen Krankenkassen und der Kassenärztlichen Bundesvereinigung auf der Grundlage von § 28 des Bundesmantelvertrags Ärzte bzw. § 82 Abs. 1 SGB V abgeschlossene "Vordruckvereinbarung", die in der Tat die bemängelten Formulare vorsah.

In ihrer Sitzung im Januar 1993 erkannte aber die "Formularkommission" der genannten Verbände meine Einwände an. Inzwischen ist ein neuer Vordruck herausgegeben worden, auf dessen für die Kassen bestimmten Durchdruck die Felder der nur für die Ärzte bestimmten Daten geschwärzt sind. Der Vordruck soll im Lande Bremen zeitgleich mit der Krankenversicherungskarte zum 01.10.1994 eingeführt werden.

8.4. Gesundheitsdatenschutz im Krankenhaus

8.4.1. Kontrollergebnisse in kommunalen Krankenhäusern

Exemplarische Prüfungen in der automatisierten Datenverarbeitung (ADV) in den drei kommunalen Krankenhäusern im Lande Bremen zeigten, daß sich sehr verschiedene DV-Landschaften mit entsprechend unterschiedlichen Datenschutzproblematiken entwickelt haben.

Ein sich aus der Struktur der modernen EDV ergebendes Problem haben allerdings alle: die nur schwer zu kontrollierende Allmacht der Systemverwaltung.

Die Darstellung auch technischer Einzelheiten fällt in diesem Bereich deshalb so ausführlich aus, weil die in den Krankenhäusern festgestellten konzeptionellen Schwierigkeiten und Sicherheitsmängel prototypisch für viele andere datenverarbeitende Stellen in Bremen sind. Die für die Krankenhäuser gemachten Verbesserungsvorschläge gelten dann dort entsprechend.

8.4.1.1. ZKH-Reinkenheide - Überholte EDV-Technik und Datenschutz

Von den Datenschutzmaßnahmen, die ich nach einem Prüfbesuch (vgl. 15. JB Ziff. 10.1.3) verlangt hatte, ist lediglich die bessere Sicherung des EDV-Raumes durch Austausch der Schließzylinder realisiert worden.

Sämtliche anderen festgestellten Mängel konnten bisher angesichts der veralteten Technologie der EDV-Anlage nicht behoben werden.

Diese soll Mitte 1994 gegen eine neue Anlage ausgetauscht werden, die auf der Basis eines Unix-Systems arbeiten wird.

Ich erwarte, daß dann die erforderlichen Datenschutzmaßnahmen einschließlich der komplexen Anforderungen an die Fernwartung (vgl. 15. JB, Ziff. 2.2.2) realisiert werden.

8.4.1.2. ZKH-Bremen-Nord - EDV-Netz und zentrale Verfügbarkeit über Patientendaten

Das ZKH Bremen-Nord arbeitete zum Prüfungszeitpunkt (Juni 1993) mit einem Novellnetz (Arcnet, Vers. 3.11).

Dort habe ich stichprobenhaft die möglichen Zugriffe auf Daten und Programme einer Person mit Systemverwalterrechten insbesondere in bezug auf eine Datei mit medizinischen Daten festgestellt.

Die gem. § 6 BrDSG erforderlichen technischen und organisatorischen Maßnahmen wurden ergriffen

1. durch weitgehende Ausnutzung und Kombination der Sicherheitskomponenten des Novell-Betriebssystems. d.h.

   - Regelung des Netzzugangs über Login-Namen und Paßwort,
   - Vergabe differenzierter individueller Zugriffsrechte auf Dateien und Programme,
   - Zuordnung zu bestimmten Benutzergruppen und Rechtevergabe auf Verzeichnisebene, wobei sich die effektiven Zugriffsrechte aus einer Kombination der Nutzerrechte (bzw. Gruppenrechte) und deren Filterung auf Verzeichnisebene ergeben,

2. durch entsprechende Konfiguration der Anwendungssoftware, exemplarisch überprüft am Beispiel "Forum Klinikum",

3. durch zusätzliche Verfahren, wie die Installation eines Sicherheitsmoduls, das eine Unterbrechung ablaufender Stapeldateien und somit einen auf diese Weise unbefugt erzielbaren Systemzugang verhindert.

Darüberhinaus sind Server, Gateway und Streamer räumlich abgesichert und nur der Systemverwaltung zugänglich.

Auf der lokalen Ebene wird unbefugtes Einspielen und Entfernen von Dateien und Programmen durch bis auf wenige Ausnahmen (z.B. Systemverwaltung) generell verwendete Diskless-Workstations und durch Sperrung der Betriebssystemebene (Menüsteuerung, Start über ein Boot-ROM der Netzwerkadapterkarte etc.) verhindert.

Folgende Schwachstellen wurden inzwischen behoben:

- Ungeschützte Festplatten in zehn Workstations.

  Für die Nutzung wurde eine schriftliche Anweisung erarbeitet, mit der sich die Nutzer/-innen der mit Festplatten ausgestatteten PCs verpflichten, keine Dateien mit personenbezogenen Daten sowie keine wichtigen krankenhausinternen Daten zu speichern. Darüberhinaus wurde versichert, daß die Datenschutzbeauftragte nach meinem Vorschlag die Daten auf der Festplatte regelmäßig überprüfen und die Ergebnisse dokumentieren wird.

- Die Möglichkeit des Paßwortwechsels für Anwender/-innen wurde installiert.

- Die zeitlich unbeschränkte Möglichkeit des vollen Systemzugangs für zwei Mitarbeiter einer Wartungsfirma wurde beseitigt. Es ist nach Aussage des Krankenhauses aufgrund meiner Beanstandung eine besondere Gruppe "Wartung" eingeführt worden, die eingeschränkte Rechte auf das Volume hat, auf dem ausschließlich Systemsteuerparameter, Novellprogramme und Utilities stehen.

Folgende Schwachstelle bleibt bestehen:

Die Funktion des/der zentralen Systemverwalters/-verwalterin unterliegt keinerlei Zugriffsbeschränkungen und beinhaltet die Konfiguration sämtlicher Sicherheitsmaßnahmen. Es ist daher unbedingt erforderlich, diese Tätigkeit nachvollziehbar und kontrollierbar zu machen.

Die Stärke der zentralen Steuerung, technische Datenschutzmaßnahmen einheitlich realisieren zu können, eröffnet auf der anderen Seite allerdings das neue, für diese Systeme besonders aktuelle Datenschutzproblem, daß die zentrale Steuerung unkontrolliert bleibt. Es findet weder eine Protokollierung der Netzverwalteraktivitäten statt noch ist ein Vier-

Augen-Prinzip realisierbar, wonach Systemarbeiten nur von wenigstens zwei Mitarbeitern durchgeführt werden dürfen.

Die sich aus der Struktur des Netzbetriebssystems ergebende Schwachstelle ist unabhängig von der potentiellen Zuverlässigkeit des Systemverwalters/der Systemverwalterin.

Im Rahmen der inzwischen angebotenen neuen Version des verwendeten Netzbetriebssystems sind diese Probleme jedoch lösbar.

Eine Protokolldatei kann darin getrennt von der Systemverwaltung eingerichtet und ausgewertet werden. Darüber hinaus ist die Möglichkeit der Vergabe eines doppelten Paßwortes gegeben (Vier-Augen-Prinzip).

Da die Sicherheitsanforderungen eine Protokollierung erfordern, habe ich den Einsatz dieser verbesserten Version des Netzbetriebssystems vorgeschlagen.

8.4.1.3. ZKH-Bremen-Ost - EDV-Inseln und Entwicklung eigener Programme

Von den im ZKH-Ost angewandten Einzelverfahren habe ich die Medizinische Dokumentation im Archiv, die vorläufige Patientenaufnahme und exemplarisch zwei Textverarbeitungs-PCs überprüft.

In allen drei Bereichen werden sensible Patientendaten verarbeitet, wobei sich die Sensibilität der im Rahmen der medizinischen Dokumentation erfaßten Daten aus der Herstellbarkeit des Personenbezugs in der Abteilung "Betriebliches Rechnungswesen" sowie im Archiv selbst (Standort des Rechners) ergibt.

In allen drei Bereichen sind demnach hohe Datenschutzanforderungen zu stellen, die in folgenden Teilbereichen nicht erfüllt wurden:

Eigenentwicklung von Programmen

Sowohl in der Patientenverwaltung als auch in der medizinischen Dokumentation wird mit in der O/C- Abteilung des Krankenhauses entwickelten Programmen gearbeitet.

Eigenentwickelte Programme enthalten ein grundsätzlich höheres Datenschutzrisiko als Standardprogramme. Die unmittelbare Verfügbarkeit des Quellcodes ermöglicht jederzeit dessen Manipulierung, d.h. z.B. die unkontrollierbare Veränderung der Verarbeitungslogik oder versteckte Programmerweiterungen.

Aus diesem Grund muß die Eigen- und Weiterentwicklung folgende bisher im Krankenhaus Bremen-Ost noch nicht geltende Standards sowohl hinsichtlich Dokumentationspflicht und Datensicherheit als auch an geeigneten organisatorischen Maßnahmen erfüllt.

Die Weiterentwicklung des Dokumentationsprogramms muß getrennt von der Anwendung erfolgen, d.h.

- in der Entwicklungsabteilung, wobei die Auslieferung nur im compilierten Modus erfolgen darf und der Quellcode unter adäquaten Sicherungsmaßnahmen beim Entwickler verbleibt,

- versionsmäßig, d.h. Programmänderungen werden im Rahmen eines definierten Zeitraumes abschließend vorgenommen,getestet und ausreichend dokumentiert (Programm- und Pflegedokumentation).

Die Programmdokumentation kann grundsätzlich frei gestaltet werden, sollte allerdings Programmauftrag, Abwicklung, Einspielung und eine Dokumentation von Änderungen in Prozeduren enthalten.

Die Pflegedokumentation sollte das Datum und die Version der Betriebsaufnahme, eine namentliche Aufführung der das Verfahren in Produktion übernehmenden Personen sowie Benutzerrechte enthalten:

Durch geeignete Maßnahmen ist sicherzustellen, daß unbefugtes Einspielen veränderter Programmversionen auch nachträglich festgestellt werden kann.

Schriftlich, z.B. durch Dienstanweisungen, müssen verbindliche Zulässigkeitskriterien für Eigenentwicklung, technische und fachliche Verantwortlichkeiten, institutionalisierte interne Kontrollen sowie Kriterien zur Programmfreigabe festgelegt werden.

Funktionstrennungen

Grundlegender Bestandteil des Sicherheitskonzeptes ist jedoch die Funktionstrennung zwischen Entwicklung, Anwendung (fachliche Verantwortung) und Systemverwaltung. Die Aufgabenzuordnung im Krankenhaus sieht die erforderliche Funktionstrennung bisher nicht vor. Systemverwaltung und Entwicklung sind grundsätzlich nicht voneinander getrennt. Es existieren keine Kriterien für die Programmentwicklung durch die Systemverwaltung .

Im Rahmen der medizinischen Dokumentation ist der Quellcode des Programms sogar für die Anwendung zugänglich und jederzeit ohne Kontrolle veränderbar.

Um die Datenverarbeitung transparenter und kontrollierbarer zu machen (eine Protokollierung der Systemtätigkeiten fehlt) ist es erforderlich, Funktionstrennungen und Möglichkeiten der internen Kontrolle zu schaffen.

Systemverwaltung

Die Systemverwaltung ist das Bindeglied zwischen den DV-Inseln. Aufgrund der genannten Schwachstellen befindet sie sich augenblicklich hinsichtlich der DV-Struktur und der Zugriffsmöglichkeiten auf Patientendaten im "Land der unbegrenzten Möglichkeiten".

8.4.2. Das Ende der Jagd nach dem ominösen "Krankenhauswanderer"

Bei einem Prüfbesuch im Zentralkrankenhaus Reinkenheide in Bremerhaven hatte ich festgestellt, daß in der Patientenaufnahme mehrere Rundschreiben von Krankenhausgesellschaften anderer Bundesländer aushingen, in denen vor einzelnen namentlich aufgeführten Personen gewarnt wurde, nach deren Krankenhausbehandlung es Schwierigkeiten mit der Abrechnung gegeben habe. Die Schreiben enthielten z. T. auch wertende Äußerungen und Einzelheiten über das Verhalten der als "Krankenhauswanderer" bezeichneten Personen. Derartige Warnschreiben kursierten bundesweit. Der Umgang mit ihnen war in den einzelnen bremischen Krankenhäusern unterschiedlich. Z. T. wurden sie lediglich abgeheftet, aber nicht ausgewertet. Jedenfalls erfuhren die Betroffenen nichts davon, können sich also nicht dagegen wehren; Zweckbindungs- und Löschungsregelungen existieren nicht. Jedenfalls fehlt es einer solchen Datensammlung an der Rechtsgrundlage, insbesondere auch für die Einschaltung der privatrechtlich organisierten Krankenhausgesellschaften.

Auf mein Betreiben hat die Krankenhausgesellschaft der Freien Hansestadt Bremen inzwischen ihre Mitgliedskrankenhäuser gebeten, Warnschreiben nicht zu übermitteln, zu speichern oder zu nutzen und bereits gespeicherte Warnschreiben unverzüglich zu vernichten. Das Zentralkrankenhaus Reinkenheide hat mir bestätigt, daß es so verfahre.

8.5. Datenschutz in den Gesundheitsämtern

8.5.1. Trennung von Beratungs- und Verwaltungsdaten

In meinem 15. Jahresbericht (Ziff. 10.2) hatte ich erneut ein Gesetz über den öffentlichen Gesundheitsdienst mit Regelungen über die Befugnisse der Gesundheitsämter zur Verarbeitung von Daten ihrer Klienten, über die Geheimhaltungspflichten und die amtsinterne Zweckbindung angemahnt. Inzwischen wird im Hause des Senators für Gesundheit, Jugend und Soziales ein Gesetzentwurf mit den erforderlichen Datenschutzbestimmungen erarbeitet, an dessen Entstehung ich beteiligt werde.

Ein Problem vor allem ist dabei zu lösen: Daten, die Klienten dem Gesundheitsamt zum Zwecke der freiwilligen Gesundheitsberatung anvertraut haben, müssen auch amtsintern einen strikten Vertrauensschutz genießen, d. h. sie dürfen nicht für die Ausübung von Überwachungs- und Zwangsmaßnahmen genutzt werden (vgl. bereits 12. JB, Ziff. 2.7.12). Dagegen wird von sozialpsychiatrischer Seite eingewandt, dies sei unpraktikabel, weil in der Sozialpsychiatrie in beiden Funktionen weitgehend dieselben Ärzte und Psychologen tätig seien und im Einzelfall nur durch Zuhilfenahme des Wissens aus der anderen Funktion Gefahren für Gesundheit und Leben der Klienten oder Dritter begegnet werden könne.

Im weiteren Gesetzgebungsverfahren werde ich darauf achten, daß auch in der sozialpsychiatrischen Beratung der Vertrauensschutz grundsätzlich gewährleistet bleibt. Wer freiwillig Beratungshilfe in Anspruch nimmt, soll beim Gesundheitsamt die gleiche Vertraulichkeit erwarten können wie bei einem freien Träger. Er soll sich darauf verlassen können, daß ihm Angaben aus einem solchen Beratungsgespräch nicht im Verwaltungsvollzug entgegengehalten werden. Ausnahmen davon, d. h. die Nutzung von Beratungsdaten für Eingriffe, z. B. für Zwangseinweisungen nach dem Gesetz über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG), müssen eng begrenzt und gesetzlich geregelt werden.

8.5.2. Neuordnung der amtsärztlichen Kartei - EDV-Einsatz, innerbehördliche Zweckbindung und Löschung von Altdaten

Fortschritte erkenne ich bei der von mir im 15. Jahresbericht (Ziff. 10.2) angemahnten Neuordnung der Kartei des amtsärztlichen Dienstes und der Aussortierung von Altakten im Hauptgesundheitsamt Bremen. Wie dringlich dieses Vorhaben ist, zeigte sich, als anläßlich eines Forschungsvorhabens bekannt wurde, daß auf dem Dachboden des Bezirksgesundheitsamts Bremen-Nord noch Teile der NS-Erbgesundheitskartei lagern. In Absprache mit mir sind diese Unterlagen kurz darauf vom Staatsarchiv übernommen worden. Bislang wurde stets darauf hingewiesen, man wolle die Neuordnung des Gesamtbestandes zusammen mit der angestrebten Automatisierung der Kartei in Angriff nehmen. Letztere steht noch in diesem Jahr an, die PC-Anträge sind bereits mit mir abgestimmt worden.

Das Bezirksgesundheitsamt Bremen-Nord hat nunmehr im Vorgriff darauf begonnen, auf den Karten der Suchkartei seines amtsärztlichen Dienstes die unterschiedlichen Untersuchungsanlässe durch jeweils eine unterschiedliche Ordnungszahl zu kennzeichnen und die Akten der einzelnen Untersuchten danach aufzugliedern. Das Archivpersonal ist angewiesen, dem anfordernden Arzt nur den auf den konkreten Untersuchungsgrund bezogenen Teil der Akte auszuhändigen, es sei denn, der Betroffene habe schriftlich in die Nutzung auch anderer Aktenteile eingewilligt. Dieses Verfahren soll entsprechend nach Installierung einer automatisierten Datei fortgeführt werden. Zugleich hat man Löschungsfristen festgelegt und begonnen, alte Karteikarten und Akten, deren Löschungsfristen überschritten sind, auszusondern, dem Staatsarchiv anzubieten bzw. zu vernichten.

Ich begrüße es, daß mit diesem als Probelauf auch für das Hauptgesundheitsamt Bremen bezeichneten Vorgehen schon vor Inkrafttreten einer bereichsspezifischen gesetzlichen Regelung ein wichtiger Schritt bei der Verwirklichung des Datenschutzes im öffentlichen Gesundheitsdienst getan wird.

8.5.3. Anonymität in der Schwangerschaftskonfliktberatung

Das Urteil des Bundesverfassungsgerichts vom 28.05.1993 zur Regelung des Schwangerschaftsabbruchs hat lebhaften öffentlichen Streit erregt. Gesetzentwürfe der CDU/CSU und FDP-Fraktion sowie der SPD-Fraktion im Deutschen Bundestag für eine Neuregelung liegen vor. Das Gericht hat bis zum Inkrafttreten eines novellierten § 218-Gesetzes eine Reihe von Maßnahmen angeordnet.

Ich habe mich den zuständigen Behörden und sonstigen betroffenen oder interessierten Stellen im Lande Bremen und den Medien gegenüber zu den datenschutzrechtlichen Aspekten der Anordnung geäußert. Ihr Schwerpunkt ist die Beratung der Schwangeren durch eine anerkannte Beratungsstelle. Dabei soll die Schwangere auf ihren Wunsch gegenüber der sie beratenden Person anonym bleiben können. Mein Vorschlag hierzu ist, die Ratsuchende auf dieses Recht nicht nur durch ein ausliegendes oder aushängendes Informationsblatt, sondern auch mündlich in einer geeigneten, dem Beratungserfolg förderlichen Weise hinzuweisen. Nach dem Beratungsgespräch hat - so das Gericht- die Beratungsstelle der Frau auf Antrag über die Tatsache, daß die Beratung stattgefunden hat, eine auf ihren Namen lautende Bescheinigung auszustellen. Die Frage ist, wie trotzdem der Wunsch nach Anonymität respektiert werden kann, zumal wenn eine Beratungsstelle zeitweise nur mit einer Person - eben der Beraterin - besetzt ist. Notfalls müsse der Schwangeren - so mein Vorschlag - erlaubt werden, selbst ihren Namen in die Bescheinigung einzusetzen. Das Bundesverfassungsgericht habe nicht eine Identitätskontrolle verlangt. Hingegen ist der Urteilsbegründung zu entnehmen, daß das Gericht als Voraussetzung für die vom ihm geforderte "ergebnisoffene" Beratung eine Beteiligung der Frau an der Suche nach einer Lösung ihres Konflikts ansieht; dies wiederum rechtfertigt es, davon abzusehen, die Frau zu verpflichten, sich im Beratungsgespräch als Person zu identifizieren. Das Gericht mißt dem Wunsch nach Anonymität einen hohen Stellenwert bei. Dann aber müssen die Beratungsstellen auf Wunsch der Schwangeren die Anonymität auch effektiv gewährleisten. Der Staat wiederum darf nur solche Beratungsstellen anerkennen, die den Anforderungen des Urteils genügen. Zugleich ist er verantwortlich, daß es solche Beratungsstellen gibt. Damit trägt er auch die Verantwortung für die Gewährleistung der Anonymität.

Die beratende Person soll, so fährt die richterliche Anordnung fort, über jede Beratung ein anonymisiertes Protokoll anfertigen, das der staatlichen Aufsicht und zu statistischen Zwecken dient. Ich habe auch hier Empfehlungen zur Gewährleistung der Anonymität ausgesprochen.

Mir ist nicht bekannt, inwieweit der Senator für Gesundheit, Jugend und Soziales als Aufsichtsbehörde meine Vorschläge aufgegriffen hat oder aufgreifen will. Ich hatte aber Gelegenheit, sie mit der Bremischen Zentralstelle für die Verwirklichung der Gleichberechtigung der Frau und Trägern von Beratungsstellen zu erörtern und habe dabei positive Reaktionen erfahren.

8.6. Sozialdatenschutz im Amt für Soziale Dienste Bremen

8.6.1. Fall: Offenbarung des Sozialhilfebezugs an den Vermieter

Der Hilfeempfänger hat nach § 35 SGB I Anspruch darauf, daß der Sozialhilfeträger seine Daten als Sozialgeheimnis schützt und nur bei Vorliegen der gesetzlichen Voraussetzungen an andere Stellen übermittelt. Ein Bürger hatte sich an mich gewandt und darüber Klage geführt, daß das Sachgebiet "Wirtschaftliche Hilfen" des zuständigen bremischen Ortsamts die Miete für seine Wohnung direkt an den Vermieter überwiesen habe, ohne ihn zuvor gefragt zu haben. Damit aber wurde zwangsläufig dem Vermieter bekannt, daß sein Mieter Sozialhilfeempfänger war.

Auf meine Intervention hin hat der Senator für Gesundheit, Jugend und Soziales im Wege der Fachaufsicht das Ortsamt und die anderen Sozialhilfebehörden angewiesen, die Miete nur dann direkt an den Vermieter zu zahlen, wenn entweder der Hilfeempfänger dem

schriftlich zugestimmt hat oder wenn aus begründetem Anlaß zu befürchten ist, daß der Betroffene selbst die Miete mit dem ihm überwiesenen Geld nicht zahlen werde.

8.6.2. Auskunftspflicht des Unterhaltspflichtigen gegenüber dem Sozialamt

Das Amt für Soziale Dienste Bremen verlangte früher von einer dem Sozialhilfeempfänger gegenüber zu Unterhaltszahlungen verpflichteten Person auch Auskunft über die Einkommens- und Vermögensverhältnisse ihres Ehegatten, obwohl dieser selbst dem Sozialhilfeempfänger gegenüber gar nicht unterhaltspflichtig war. Diese Praxis hatte ich aus Rechtsgründen bemängelt und auf die Freiwilligkeit der den Ehegatten betreffenden Antworten hingewiesen. Nachdem das Bundesverwaltungsgericht im gleichen Sinne entschieden (abgedruckt im Deutschen Verwaltungsblatt 1993, 791) und auch der Datenschutzausschuß der Bremischen Bürgerschaft die Problematik erörtert hatte (vgl. o. Ziff. 1.4), hat der Senator für Gesundheit, Jugend und Soziales den Entwurf einer entsprechenden Änderung seiner Richtlinien vorgelegt und die Änderung des Vordrucks für die an die Unterhaltspflichtigen gerichteten Fragebögen angekündigt.

Die aus der Sicht der Sozialhilfeträger erhobene entgegengesetzte Forderung, die einschlägige Vorschrift des § 116 BSHG um die Auskunftspflicht des selbst nicht unterhaltspflichtigen Ehepartners zu ergänzen, hat der Gesetzgeber bisher nicht aufgegriffen.

Zugleich bestätigte das Bundesverwaltungsgericht mit dem zitierten Urteil eine Praxis des Amtes für Soziale Dienste, gegen die sich ein Bürger beschwerdeführend an mich gewandt hatte. Er hatte gegenüber dem Amt bestritten, daß er einer Sozialhilfeempfängerin zum Unterhalt verpflichtet sei und daraus geschlossen, daß deshalb § 116 BSHG ihn nicht zur Auskunft über seine Einkommens- und Vermögensverhältnisse verpflichte. Dagegen - so das Gericht - setze der gesetzliche Auskunftsanspruch nicht voraus, daß der Unterhaltsanspruch tatsächlich bestehe. Denn Zweck der Auskunft sei es gerade auch, dem Sozialhilfeträger die Prüfung zu ermöglichen, ob er überhaupt auf ihn übergegangene Unterhaltsansprüche geltend machen könne.

8.6.3. Schutz des Beratungsgeheimnisses innerhalb des Amtes für Soziale Dienste - neue Dienstanweisungen

Meine Initiative, die Daten auf das erforderliche und nach dem KJHG rechtlich zulässige Maß zu begrenzen, die der ambulante Sozialdienst bzw. das Kindertagesheim dem Sachgebiet "Wirtschaftliche Jugendhilfe" des Amtes für Soziale Dienste Bremen zwecks Entscheidung über die Kostentragung einer Leistung der Jugendhilfe weitergeben darf und muß (vgl. 15. JB, Ziff. 9.1), war teilweise erfolgreich. Nachdem der Datenschutzausschuß der Bremischen Bürgerschaft sich mehrere Male mit der Problematik befaßt hatte, hat inzwischen der Senator für Gesundheit, Jugend und Soziales in den Dienstanweisungen "Datenschutz" und "Hilfeplanung" Regelungen der Problematik vorgelegt. Beiden hat der Jugendhilfeausschuß der Bremischen Bürgerschaft zugestimmt, der Personalrat des Amtes für Soziale Dienste lehnt sie ab.

Die vorgelegten Dienstanweisungen ordnen eine Eingrenzung des Datenaustauschs an. Der vom Sozialdienst zu erstellende Hilfeplan nach § 36 KJHG soll alleinige Grundlage der Kostenentscheidung sein. Alle anderen Unterlagen wie psychosoziale Diagnosen, ärztliche oder psychologische Gutachten und Entwicklungs- oder Verlaufsberichte von Einrichtungen sollen beim Sozialdienst verbleiben. Leider ist meine Anregung, den Hilfeplan mittels eines Vordrucks zu standardisieren und quantitativ einzugrenzen, nicht aufgegriffen worden. Entsprechend der Erwartung des Datenschutzausschusses werde ich nach Abschluß der vom Ressort angekündigten Testphase für die beiden Dienstanweisungen prüfen, wie weit nunmehr die Praxis anders als bisher den gesetzlichen Voraussetzungen gerecht wird.

Dagegen sind die Gespräche mit Hauptamt, Sozialamt und Gesundheitsamt über die entsprechende Eingrenzung des Datenflusses bei der Eingliederungshilfe für Erwachsene in Bremerhaven immer noch nicht abgeschlossen (vgl. 15. JB, Ziff. 9.1, 3. Spiegelstrich).

Zwar meinte der Senat in seiner Stellungnahme, die Standpunkte des Magistrats der Stadt Bremerhaven seien meinen Vorstellungen weitgehend angepaßt. Hauptamt und Sozialamt beharren aber darauf, daß die Berichte der Träger von Eingliederungshilfe (etwa "Betreutes Wohnen"), die Grundlage von sozialpsychiatrischen Stellungnahmen des Gesundheitsamts sind, von diesem an das Sozialamt weitergeleitet werden. Lediglich in der Frage der inhaltlichen Begrenzung und Vorstrukturierung der Berichte der Träger und der Stellungnahmen des Gesundheitsamtes zeichnet sich eine Verständigung ab.

8.6.4. Raumnot gefährdet Sozialgeheimnis

Die räumlichen Verhältnisse, in denen die Sozialhilfesachbearbeiter arbeiten, sind in zahlreichen Ämtern Bremens derart beengt, daß zugleich mehrere Klienten in einem Raum "abgefertigt" werden müssen. Folge ist, daß der eine Klient zwangsläufig Daten des anderen mithört - eine klare Verletzung des Sozialgeheimnisses. Pflicht des Sozialhilfeträgers ist es, diesem Zustand durch bauliche und organisatorische Maßnahmen abzuhelfen (§ 35 SGB I).

Zuletzt hatte ich in meinem 11. Jahresbericht (Ziff. 5.5.1.6) über derartige Probleme in den Regionalabteilungen Süd und Ost des Amtes für Soziale Dienste berichtet. Was erstere betrifft, hat sich durch ihren zwischenzeitlichen Umzug anscheinend die Angelegenheit erledigt. Anders verhält es sich mit der Regionalabteilung Ost - trotz Umzugs - und mit dem Sachgebiet "Wirtschaftliche Hilfen" des Ortsamtes Osterholz. Beide Fälle wurden auch von den Medien aufgegriffen. Im zweiten Fall habe ich nach Überprüfung der Verhältnisse vor Ort an das Ortsamt selbst, den Senator für Inneres und Sport und den Senator für Gesundheit, Jugend und Soziales geschrieben und auf Abhilfe gedrängt. Wie ich wiederum aus den Medien erfuhr, ist eine schnellere Besserung jedenfalls durch zusätzliche Räume nicht zu erwarten.

Dagegen hat jetzt der Magistrat Bremerhaven mitgeteilt, er habe organisatorische Vorkehrungen dafür getroffen, daß im Sozialamt - zumindest bei der Aufnahme von Erstanträgen - nach Möglichkeit kein weiterer Hilfeempfänger parallel bedient werde. Entsprechendes werde für alle Gespräche mit Klienten angestrebt. Ich sehe hierin einen Schritt, mit der der Sozialhilfeträger im Rahmen knapper Mittel und beengter Räume versucht, seiner Verantwortung für die Wahrung des Sozialgeheimnisses der Sozialhilfeempfänger gerecht zu werden. Finanzielle Gegenargumente dürfen m. a. W. so lange nicht angeführt werden, wie der Vertraulichkeitsgrundsatz durch organisatorische Änderungen verbessert werden kann.

8.7. Sozialdatenschutz beim Senator für Gesundheit, Jugend und Soziales - Bereich Jugend und Soziales

8.7.1. Mitarbeiter- und Klientenlisten - Personenbezug auch für Planung, Statistik und Aufsicht

8.7.1.1. Heimaufsicht

Ein freier Träger hatte mir einen Fragebogen vorgelegt, mit dessen Hilfe der Senator für Gesundheit, Jugend und Soziales die Personalien der Mitarbeiter seiner Kindertagesheime abfragte. Die Daten sollten erklärtermaßen zugleich für die Heimaufsicht, für die Bedarfsplanung und als Grundlage für die Verhandlungen zur angestrebten Veränderung der Betriebszuschüsse genutzt werden.

Ich habe vor allem darauf aufmerksam gemacht, daß die Daten nur zum Zwecke der Heimaufsicht erhoben werden dürften und nach § 11 Abs. 2 Satz 2 des Bremischen Ausführungsgesetzes zum Kinder- und Jugendhilfegesetz nach Abschluß der Eignungsüberprüfung die Daten unverzüglich zu vernichten seien, die den durch § 47 KJHG geregelten Umfang überstiegen. Unabhängig davon aber dürfen die in diesem Zusammenhang erhobenen personenbezogenen Daten zum Zwecke der Bedarfsplanung und der Zuschußverhandlungen nur in anonymisierter Form genutzt werden. Nachdem ich wiederholt insi-

stiert hatte, hat nunmehr die senatorische Dienststelle zugesagt, man werde künftig auf die maschinelle Erfassung von Namen und vollständigen Geburtsdaten der Mitarbeiter verzichten.

8.7.1.2. Weitere Fälle

Über diesen Vorgang hinaus beobachte ich, daß zunehmend personenbezogene Daten von Mitarbeitern und Klienten von Einrichtungen der Sozial- und Jugendhilfe zum Zwecke nicht etwa der Entscheidung über die Hilfe oder ihre Kosten im Einzelfall, sondern zu Zwecken der Statistik, der Bedarfsplanung oder der Entscheidung über institutionelle oder projektbezogene Zuschüsse erhoben und ausgewertet werden:

- Der Senator für Gesundheit, Jugend und Soziales erhebt als überörtliche Betreuungsbehörde nach § 4 des Bremischen Ausführungsgesetzes zum Betreuungsgesetz bei den Betreuungsvereinen die Personalien nicht nur der von diesen beratenen ehrenamtlichen Betreuer, sondern auch der "durch den Verein informierten BürgerInnen, die sich für ein Ehrenamt interessiert haben, aber dem Gericht noch nicht benannt wurden". Als Grund werden Richtlinien angegeben, nach denen anerkannte Betreuungsvereine dann finanziell gefördert werden können, wenn sie mindestens 25 Personen namentlich nachgewiesen haben, die zur Betreuung bestellt wurden oder bereit sind, Betreuungen zu übernehmen.

- Der Senator für Gesundheit, Jugend und Soziales erhebt zum Zwecke der Aufsicht über Seniorenheime im Lande Bremen personenbezogene Daten von deren Mitarbeitern.

- Der Senator für Gesundheit, Jugend und Soziales erhebt für statistische Zwecke bei den Trägern des Betreuten Wohnens zahlreiche Daten über deren Klienten.

- Der Leiter des Zentralkrankenhauses Bremen-Ost hat in seiner Eigenschaft als Projektleiter einer "Kommission zur Personalbemessung im komplementären Bereich" der "Aktion psychisch Kranke" die Träger des Betreuten Wohnens um Ausfüllung von Bögen gebeten, die eine Fülle von Daten über ihre Klienten erfragen. Das Projekt soll der "klientenbezogenen Ermittlung des Bedarfs an notwendigen Hilfen" dienen.

- Der Bundesminister für Arbeit und Sozialordnung verlangt vom Träger eines Projekts zur Berufsberatung für ausländische Frauen, für das Mittel des Europäischen Sozialfonds beantragt worden sind, die Hergabe von Listen mit den Personalien der ratsuchenden Frauen zur Weiterleitung an die EG-Kommission.

Es handelt sich um unterschiedliche Sachverhalte. Gemeinsam ist ihnen, daß individuelle Daten von Mitarbeitern oder Klienten abgefragt werden, es aber nicht um personenbezogene Einzelentscheidungen geht, sondern um Zuschüsse, aufsichtsbehördliche Fragestellungen oder statistische und planerische Zwecke. Auffällig ist, daß sich Anfragen von freien Trägern aus den Bereichen der Sozial- und Jugendarbeit häufen, die Bedenken gegen die Preisgabe von Daten ihrer Mitarbeiter und Klienten haben.

Ich werde vor allem darauf achten, daß

- die beruflichen Schweigepflichten bzw. Beratungsgeheimnisse gewahrt bleiben

- die Datenverarbeitung auf das erforderliche Maß begrenzt bleibt, insbesondere der Personenbezug dort unterbleibt, wo aggregierte Angaben ausreichen

- die Zweckbindung bei der Verarbeitung personenbezogener Daten eingehalten wird und

– die Transparenz für die Betroffenen gewahrt bleibt und sie bei Datenerhebungen über das gesetzlich geregelte Maß hinaus um ihre Einwilligung gebeten werden.

8.7.2. Zugriffsschutz und Textverarbeitung im PROSOZ-Verfahren

Der Praxis des dialogorientierten Sozialhilfeberechnungsverfahrens "PROSOZ" liegt seit seiner Einführung ein differenziertes Datenschutzkonzept zugrunde, das sowohl inhaltliche als auch technische und organisatorische Datenschutzbelange berücksichtigt (vgl. 10. JB Ziff. 5.6.1, 11. JB Ziff. 5.5.1.1, 13. JB Ziff. 2.5.3).

Funktionserweiterungen, die sich aus der praktischen Arbeit mit dem System ergaben, sind jedoch nicht mehr in das Datenschutzkonzept eingegangen. Dies führt auf Dauer zu einer Abkopplung des Systems von der ursprünglichen Datenschutzkonzeption. Nur durch die Interaktion zwischen Verarbeitungs- und Schutzfunktionen kann eine praktikable und angemessene Datenschutzkomponente in das System integriert werden.

Während meines Prüfbesuches beim Senator für Jugend, Gesundheit und Soziales stellte ich auf dem zur Prüfung ausgewählten Rechner der ADV-Verbindungsstelle fest, daß folgende Funktionserweiterungen ohne Abstimmung mit dem Datenschutzkonzept und damit im Widerspruch zu § 79 SGB X i.V.m. § 9 BDSG erfolgt sind:

- Der Zugriff auf Echtdaten für Koordinations- und Weiterentwicklungsaufgaben darf nicht auf personenbezogene Falldaten, sondern nur auf eine Testdatenbank erfolgen (vgl. 1.6.2 des Datenschutzkonzeptes).

- Mitarbeiter der ADV-Verbindungsstelle dürfen sich selbst nicht uneingeschränkt Zugriffsrechte fallbearbeitender Sachbearbeiter/-innen zuweisen können.

Die erforderliche Aktualisierung des DS-Konzeptes soll in diesem Jahr mit der Erweiterung des PROSOZ-Systems um eine Textverarbeitungssoftware für die Anwender/-innen aus dem Bereich der Sozialhilfeverwaltung erfolgen. Dabei wurde ich zu Beginn der Planungsphase beteiligt.

Folgende Standards sind bereits festgelegt, wobei die Datenschutzsoftware "Safe-Guard", die bei der Sensibilität der zu verarbeitenden Daten erforderlich wäre, aus technischen Gründen nicht eingesetzt werden kann:

- Der im bisherigen Datenschutzkonzept festgelegte Standard soll erhalten bleiben.

- Aus dem Programmsystem PROSOZ soll nur ein eng begrenzter Datenumfang in die Textverarbeitung übernommen werden.

- Die Zugangsberechtigung für die Arbeit mit dem Programmsystem PROSOZ wird nicht verändert.

- Bei den Arbeitsplatzrechnern wird der Paßwortschutz des System-Bios aktiviert.

- Die Diskettenlaufwerke bleiben gesperrt.

- Die Textdateien und deren Sicherungskopien werden automatisch nach einer Woche, temporäre Dateien täglich gelöscht.

- Es erfolgt eine physische Löschung der o.g. Dateien, so daß eine Wiederherstellung nicht möglich ist.

8.8. Arbeit und Frauen

8.8.1. Arbeitsschutz und Genomanalyse

8.8.1.1. Der Entwurf eines Arbeitsschutzrahmengesetzes

Die Bundesregierung hat am 05.1.1993 (BR.-Drs. 792/93) den Entwurf eines Arbeitsschutzrahmengesetzes (ASRG) vorgelegt. Ich habe dazu gegenüber dem Senator für Arbeit und Frauen ausführlich Stellung genommen.

Mit diesem Entwurf ist beabsichtigt, die einschlägigen EG-Richtlinien zur Verbesserung der Sicherheit und des Gesundheitsschutzes bei der Arbeit und in Arbeitsstätten in nationales Recht umzusetzen. Insbesondere will der Gesetzentwurf zulassen, im Rahmen arbeitsmedizinischer Vorsorgeuntersuchungen auch genomanalytische Untersuchungen vorzunehmen, obwohl sie besonders tief in das informationelle Selbstbestimmungsrecht des Beschäftigten eingreifen und daher auch besonders umstritten sind. Genomanalytische Untersuchungen tangieren die Lebenssituation der Beschäftigten deshalb so stark, weil

- eine festgestellte genetische Veranlagung von dem Betroffenen nicht beeinflußt werden kann,
- das genetische Merkmal vererblich ist und
- die Gefahr einer sozialen Selektion besteht ("erbschwache" und "erbstarke" Arbeitnehmer).

Die Risiken und Gefährdungen genomanalytischer Untersuchungen im Arbeitsverhältnis sind in parlamentarischen Gremien auf Bundesebene ebenso wie in jeweiligen Fachkreisen ausgiebig erörtert worden. Zu verweisen ist u. a. auf den Bericht der Enquête-Kommission "Chancen und Risiken der Gentechnologie" vom 06.01.1987 (BT-Drs. 10/6775), die Beschlußempfehlung und den Bericht des Ausschusses für Forschung und Technologie des Deutschen Bundestages zum Bericht der Enquête-Kommission vom 04.10.1989 (Drs. 11/5320, S. 13 ff), den Abschlußbericht der Bund-Länder-Arbeitsgruppe "Genomanalyse" vom Mai 1990 (gebildet aus Vertretern der Justiz- und Gesundheitsressorts von Bund und Ländern sowie Vertretern verschiedener Bundesministerien, darunter auch des Bundesministeriums für Arbeit und Sozialordnung) sowie die daraus resultierende "Entschließung des Bundesrates zur Anwendung gentechnischer Methoden" vom 16.10.1992 (BR-Drs. 424/92, S. 5).

Aus datenschutzrechtlicher Sicht stehen die Fragen der Einwilligung, der Geeignetheit und des Fragerechts des Arbeitgebers im Vordergrund.

8.8.1.2. Einwilligung und Abhängigkeit

Sowohl bei Erst- als auch bei sonstigen Vorsorgeuntersuchungen sollen nach dem Entwurf die Einwilligung des Beschäftigten sowie eine umfassende Aufklärung Voraussetzungen für die Zulässigkeit sein. Der Arbeitnehmer sieht sich jedoch sowohl bei Erstuntersuchungen - nicht nur im Rahmen von Einstellungsuntersuchungen - als auch bei späteren Vorsorgetests in häufig für ihn schwer einschätzbaren Situationen stärkeren Gegenspielern (Arbeitgeber, Personalchef, Betriebsarzt) gegenüber, und zwar meist allein ohne Beisein etwa des Betriebsrats. Dann dürfte ihm schwerfallen, auf die Einhaltung differenzierter Schutzvorschriften zu bestehen. Dies gilt in besonderem Maße in Zeiten der Rezession und verstärkter Angst vor Arbeitslosigkeit und Entlassung. In Konstellationen starker persönlicher Abhängigkeit versagt die Einwilligung als Verarbeitungslegitimation. Hinzu kommt, daß auch eine noch so umfassende und gutgemeinte Aufklärung ihm angesichts der Vorläufigkeit des derzeitigen wissenschaftlichen Erkenntnisstandes nicht hinreichend die Auswirkungen einer eventuellen Einwilligung vermitteln kann.

Auch der Vorschlag der Enquête-Kommission des Deutschen Bundestages (a.a.O., S. 168 ff), Untersuchungen nur über die gegenwärtige gesundheitliche Eignung zuzulassen, dagegen Untersuchungen über Krankheitsanlagen und künftige Krankheiten auszuschließen, scheint in der Praxis kaum überprüfbar. Er geht außerdem an den Interessen des Arbeitgebers vorbei und wird den spezifischen Möglichkeiten der Genomanalyse nicht gerecht. Beide richten sich übereinstimmend auf das, was die Kommission gerade verbieten will. Zur Feststellung der aktuellen Gesundheitssituation reichen in der Regel die konventionellen ärztlichen Methoden aus. Die Genomanalyse wird hier kaum zusätzliche Erkenntnisse liefern können; ihre besondere Qualität ist vielmehr der "Blick in die Zukunft".

Dem Beschäftigten selbst sollte es unbenommen bleiben, sich durch eine vom Arbeitgeber unabhängige Untersuchung, d. h. durch einen Arzt seines Vertrauens, über mögliche Gefährdungen und Risiken Sicherheit zu verschaffen. In jedem Fall muß er dann über die so gewonnenen Erkenntnisse allein verfügungsberechtigt bleiben. Es darf nicht zugelassen werden, daß er unter Druck gesetzt wird bzw. sich ihm ausgesetzt fühlt, seinen Zustand zu offenbaren. Unverzichtbar ist ein gesetzliches Verbot für den Arbeitgeber, sich die Ergebnisse der freiwilligen Untersuchung außerhalb des Arbeitsverhältnisses vorlegen zu lassen.

8.8.1.3. Prinzipielles Verbot genomanalytischer Untersuchungen

In der Begründung zu diesem Gesetzentwurf wird ausgeführt, bisher existierten kaum Laboratoriumstests auf DNA- oder Gen-Produktebene zur Feststellung genetisch bedingter individueller Risiken. Die Entwicklung solcher Tests sei aber nicht auszuschließen und würden voraussichtlich eine präzisere Aussage über das anlagebedingte Risiko einer Erkrankung bei einer bestimmten Einwirkung am Arbeitsplatz erlauben. Daraus ergibt sich, daß derartige Tests nach dem derzeitigen wissenschaftlichen Erkenntnisstand nicht geeignet sind, dem Ziel einer arbeitsmedizinischen Vorsorge gerecht zu werden. Auch aus diesem Grunde ist eine Erlaubnisregelung für genomanalytische Untersuchungen nicht geboten.

Ich trete daher dafür ein, nicht nur - wie es der Gesetzentwurf bereits vorsieht - Untersuchungen, die der bloßen Aufdeckung der Erbanlagen dienen (Genomanalysen), zu verbieten, sondern auch Untersuchungen, durch die bestimmte ererbte Veranlagungen für Erkrankungen ermittelt werden können (genomanalytische Untersuchungen). Dies entspricht der Position, die die Bundesregierung noch selbst in ihrem Bericht vom 05.12.1990 über die Umsetzung des Beschlusses des Deutschen Bundestages zum Bericht der Enquête-Kommission (Drs. 11/8520, S. 19 ff) eingenommen hatte, und zwar auch für den Fall, daß die zukünftige Krankheit die Einsetzbarkeit am vorgesehenen Arbeitsplatz beeinträchtigen könnte. In dem o. a. Bericht hatte sich die Bundesregierung auch dafür ausgesprochen, Verletzungen der Fragegrenzen des Arbeitgebers strafrechtlich zu ahnden, sich allerdings für die Frage der Sanktionen noch eine weitere Prüfung vorbehalten.

Dem Senator für Arbeit und Frauen gegenüber habe ich diese Position unterstützt, daß ein Verbot genomanalytischer Untersuchungen nur dann wirksam eingehalten werden kann, wenn Überschreitungen des Fragerechts durch den Arbeitgeber, d. h. die Forderungen nach Durchführung eines solchen Tests oder auf Herausgabe von Unterlagen darüber, strafrechtlich geahndet werden.

8.8.1.4. Die aktuelle Position des Bundesrats

Der Bundesrat hat in seiner am 17.12.1993 verabschiedeten Stellungnahme zu dem Gesetzentwurf (BR-Drs. 792/93, Ziff. 49) die Bundesregierung u. a. gebeten, im weiteren Gesetzgebungsverfahren auch ein völliges Verbot genomanalytischer Vorsorgeuntersuchungen zu prüfen.

Der Bundesrat hat seine restriktive Haltung mit den auch von mir für stichhaltig erachteten Argumenten begründet: Diese Untersuchungen würden tief in das Persönlichkeitsrecht des betroffenen Arbeitnehmers eingreifen und könnten seine Chancen auf dem Arbeits-

markt entscheidend beeinflussen. Der Arbeitnehmer habe grundsätzlich das Recht auf Nichtwissen seiner genetischen Konstitution und auf informationelle Selbstbestimmung über seine genetischen Daten.

Diese Bedenken würden durch ein Einwilligungserfordernis nicht ausgeräumt. Der Arbeitnehmer sei gegenüber dem Arbeitgeber in aller Regel in abhängiger Position und könne sich dessen Forderungen nur schwer widersetzen.

Das Gesetzgebungsverfahren ist noch nicht abgeschlossen. Der Bundestag hat Ende Februar 1994 den Entwurf in erster Lesung beraten.

8.8.2. Präziser Datenkatalog für das Schwerbehinderten-Verzeichnis

Nach § 13 des Schwerbehindertengesetzes (SchwbG) haben die Arbeitgeber ein Verzeichnis der bei ihnen beschäftigten Schwerbehinderten, Gleichgestellten und sonstigen auf die Pflichtquote anrechnungsfähigen Personen laufend zu führen und den Vertretern des Arbeitsamtes und der Hauptfürsorgestelle auf Verlangen vorzuzeigen. Des weiteren enthält diese Vorschrift die Verpflichtung der Arbeitgeber, einmal jährlich eine Anzeige an das zuständige Arbeitsamt vorzunehmen, die bestimmte Angaben enthalten muß. Dieser Anzeige ist außerdem das o. a. Verzeichnis beizufügen.

Da im Gesetz nicht im einzelnen festgelegt ist, welche personenbezogenen Daten der Arbeitgeber in das Verzeichnis aufzunehmen hat, kann der Betroffene nicht hinreichend erkennen, in welchem Umfange durch die Weitergabe sensibler Angaben über seinen Gesundheitszustand bzw. seine Behinderung in sein Persönlichkeitsrecht eingegriffen werden darf. Auch die Herausgabe eines entsprechenden Vordruckes durch die Bundesanstalt für Arbeit kann die fehlende gesetzliche Detailregelung nicht ersetzen.

Ich habe daher den Senator für Arbeit und Frauen gebeten, sich auf Bundesebene für eine entsprechende Ergänzung des SchwbG einzusetzen. Er teilt meine Rechtsauffassung und hat sich in dieser Angelegenheit an den Bundesminister für Arbeit und Sozialordnung gewandt.

8.8.3. Weiterbildungsdatenbank

Bei der Weiterbildungsdatenbank Bremen handelt es sich um ein Informationssystem, das vor allem von regionalen Trägern gemeldete Bildungsangebote umfaßt und der Allgemeinheit zur Verfügung stellt. Personenbezogene Daten werden u. a. über Dozenten, Kontaktpersonen und Ansprechpartner für Bildungsangebote verarbeitet. Entwickelt und betrieben wird das System im Auftrag des Senators für Arbeit und Frauen von dem dem Berufs-Bildungs-Institut der Angestelltenkammer angeschlossenen Gemeinnützigen Zentrum für Informationstechnik (GZI) Bremerhaven, das auch die Entwicklung und Pflege von Software und Datenbank verantwortet.

Das Informationssystem ist in sogenannten Clustern organisiert, d. h. selbständigen Informationseinheiten, die der zentralen Datenhaltung und der Ermöglichung von Online-Abfragen dienen. Wegen der geographischen Struktur des Landes Bremen gibt es jeweils einen Cluster im GZI Bremerhaven und im GZI Bremen. Die Datenbankpflege und -verwaltung erfolgt im GZI Bremerhaven zentral von einem sogenannten Master-Cluster aus. Informationsstationen, an denen sich Interessenten über Kurs- und Weiterbildungsangebote informieren können, sind derzeit im Landesamt für Weiterbildung, in der Zentralstelle für die Verwirklichung der Gleichberechtigung der Frau, Hauptstelle Bremen und Außenstelle Bremerhaven, im GZI Bremen und im GZI Bremerhaven eingerichtet.

In meiner Stellungnahme gegenüber dem GZI Bremerhaven ging es insbesondere um die Abgrenzung unterschiedlicher Verantwortungsbereiche und Zuständigkeiten zwischen den beteiligten Stellen, die notwendigen Zugangs- und Zugriffssicherungen und die Zulässigkeit der personenbezogenen Datenhaltung. Das System ist zwischenzeitlich in Betrieb

genommen worden. Ich werde zu prüfen haben, inwieweit meinen Anregungen Rechnung getragen wurde.

9. Wirtschaft, Mittelstand und Technologie

9.1. Neues Gewerbemeldeverfahren

Mit der Ablösung des Einwohnermeldesystem EDAS durch DEMOS im Laufe des Jahres 1994 wird es erforderlich, auch ein neues Gewerbemeldeverfahren in der Stadtgemeinde Bremen einzuführen. Das bisherige Verfahren ist mit dem Einwohnermeldesystem verknüpft, was ich in mehreren Jahresberichten kritisiert habe, weil Daten in einer Datenbank verwaltet und über Bildschirm dargestellt werden, die verschiedenen Zwecken dienen. Nunmehr ist das Stadtamt aufgefordert, ein neues Verarbeitungs- und Auskunftssystem zu projektieren und zu installieren.

Ich habe meine Bereitschaft zur Mitarbeit in der entsprechenden Arbeitsgruppe erklärt und bereits vorab einige datenschutzrechtliche Vorgaben gemacht. Notwendig sind u. a. ein klar festgelegter Datenkatalog, die Festschreibung von Abruf- und Datenübermittlungsverfahren, die Protokollierung der Aktivitäten im DV- und Zugriffssystem sowie Sperr- und Löschungsfunktionen. Einzelheiten werden in einem umfangreichen Datenschutzkonzept zu beschreiben sein.

Sollte es noch in dieser Legislaturperiode zu der angestrebten Änderung der Gewerbeordnung mit bereichsspezifischen Regelungen für die Erhebung und Übermittlung von Daten in Gewerbezulassungs- und -versagungsverfahren kommen, wird dies die Basis für die Struktur des neuen Verfahrens werden. Der mir im Sommer 1993 zugegangene Entwurf sieht allerdings noch viel zu weitgehende Mitteilungspflichten, Weitergabebefugnisse und Zweckänderungsregelungen vor.

9.2. Integriertes Verwaltungs- und Kontrollsystem (InVeKos) im Bereich der Landwirtschaftsförderung

Im Lande Bremen bestehen ca. 500 (!) landwirtschaftliche Betriebe, von denen ca. die Hälfte Vollerwerbsbetriebe sind. Die EG hat durch zwei Verordnungen (EWG-VO Nr. 3508/92 und Nr. 3887/92) den Mitgliedstaaten u.a. ein Kontrollsystem für die landwirtschaftlichen Förderungsmaßnahmen vorgeschrieben. Ziel dieses Kontrollsystems ist es, den ungerechtfertigten Bezug von europäischen Agrarförderungsmitteln festzustellen oder zu verhindern. Nach diesen Verordnungen ist zunächst ein Kataster der landwirtschaftlich genutzten Flächen mit den darauf befindlichen Kulturen zu erstellen - für die die Landwirte Beihilfen erhalten - und sodann die Einhaltung dieser Vorgaben zu überwachen. Diese Überwachung erfolgt derzeit durch stichprobenweise Nachschau vor Ort durch Beamte der Landwirtschaftsbehörde.

Die Kontrolle soll in Zukunft durch DV-gestützte Systeme erfolgen, durch die Doppelangaben ausgeschlossen werden, und durch Fernaufklärung aus dem Weltraum. Diese Satellitenaufklärung macht es möglich, die tatsächlichen Anbauflächen mit einer hohen Genauigkeit nachzuprüfen und dabei festzustellen, welche Nutzungsart (Milchwirtschaft, Forstwirtschaft oder Art der Kulturpflanze) angebaut wird. Abweichungen zu dem Förderantrag lassen sich auf diese Weise unschwer ermitteln.

Ich halte die flächendeckende Erfassung in dieser Form für einen unverhältnismäßigen Grundrechtseingriff; es werden u. a. zahlreiche Daten (z.B. Gebäudeflächen von privaten Haushalten, private Schwimmbäder, Nutzung von Gärten) miterhoben, die nicht benötigt werden, da die betroffenen Grundstückseigentümer entweder keine Förderung beantragt haben oder aber nicht unter die Förderprogramme fallen. Die Konferenz der Datenschutzbeauftragten hat in einer Entschließung vom Oktober 1993 die wichtigsten Anforderungen an ein grundrechtskonformes Kontrollsystem im Agrarbereich zusammengefaßt (vgl. Ziff. 15.7).

In Bremen sollen diese Daten im Auftrag des Senators für Wirtschaft, Mittelstand und Technologie von der Landwirtschaftskammer erhoben und bis zum Bewilligungsbescheid aufbereitet werden. Die Durchführung von Abgleichs- und Kontrollmaßnahmen ist jedoch im Landwirtschaftskammergesetz nicht vorgesehen, so daß eine derartige Aufgabenübertragung rechtlich - auch datenschutzrechtlich - abgesichert werden muß. Gleichwohl habe ich mit der senatorischen Dienststelle und der Landwirtschaftskammer Bremen erste Gespräche zur Entwicklung eines Datenschutzkonzeptes geführt.

10. Senator für Finanzen

10.1. Fall: Freibeträge auf der Steuerkarte und medizinische Daten

Viele Lohnsteuerpflichtige machen von der Möglichkeit Gebrauch, bestimmte Freibeträge in ihre Lohnsteuerkarte eintragen zu lassen, um bereits im Laufe des Kalenderjahres in den Genuß entsprechender Steuerreduzierungen zu kommen. Freibeträge gibt es auch für Körperbehinderung. Durch die Eintragung des Freibetrages in der Lohnsteuerkarte erhält der Arbeitgeber ihm sonst nicht ohne weiteres zugängliche Zusatzinformationen (z. B. über den Grad der Erwerbsminderung), die ggf. auch Grundlage für arbeitsrechtliche Maßnahmen werden könnten. Regelmäßig gelten die Freibeträge mehrere Jahre und die Finanzämter unterrichten daher die Lohnsteuerkartenstellen, um bei einer Folgekarte den entsprechenden Freibetrag zu vermerken.

Ich weise regelmäßig die betroffenen Arbeitnehmer auf die Möglichkeit hin, daß sie auf dem entsprechenden Antragsformular dieser Mitteilung widersprechen können. Die Finanzämter sind ihrerseits gehalten, darauf aufmerksam zu machen, daß den Steuerpflichtigen freigestellt ist, ob der Freibetrag vorgetragen wird oder nicht.

10.2. Fall: Religionsmerkmale auf der Lohnsteuerkarte

Auf der Lohnsteuerkarte stehen nicht nur Angaben zur Person des Steuerpflichtigen und zu seiner Steuerklasse, sondern auch zu seiner Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft. Dies ist durch das Kirchensteuerrecht und die für das Verhältnis zwischen Staat und Kirche fortgeltenden Regelungen der Weimarer Reichsverfassung geregelt. Diese Vorschriften enthalten jedoch keine Ermächtigung zur Eintragung der Religionszugehörigkeit auch des Ehepartners. Eine Notwendigkeit für die Verrechnung der Kirchensteuer zwischen den öffentlich-rechtlichen Religionsgesellschaften besteht nicht, wenn beide Partner der gleichen Kirche angehören oder der Partner des Steuerpflichtigen Mitglied keiner Kirche, einer nicht anerkannten Glaubensgemeinschaft oder einer Freikirche ist. In diesen Fällen bedarf es dementsprechend auch keiner Eintragung des konfessionsverschiedenen oder konfessionslosen Ehegatten.

Aufgrund mehrerer Eingaben habe auch ich - wie eine Reihe meiner Kollegen - auf eine entsprechende Änderung der Handhabung bei der Ausfüllung der Lohnsteuerkarten gedrängt. Die zuständigen Referenten der Finanzressorts von Bund und Ländern sind inzwischen übereingekommen, ab 1995 so zu verfahren.

10.3. Fall: Scheidungsurteil an das Finanzamt

Steuerpflichtige sind nach dem Einkommensteuergesetz und den dazu erlassenen Richtlinien verpflichtet, ihre Steuerkarte ändern zu lassen, wenn sie "in Trennung leben". Ein Bürger, der sich an mich wandte, hatte - aus welchen Gründen auch immer -, diese Änderung nicht rechtzeitig vorgenommen. Als er zwei Jahre später - nach bereits erfolgter Scheidung - das Urteil vorlegte, fertigte die Sachbearbeiterin bei der Lohnsteuerkartenstelle des Magistrats der Stadt Bremerhaven ohne Kenntnis des Betroffenen eine Fotokopie von den wesentlichen Seiten und übersandte diese mit einem Anschreiben, in dem auf das Trennungsdatum im Urteil hingewiesen wurde, an das Finanzamt Bremerhaven.

Bei einer Einsicht in die Steuerakte bekam der Betroffene von diesem Vorgang Kenntnis. Die Sachbearbeiterin berief sich auf ihre Unterrichtungspflicht gegenüber dem Finanzamt.

Sie war sich aber nicht bewußt, daß sie mit den Ablichtungen weit über das erforderliche Maß hinaus Daten übermittelt hat. Nach meiner Intervention hat das Finanzamt Bremerhaven die Lohnsteuerkartenstelle angewiesen, zukünftig von Scheidungsurteilen oder ähnlichen Dokumenten keine Kopien mehr anzufertigen, sondern ein evtl. eingetragenes Trennungsdatum nur im Anschreiben zu vermerken.

10.4. Datensicherung beim Haushalts- und Mittelbewirtschaftungssystem (HIS-MBS) - Realisierung einer Netzwerklösung

Im Rahmen einer Neugestaltung des bremischen Haushalts-, Kassen- und Rechnungswesens (HKR), die eine Optimierung dieser Verfahren in einem Gesamtverfahren für das "integrierte bremische Finanzwesen" vorsieht, wird das Softwareprodukt "Mittelbewirtschaftungssystem HIS-MBS" eingesetzt. Die vorliegende Version bietet Unterstützung bei der Führung der Haushaltsüberwachungslisten, bei der Mittelbewirtschaftung und beim Druck von Kassenanordnungen.

Ein von mir vorgenommener Test der neuen Einzelplatzversion 4.1 HIS-MBS und der Netzversion 4.2 ergab, daß die bereits im letzten Jahresbericht (vgl. 15 JB, Ziff. 13.2) festgestellten Mängel hinsichtlich der inneren Logik der Paßwort- und Rechteorganisation bis auf die folgende geringfügige Änderung in der Netzversion nicht beseitigt worden sind:

Der sogenannte "privilegierte Sachbearbeiter (01)", der Systemverwalterfunktionen wahrnimmt, ist nicht mehr in der Lage, die Paßworte der anderen Nutzer/-innen einzusehen.

Dennoch erfüllt das System aufgrund folgender Mängel weiterhin nicht die erforderlichen datenschutzrechtlichen Anforderungen:

- Für alle Nutzer/-innen (incl. 01) ist das Einloggen in das System über ein einziges Paßwort möglich, d.h. die erforderliche individuelle Benutzeridentifikation wird vom System nicht gewährleistet.

- Auch wenn der "privilegierte Sachbearbeiter" die Paßworte der anderen Nutzer/-innen nicht mehr einsehen kann (s.o.), müssen diese immer noch die Zugangsberechtigung zum Verwaltungsmenue haben, um das zugewiesene Paßwort durch ein individuelles ersetzen zu können.

- Verweigert der "privilegierte Sachbearbeiter" den Zugang zum Verwaltungsmenue, ist der Nutzer/die Nutzerin gezwungen, unter dem zugewiesenen Paßwort zu arbeiten.

- Ohne Zugang zum Verwaltungsmenü ist auch die erforderliche physische Löschung der Daten, die in der Einzelplatzversion ohnehin nur der "privilegierte Sachbearbeiter" veranlassen kann, nicht möglich.

- Vergibt der "privilegierte Sachbearbeiter" jedoch die entsprechende Zugangsberechtigung, so ist gleichzeitig der Zugang zum Duplizieren der vorliegenden Originaldateien offen, d.h. jeder Nutzer/jede Nutzerin kann diese Daten unkontrolliert weiterverarbeiten.

- In bezug auf Leistungskontrollen bleiben die Auswertungsmöglichkeiten bestehen (Art, Anzahl, Daten der Buchungen eines bestimmten Sachbearbeiters aus der Datei "Huel.dbf" etc.). Durch Einsichtnahme in ein entsprechendes Fenster bei der individuellen Paßworteingabe kann jeder Nutzer/jede Nutzerin die Zuordnung von Benutzernummern u. -namen erkennen, so daß hier der Personenbezug für etwaige Auswertungen durch jeden Systemnutzer/jede Systemnutzerin direkt herstellbar ist, sofern er nicht schon bekannt ist.

Es ist erforderlich, diese Mängel durch Entwicklung und Integration eines eigenen Moduls zur Paßwortverwaltung sowie durch eine entsprechende Konfiguration der mit "HIS-MBS" einzusetzenden Datenschutzsoftware zu beheben.

Als organisatorische Maßnahme wurde vom Senator für Finanzen eine "Rahmendienstanweisung für den Einsatz eines einheitlichen Programms für Haushaltsüberwachung und Mittelbewirtschaftung für PC" mit meiner Beteiligung erstellt.

Sie enthält u.a. folgende für den Datenschutz wesentlichen Punkte:

- Die Landeshauptkasse teilt mir die das System nutzenden Dienststellen auf Aufforderung, mindestens jedoch einmal im Jahr mit.

- Das Verfahren darf nur in Verbindung mit der Sicherheitssoftware Safeguard eingesetzt werden.

- Für den Einsatz vor Ort sind in einer Dienstanweisung folgende Punkte festzulegen:

  - Verantwortlichkeiten für den Systemeinsatz (grundsätzlich gekoppelt an die Funktion "Beauftragter für den Haushalt"),

  - Vier-Augen-Prinzip bei Änderung von Nummern, Name und Paßwort,

  - Definition der Inhalte der Freitextfelder,

  - Index-und Dateistrukturen sowie die Zuständigkeit für durch Indizes gesteuerte Auswertungen.

Das Hafenamt und das Stadtamt planen den Einsatz von "HIS-MBS" im Netz. Neben der Beseitigung der oben genannten Mängel ist hierfür der Einsatz eines Netzwerkbetriebssystems erforderlich, das eine adäquate Abschottung der Haushaltsdaten von anderen auf dem Server verwalteten Datenbeständen ermöglicht.

Die Auswahl des Netzwerkbetriebssystems sowie die Organisation der Zugriffe muß die Mindestanforderungen an PC-Netze (vgl. 15. JB, Ziff. 2.2.1.1) erfüllen und die Ergebnisse des Pilotprojektes Netze (vgl. Ziff. 2.3.4), insbesondere das Verhältnis der Art der auf dem Server verwalteten Daten zum erforderlichen Sicherheitsumfang des Betriebssystems, berücksichtigen.

10.5. Verfahren VERBIS - Veranlagung am Bildschirm

Die Oberfinanzdirektion Bremen (OFD) ist wegen Überalterung der bisherigen Technik gezwungen, diese zu ersetzen. Die Hard- und Software des alten Systems entsprechen nicht mehr ergonomischen Anforderungen; es gibt keine Ersatzteile und damit auch keine sichere Wartungsmöglichkeit mehr.

Mit dem neuen Konzept geht die Steuerverwaltung den Weg zu einer ganzheitlichen Bearbeitung der Steuerdaten. Die Angaben der Steuerpflichtigen werden nur einmal erfaßt, von dem System geprüft und berechnet sowie in Form eines Steuerbescheides ausgewertet. Die Steuerverwaltung erhofft sich eine schnellere Erledigung der Steuerfälle, eine höhere Flexibilität und eine größere Unterstützung der Steuerbeamten.

VERBIS soll in den Veranlagungsbereichen der bremischen Finanzämter eingesetzt werden und im Endausbau ca. 1.000 Arbeitsplatzrechner, ein Netzwerk mit entsprechenden Servern und Anschlüsse an den Host (Großrechner) des Rechenzentrums der bremischen Verwaltung (RbV, seit 01.01.1994 "Informations- und Datentechnik Bremen - BremID") umfassen. Das äußerst komplexe System besteht danach aus verschiedenen Ebenen:

1. Ebene: Arbeitsplatzrechner

   Es handelt sich um einen gewöhnlichen PC, mit dem der Steuerbeamte Schriftstücke erstellen und Berechnungen oder Auswertungen vornehmen kann.

2. Ebene: Netzebene

   Die Netzebene stellt den PCs neben den o. a. Standardprogrammen Programme für die Veranlagung am Bildschirm, für die Kommunikations- und Zugriffsverwaltung sowie für die Verschlüsselung und Protokollierung zur Verfügung. Die Speicherung der Steuerdaten erfolgt sowohl auf der Netzwerkebene - für bestimmte Verarbeitungsschritte - als auch auf der

3. Ebene, d. h. im Großrechner der BremID (früheres RbV).

   Er dient der DV-technischen Produktion, d.h. die Steuerdaten werden dort gerechnet, ausgewertet und gesichert sowie die Steuerbescheide ausgedruckt und versandfertig gemacht.

Das neue System befindet sich derzeit in der Ausschreibungsphase. Vor der Ausschreibung hat mich die OFD beteiligt. Meine Aufgabe besteht darin, mit der OFD ein schlüssiges Datenschutzkonzept zu entwickeln und später zu implementieren, dessen Anforderungen bereits bei der Entscheidung über die Erteilung des Zuschlags zu berücksichtigen sind.

Bei der Ausgestaltung von VERBIS muß auch die Geltung des Steuergeheimnisses zwischen und innerhalb der Finanzämter beachtet werden. Daten der Steuerpflichtigen sind auch zwischen den Finanzämtern nicht beliebig austauschbar; vielmehr hat jeder Steuerbeamte auch gegenüber seinen mit der konkreten Veranlagung nicht befaßten Kollegen das Steuergeheimnis zu wahren und darf Steuerdaten nur offenbaren, wenn § 30 der Abgabenordnung oder eine andere Steuervorschrift es zuläßt. Entsprechend zu konfigurieren sind daher die Datensicherungsvorkehrungen, d. h. die Zugriffsbefugnisse, Datenarten und Protokollierungen.

10.6. Lockerung des Steuergeheimnisses statt datenschutzkonformer AO-Novellierung

In den letzten Jahren wurden immer wieder Anläufe zur Schaffung von bereichsspezifischen Datenschutzregelungen in der Abgabenordnung (AO) genommen. Die Datenschutzbeauftragten haben sich nachhaltig für eine präzisere und zeitgemäßere Ausgestaltung des Steuergeheimnisses sowie für klare Vorgaben für die Speicherung und Nutzung von Steuerdaten ausgesprochen und immer wieder zu den verschiedenen Referentenentwürfen das Bundesfinanzministeriums Stellung genommen (vgl. 13. JB, Ziff. 2.10.1). Überraschenderweise hat 1993 das Ministerium die geplante umfassende Neuregelung - zumindest für die laufende Legislaturperiode - für entbehrlich erklärt. Während die Datenschutzbeauftragten noch die neuesten AO-Entwürfe diskutierten, brachte der Bundesminister der Finanzen einige ihm wichtig erscheinende Verarbeitungswünsche im Gesetz zur Bekämpfung des Mißbrauchs und zur Bereinigung des Steuerrechts (StMBG) unter.

Die Finanzbehörden dürfen jetzt u. a. Grundsteuerdaten an die Kommunen nicht nur zur Erhebung der Grundsteuer und damit verbundener Abgaben mitteilen, sondern auch zur Erfüllung sonstiger Aufgaben der öffentlichen Verwaltung. Zu diesen Zwecken dürfen die Daten auch an andere öffentlich-rechtliche Körperschaften übermittelt werden. Damit wird der Datenbestand der Steuerverwaltung für externe Nutzungsinteressen ohne Rücksicht auf die Zweckbindung weit geöffnet, z. B. auch für Planungen der Abwasserentsorgung, des Straßennetzes, des Wohnungsbaus oder von Umweltmaßnahmen.

Angaben dürfen über die konkrete Veranlagung hinaus jetzt auch genutzt werden, um Vergleichsdaten für zukünftige Steuerverfahren zu gewinnen. Mit einer derart weit gefaßten Norm kann man vielfältige Auswertungen legitimieren. Eingeführt wird gleichsam eine Speicherung auf Vorrat für den Fall, daß künftig ein abweichendes steuerrelevantes Verhalten erkennbar wird oder werden könnte. Die Kontrolldichte wird damit ohne klare Definition der Kontrollanlässe und -zwecke verstärkt, das Prinzip der Erhebung beim Betroffenen weiter ausgehöhlt.

In der nächsten Legislaturperiode werde ich mich dafür einsetzen, daß es eine neue Initiative für die Einführung eines umfassenden Sonderschutzes für die sensiblen Daten in der Finanzverwaltung geben wird.

11. Rechnungsprüfungsamt Bremerhaven

11.1. Online-Abruf für die Rechnungsprüfung

Gegenüber dem Magistrat der Stadtgemeinde Bremerhaven habe ich Stellung genommen zum gewünschten Direktabruf von Daten aus den Bereichen Personalwesen und Ordnungswidrigkeiten durch das Rechnungsprüfungsamt. Der Magistrat war der Auffassung, da § 12 Abs. 3 BrDSG eine Zweckänderung für die Rechnungsprüfung ausdrücklich zuläßt, könne auch ein online-Anschluß an DV-Verfahren der Verwaltung ohne weitere Voraussetzungen eingerichtet werden.

Ich habe dagegen eingewandt, daß ungeachtet der Zulässigkeit der Zweckänderung die Datenweitergabe vom Fachamt an das Rechnungsprüfungsamt eine Übermittlung darstellt. Datenübermittlungen mittels automatisierter Abrufverfahren sind aber nach § 14 Abs. 2 BrDSG nur zulässig, wenn der Direktabruf für die Aufgabenerfüllung der beteiligten Stellen angemessen ist und ausreichende Vorkehrungen zum Schutz des informationellen Selbstbestimmungsrechts des betroffenen Personenkreises getroffen wurden. In einer Rechtsverordnung müssen der Datenempfänger, die Datenart, die abgefragt werden soll, und der Zweck des Abrufs festgelegt werden.

Der Senator für Finanzen hat mir daraufhin die Entwürfe zu zwei entsprechenden Rechtsverordnungen vorgelegt. Ich habe zunächst die Kompetenz des Senators für Finanzen zum Erlaß dieser Verordnungen in Zweifel gezogen. Kritisiert habe ich weiter die undifferenzierte Abrufmöglichkeit im Hinblick auf die Einhaltung des Verhältnismäßigkeits- und Angemessenheitsgrundsatzes. Auch habe ich zum Ausdruck gebracht, daß eine Ermächtigungsnorm für entsprechende Rechtsverordnungen, z. B. in der Landeshaushaltsordnung, geschaffen werden müßte. Nach Auffasung des Senators für Justiz und Verfassung reicht jedoch § 14 Abs. 2 BrDSG als Verordnungsermächtigung aus. Diese Frage muß bei der anstehenden Novellierung des Bremischen Datenschutzgesetzes geklärt werden.

12. Häfen, Schiffahrt und Außenhandel

12.1. Betriebskostenmodul beim Hansestadt Bremischen Amt Bremerhaven

Das Hansestadt Bremische Amt Bremerhaven (HBA) ist eine Behörde, die die Kommunalaufgaben der Stadtgemeinde Bremen in Bremerhaven wahrnimmt, d.h. sie ist zuständig für alle Verwaltungsaufgaben im bremischen Teil Bremerhavens. Damit fallen in einer Behörde viele Aufgaben zusammen, die in der Stadtgemeinde Bremen verschiedenen Verwaltungsbehörden übertragen sind. So ist das HBA nicht nur Hafenbehörde, sondern auch z. B. Bauordnungsamt, Wasser- und Umweltbehörde oder auch eine verwaltungspolizeiliche Behörde. Diese Konstruktion verlangt bei der DV-Ausstattung besondere Datenschutzkonzepte. Die zuständigen Mitarbeiter haben dieses erkannt und beteiligen mich sehr früh an neuen Entwicklungen und Vorhaben. Derzeit plant das HBA den Einsatz eines Betriebskostenmoduls, um die personalwirtschaftlichen und materiellen Ressourcen kontinuierlich zu erfassen und zu verarbeiten.

Die Personaldatenverwaltung erfordert hierbei besonders differenzierte und effiziente Datenschutzmaßnahmen. Technische Datenschutzkomponenten wurden bereits bei der Programmentwicklung berücksichtigt und in die Software integriert. Die Vorbildfunktion dieser Vorgehensweise besteht darin, daß Sicherheitslücken bereits auf Programmebene und nicht erst nachträglich durch zusätzliche Implementierung von Sicherheitsmodulen geschlossen werden. Die in Eigenentwicklung erstellte Personalsoftware des HBA stellt eine Lösung für die Aufgabenstellungen Stammdatenverwaltung, Lohnstundenschreibung und Kostenermittlung dar.

Bei der Stammdatenverwaltung und Lohnstundenschreibung handelt es sich um zwei eigenständige Programme. Das Programm Lohnstundenschreibung ermöglicht die Erstellung monatlicher Lohnabrechnungen für Arbeitnehmer und die Erfassung von Lohnkosten für die Kostenermittlung. Das Programm Stammdatenverwaltung ermöglicht die Verwaltung und Aktualisierung von Personaldaten der HBA-Mitarbeiter.

Die Personaldaten werden durch folgende software-technische Maßnahmen geschützt:

- Spezieller Zugangsschutz

  Die Programme sind durch einen integrierten Paßwortschutz vor unbefugtem Aufruf geschützt (Speicherung in verschlüsselter Form, jederzeitige Änderbarkeit durch zugriffsberechtigte Anwender), d.h. es besteht eine von anderen Schutzmechanismen (gegeben durch die Schutzsoftware "Safe-Guard", Rechner-Paßworte und Netzbetriebssystemsoftware) unabhängige zusätzliche Schutzstufe.

- Online-Verschlüsselung der Datenbestände

  Die Datenbestände der Personalsoftware werden hinreichend durch eine Onlineverschlüsselung aller wichtigen Datenfelder geschützt.

  Der Schutz hindert nach dem Programmaufruf jeden, mit anderen Programmen, die das Datenbankformat weiterverarbeiten können (wie z.B. das Programm Q+E, das zum Lieferumfang von Excel gehört), unbefugte Auswertungen von Personaldaten vorzunehmen.

  In entschlüsselter Form liegen die Daten nur im Arbeitsspeicher vor, d.h. bei einer Programmunterbrechung kann nicht auf entschlüsselte Daten zugegriffen werden.

  Damit ist sowohl ein zusätzlicher Schutz gegen unberechtigten Zugriff Dritter (bei eventueller Überwindung sämtlicher das Programm schützender Mechanismen) als auch der Schutz vor unbefugter Verarbeitung durch zugriffsberechtigte Personen gewährleistet.

- Keine Verwendung von Freitextfeldern

Die direkte Integration technischer Datenschutzmaßnahmen in die vom HBA entwickelte Personalsoftware stellt eine an den Funktionsumfang und die Datenbasis optimal angepaßte Datenschutzlösung dar.

Es ist geplant, die Personalsoftware in ein Netz zu integrieren, das eine Kostenermittlung und somit Kostenkontrolle der einzelnen Betriebsbereiche des HBA ermöglichen soll. Um die Kostenermittlung zu erstellen, wurde eine Individualsoftware entwickelt, die dafür erforderliche Daten aus den Bereichen Lager, Beschaffungsstelle, Haushaltswesen und Personalstelle verarbeitet.

Aus dem Programm Lohnstundenschreibung werden allgemeine Lohnkostendaten in die Kostenermittlung exportiert, die keine individuellen Rückschlüsse ermöglichen.

Die Konfiguration der Sicherheitskomponenten des Novell-Betriebssystems soll die höchste Sicherheitsstufe für die Personaldaten ermöglichen, d.h. der Anwender der Kostenermittlung wird nur Zugriff auf eine Datei erhalten, die lediglich objektbezogene Lohnkostendaten erhält.

Das Datenschutzkonzept ist zu gegebener Zeit um die Konfiguration der Zugriffsorganisation unter dem Netzwerkbetriebssystem zu ergänzen.

13. Nicht-öffentlicher Bereich

13.1. Ladendiebstahlsdatei

Eine Arbeitsgemeinschaft des Einzelhandels hat sich an die Datenschutzbeauftragten und die Aufsichtsbehörden gewandt und um Klärung gebeten, in welchem Umfang und durch wen Daten aus bzw. über Ladendiebstahlsanzeigen durch private Stellen erfaßt, abgeglichen und sonst verarbeitet werden dürfen. Ich habe diese Anfrage zum Anlaß genommen, das Problem mit den anderen Obersten Aufsichtsbehörden für den Datenschutz im Düsseldorfer Kreis zu erörtern.

Auch wenn lediglich verdächtige Personen nicht gespeichert werden sollen, sondern nur solche, die eines Ladendiebstahls auch überführt sind, ist genau zu prüfen, zu welchen konkreten Zwecken welche Daten - mit oder ohne zusätzliche Hinweise auf eine Einstellungsentscheidung nach den §§ 153, 153 a StPO - ab wann und wie lange verarbeitet werden sollen.

Soweit eine primär auf Zwecke der Strafverfolgungsbehörden und der Gerichte abzielende Datenverarbeitung und -nutzung gleichsam für diese Stellen entweder unternehmensintern oder unternehmensübergreifend wahrgenommen werden soll, bestehen erhebliche Bedenken. Es ist Sache der Strafverfolgungsbehörden und der Gerichte, sich auf der Grundlage der einschlägigen gesetzlichen Regelungen die ihnen erforderlich erscheinenden Daten zu beschaffen. Insoweit ist auch nicht erkennbar, daß eine (parallele) Datensammlung und -verwertung durch private Unternehmen zur Wahrung "öffentlicher Interessen" (§ 28 Abs. 2 Nr. 1 BDSG) erforderlich ist.

Die Zulässigkeit könnte sich danach allenfalls im Hinblick auf die Wahrnehmung eigener berechtigter Interessen des jeweiligen Unternehmens unter Abwägung mit schutzwürdigen Interessen des Betroffenen ergeben (vgl. § 28 Abs. 1 Satz 1 Nr. 2 BDSG).

Soweit vorbehaltlich einer positiven Beantwortung der o. a. Zulässigkeitsfragen eine unternehmensinterne Speicherung und Nutzung von Angaben über Ladendiebe zur Wahrnehmung eigener Rechte des jeweils betroffenen Unternehmens legitimiert werden kann, z. B. zur Durchsetzung von Hausverboten o. ä., bestehen gleichwohl gegen die Übermittlung an andere Firmen, sei es unmittelbar oder über eine dritte Institution wie einen Verband o. ä., erhebliche Bedenken. Insbesondere in Fällen der Einstellung der §§ 153, 153 a StPO bestünde bei einer Mitteilung an Dritte die Gefahr, daß ein unzutreffendes Bild über den Betroffenen vermittelt wird.

Nach meiner Auffassung steht der Speicherung von Angaben über strafbare Handlungen in zentralen Ladendiebstahlsdateien für eine Vielzahl verschiedener Unternehmen § 29 Abs. 1 Satz 1 Nr. 1 BDSG entgegen. Während die Verarbeitung derartiger Hinweise als zusätzliche Information zu bereits registrierten Personen durch Kreditinformationssysteme und Detekteien im Einzelfall zulässig sein kann, beeinträchtigen Dateien, in denen allein Vorstrafen registriert werden, schutzwürdige Interessen der Betroffenen. Durch solche Dateien wird das sorgfältig abgestimmte Schutzsystem des Bundeszentralregistergesetzes (BZRG), das die Zulässigkeitsvoraussetzungen einschließlich der Tilgungsfristen in diesem sensiblen Bereich detailliert regelt, faktisch außer Kraft gesetzt. Die Resozialisierung der Betroffenen, eines der Hauptziele des Bundeszentralregisters, wäre gefährdet.

13.2. Inkassodaten für Auskunfteizwecke

Mehrere Eingaben betrafen wie in früheren Jahren (vgl. 11. JB, Ziff. 6.3.1; 12. JB, Ziff. 4.7.2) die Nutzung von Daten, die einer großen deutschen Auskunftei im Rahmen ihrer Inkassotätigkeit bekannt geworden waren, für Auskunfteizwecke. Ich habe diese systemtechnische und informationelle Verquickung zweier unterschiedlicher Geschäftsbereiche, also des Forderungseinzuges und der kommerziellen Informationssammlung bzw. -weitergabe, wiederholt kritisiert. Auch die Obersten Aufsichtsbehörden für den Datenschutz haben zu diesem bundesweit diskutierten Problem bereits mehrfach die Auffassung vertreten, daß beide Tätigkeitsbereiche datenschutzrechtlich getrennt zu sehen und Datenflüsse zwischen ihnen als vom Bundesdatenschutzgesetz nicht gedeckte Übermittlungen zu qualifizieren sind. Dennoch hat sich die betreffende Auskunftei bislang geweigert, ihre abweichende Praxis zu ändern. Zwangsmittel zur Abstellung rechtswidriger Verarbeitungsvorgänge gibt das BDSG den Aufsichtsbehörden nicht.

Eine Reihe von Petenten beklagte sich auch darüber, daß einzelne Auskunfteien ihrer nach § 33 BDSG bestehenden Benachrichtigungspflicht nicht oder nicht vollständig nachkommen. Nach § 33 Abs. 1 Satz 2 BDSG müssen die Betroffenen über die erstmalige Übermittlung ihrer Daten unterrichtet werden. Die Information muß auch die "Art der übermittelten Daten" umfassen, d. h. die Betroffenen müssen Rückschlüsse auf die Gesamtheit der von der Auskunftei über sie gespeicherten Angaben ziehen können. In den mir bekannt gewordenen Fällen enthielten die Benachrichtigungsschreiben Formulierungen (z. B. "Bei den über Sie gespeicherten Informationen handelt es sich insbesondere um Angaben wie..."), aus denen nicht der gesamte Datenkatalog erkennbar ist.

Ich habe die in den jeweiligen Eingaben genannten Auskunfteien angeschrieben, sie auf die Rechtslage hingewiesen und um deren künftige Berücksichtigung gebeten.

13.3. Fall: Registrierung bei Bankbesuchen - Konsequenzen des Geldwäschegesetzes

Ende November 1993 trat das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten, kurz Geldwäschegesetz (GwG) genannt, in Kraft. Bereits einen Tag später beschwerte sich ein Bürger, der bei einer Sparkasse für den geplanten Kauf eines Haushaltsgerätes mehrere kleine Scheine in einen Tausend-Mark-Schein umwechseln wollte, darüber, daß er aufgefordert worden sei, sich zuvor durch Ausweispapiere zu identifizieren.

Der Filialleiter der Sparkasse hat zwar öffentlich erklärt, es habe sich dabei nicht um eine Maßnahme nach dem Geldwäschegesetz gehandelt, sondern um eine Verfahrensweise, um Nichtkunden von häufigem Geldwechseln abzuhalten. Gleichwohl habe ich diesen Vorgang zum Anlaß genommen, mich mit der geplanten Umsetzung des Geldwäschegesetzes bei einzelnen meiner Kontrolle unterliegenden Kreditinstituten zu informieren. Nach dem Geldwäschegesetz treffen die Kreditinstitute

- Identifizierungspflichten, u. a. nach § 2 allgemein bei der Annahme oder Abgabe von Werten in der Höhe von DM 20.000,-- und mehr oder nach § 6 in Verdachtsfällen, wenn ein Institut Tatsachen feststellt, die darauf schließen lassen, daß die vereinbarte Finanztransaktion einer Geldwäsche nach § 261 des Strafgesetzbuches dient oder im Falle ihrer Durchführung dienen würde;

- Aufzeichnungspflichten;

- Aufbewahrungspflichten;

- Anzeigepflicht bei sonstigen Verdachtsfällen (§ 11).

Bei meiner Nachfrage habe ich feststellen können, daß die jeweiligen Kreditinstitute dazu auf der Grundlage der von ihren Verbänden erstellten Empfehlungen dezidierte Anweisungen erlassen haben. Neben den Anweisungen sind zum Teil Formblätter entwickelt

worden, u. a. für die Identifizierung, die Meldung von Verdachtsfällen nach § 11 GwG und die eingeschränkte Aufzeichnung bei Personen wie Kassen- oder Geldboten, die regelmäßig für Firmen größere Beträge einzahlen oder abheben.

Schließlich haben einige Institute "Geldwäschebeauftragte" eingesetzt, die die Fälle, in denen eine Anzeige an die zuständigen Strafverfolgungsbehörden ergehen soll, noch einmal genau daraufhin überprüfen sollen, ob die Voraussetzungen des Geldwäschegesetzes gegeben sind.

Nach öffentlichen Darstellungen des Leitenden Oberstaatsanwalts sind den Strafverfolgungsbehörden in den zwei Monaten nach dem Inkrafttreten des Gesetzes lediglich fünf Fälle gemeldet worden. Gleichwohl gehe ich davon aus, daß insbesondere die Identifizierungspflichten gegenüber den Bankangestellten ein erhebliches Maß an Verärgerung bei den Kunden hervorrufen werden. Wenn darüber hinaus die Prognosen der Kreditwirtschaft zutreffen, daß pro Jahr schätzungsweise 50 Millionen Vordrucke auszufüllen seien, wird sich bei den Banken und Sparkassen ein erheblicher Papier- und Datenberg sammeln. Ich werde die Anwendung des neuen Gesetzes sowohl bei den Geldinstituten als auch bei den Strafverfolgungsbehörden aufmerksam beobachten. Sobald ausreichend Erfahrungen vorliegen, muß auch die Geeignetheit der vom GwG getroffenen Maßnahmen zur Eindämmung illegaler Geldwäsche insgesamt auf den Prüfstand.

13.4. Verkauf von Arztpraxen: Einwilligung der Patienten

Auch eindeutige höchstrichterliche Urteile erfahren zuweilen eine eigenwillige Interpretation, so sie den Interessen der Interpretierenden zuwiderlaufen. Oder anders ausgedrückt: Auch Ärzte/Zahnärzte nehmen ihre beruflichen Schweigepflichten dann nicht gar so ernst, wenn ihnen daraus finanzielle Nachteile oder andere Unannehmlichkeiten erwachsen könnten.

Wie befürchtet, versuchen Ärzteorganisationen das Urteil zu umgehen, in dem der Bundesgerichtshof (BGH) unmißverständlich verlangt hat, daß Ärzte ihre Patientenunterlagen dem Käufer ihrer Praxis nur übergeben dürfen, soweit ihre Patienten dem individuell zugestimmt haben (vgl. dazu 15. JB, Ziff. 10.4). Die Zahnärztekammer Bremen hat dies in einem Beschluß ihrer Delegiertenversammlung so ausgelegt, daß der verkaufende dem kaufenden Arzt die Unterlagen ohne weiteres aushändigen dürfe, nur letzterer sie unter Verschluß halten müsse und sie nur mit Einwilligung des Patienten einsehen oder weitergeben dürfe. Demgegenüber ist daran festzuhalten, daß sich der abgebende Arzt aktiv um die Zustimmung seiner Patienten bemühen muß. Fällt die Reaktion negativ aus, darf er die Unterlagen überhaupt nicht übergeben. Erhält er keine Reaktion, darf er sie allenfalls in verschlossenem Umschlag übergeben und muß seinen Nachfolger verpflichten, diesen nur mit Einwilligung des Patienten zu öffnen oder weiterzugeben. Sind die Daten automatisiert gespeichert - womit sich die Zahnärztekammer gar nicht beschäftigt, angesichts des Trends zur EDV in Arztpraxen unverständlicherweise - so hat der abgebende Arzt entsprechende technische Sicherungsvorkehrungen zur Sperrung der Daten zu treffen.

Ich sehe mich hierin grundsätzlich in Übereinstimmung mit dem die Rechtsaufsicht über die Zahnärztekammer führenden Senator für Gesundheit, Jugend und Soziales. Dieser hatte der Kammer gegenüber insbesondere darauf Wert gelegt, daß der Arzt, dem der Patient im Vertrauen auf dessen Berufsgeheimnis seine Daten anvertraut hatte, nicht ohne weiteres aus seiner Schweigepflicht entlassen werden dürfe. Ich gehe davon aus, daß der Senator für Gesundheit, Jugend und Soziales den Beschluß der Zahnärztekammer nicht genehmigt und weiterhin die Vorstellung verfolgt, in das Heilberufsgesetz die Verpflichtung der Ärzte- und Zahnärztekammer aufzunehmen, in ihren Berufsordnungen Regelungen zu treffen, die das höchstrichterliche Urteil umsetzen.

Diese Forderung gilt auch für die Wahrung der ärztlichen Schweigepflicht bei der Übermittlung der Daten von Privatpatienten zwecks Honorareinziehung an Verrechnungsstellen (vgl. 14. JB, Ziff. 3.6). Auch hier hatte der BGH eindeutig entschieden: Ohne Einwilligung des Patienten verstößt der Arzt gegen seine Schweigepflicht. Einen originellen

Ausweg hat ein Bremer Arzt zu finden geglaubt, der trotz ausdrücklichen Widerspruchs eines Patienten die Honorarabrechnung durch die Privatärztliche Verrechnungsstelle veranlaßt hatte. Er schickte - durch den Patienten auf seinen Widerspruch aufmerksam gemacht - ihm einfach die Rechnung noch einmal zu, ersetzte lediglich den Briefkopf der Verrechnungsstelle durch den seinen, gab aber weiterhin Telefonnummer und Bankkonto der Verrechnungsstelle an. Das gleiche wiederholte er bei einer weiteren Rechnung. Der Arzt entschuldigte sich damit, die Herausnahme der ersten Rechnung aus der für die Verrechnungsstelle bestimmten Diskette sei "ohne vertretbaren Mehraufwand nicht machbar" gewesen, bei der zweiten Rechnung seien der Verrechnungsstelle die Daten des Patienten versehentlich übermittelt worden. Beides sind Behauptungen, die ich nicht widerlegen kann, die aber Unbehagen und Mißtrauen erwecken. Die Privatärztliche Verrechnungsstelle hat sich erstaunt dazu geäußert, daß ich der Sache überhaupt nachgehe. Es sei der erste Fall, in dem ihr bekannt geworden sei, daß ein Patient der Abrechnung durch sie widersprochen habe. Dies kann man auch anders herum sehen: Es ist aufschlußreich, daß gleich in diesem ersten Falle die Sache derart "schief geht".

14. Register der nach dem Bundesdatenschutzgesetz meldepflichtigen Stellen

Im Berichtsjahr habe ich erneut eine große Anzahl von Unternehmen, insbesondere Detekteien und Auskunfteien, Datenerfassungsbetriebe, Rechenzentren sowie Daten- und Aktenvernichtungsunternehmen angeschrieben und um Prüfung der Meldepflicht nach § 32 BDSG und ggf. Anmeldung ihres Unternehmens gebeten. Acht Firmen haben sich daraufhin zu dem bei mir zu Kontrollzwecken geführten Register neu gemeldet. Bei mehreren Unternehmen, die eine Pflicht zur Anmeldung verneint haben, ist aufgrund der zum Teil widersprüchlichen Angaben noch durch Prüfungen vor Ort zu klären, ob nicht doch die gesetzlichen Voraussetzungen vorliegen. Falls erforderlich, werde ich ggf. Bußgeldverfahren nach § 44 BDSG einleiten.

Insgesamt sind derzeit im Register 93 Unternehmen verzeichnet, von denen 74 in Bremen und 19 in Bremerhaven ihren Sitz haben. Einzelheiten zeigt die folgende Tabelle:

Art der Tätigkeit	insgesamt	Bremen	Bremerhaven
Speicherung personenbezogener Daten zum Zwecke der Übermittlung (z. B. Auskunfteien, Kreditinformationssysteme)	7	4	3
Speicherung personenbezogener Daten zum Zwecke der anonymisierten Übermittlung (z. B. Markt- und Meinungsforschung)	1	1	0
Verarbeitung oder Nutzung personenbezogener Daten im Auftrag als Dienstleistungsunternehmen (z. B. DV-Erfassungs- und Produktions-Betriebe)	85	69	16
Gesamt	**93**	**74**	**19**

15. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

15.1. Entschließung zur Richtlinie des Rates vom 07.06.1990 über den freien Zugang zu Informationen über die Umwelt (30/313/EWG) vom 16./17.02.1993

Im Interesse eines wirksamen Umweltschutzes hat der Ministerrat der Europäischen Gemeinschaften die Umweltinformationsrichtlinie erlassen, die jedem Bürger ein Recht auf Zugang zu den bei Behörden vorhandenen Informationen über die Umwelt gewährt. Da es nicht gelungen ist, die Richtlinie innerhalb der vorgesehenen Frist bis Ende 1992 in deutsches Recht umzusetzen, herrscht gegenwärtig Rechtsunsicherheit bei Bürgern und Behörden über den Zugang zu Umweltinformationen.

Die Konferenz der Datenschutzbeauftragten sieht in der Gewährung eines freien Zugangs zu Umweltinformationen einen wesentlichen Beitrag zu größerer Transparenz des Verwaltungshandelns. Informationsfreiheit und Datenschutz bilden dabei keinen unlösbaren Gegensatz. Die Konferenz hält es für geboten, die Arbeit am Entwurf des Umweltinformationsgesetzes (UIG) zügig zum Abschluß zu bringen. Sie begrüßt entsprechende Initiativen auf Landesebene.

In den Gesetzen sind folgende datenschutzrechtliche Grundsätze zu berücksichtigen:

Soweit Umweltinformationen auf Personen beziehbar sind, ist das Grundrecht auf informationelle Selbstbestimmung zu beachten. Deshalb sind Informationen grundsätzlich in anonymisierter oder aggregierter Form zu geben. Wenn damit das Informationsinteresse nicht erfüllt werden kann, sind Eingriffe in das Persönlichkeitsrecht nur unter klaren gesetzlichen Voraussetzungen zulässig, welche die Rechte, insbesondere die Verfahrensrechte, der Betroffenen wahren.

15.2. Entschließung zum Datenschutz bei der Privatisierung der Deutschen Bundespost Telekom und bei der europaweiten Liberalisierung des Telefonnetzes und anderer Telekommunikationsdienste vom 26./27.10.1993

Im Zuge der sog. Postreform II soll die Deutsche Bundespost Telekom - nach der dafür notwendigen Änderung des Grundgesetzes - in Form einer Aktiengesellschaft privatisiert werden. Zugleich hat der Ministerrat der Europäischen Gemeinschaften in seiner Entschließung vom 22. Juli 1993 (Amtsblatt der EG Nr. C 213 vom 6. 8. 1993) seine Entschlossenheit bekräftigt, die Monopole im öffentlichen Sprachtelefondienst (Festnetz) der Mitgliedstaaten bis zum 1. Januar 1998 zu beseitigen.

In absehbarer Zeit werden daher in Deutschland neben der "Telekom AG" auch im Telefondienst andere private Unternehmen Telekommunikationsdienstleistungen anbieten. Diese Privatisierung hat Konsequenzen für den Datenschutz, der bisher für die Deutsche Bundespost Telekom auf einem vergleichsweise hohen Niveau geregelt ist. Insbesondere das grundgesetzlich garantierte Fernmeldegeheimnis würde für private Netzbetreiber und Diensteanbieter jedenfalls nicht mehr unmittelbar gelten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für unabdingbar, daß durch die Privatisierung und Liberalisierung der Schutz der Bürger insbesondere in solchen Bereichen nicht verringert wird, die - wie der Telefondienst - der Daseinsvorsorge zuzurechnen sind. So wie bisher die konkurrierenden privaten Betreiber der Mobilfunknetze einen gleichmäßig hohen Datenschutzstandard gewährleisten müssen, hat dies auch zu gelten, wenn in Zukunft private Unternehmen im Wettbewerb miteinander stationäre Telefonnetze betreiben und entsprechende Dienste anbieten. Die Einhaltung von datenschutzrechtlichen Bestimmungen bei Telekommunikationsnetzen und -diensten muß zukünftig von einer unabhängigen Stelle nach bundesweit einheitlichen Kriterien und von Amts wegen kontrolliert werden können.

Da der Wettbewerb zwischen privaten Netzbetreibern und Diensteanbietern nicht nur national begrenzt, sondern im europäischen Binnenmarkt stattfinden wird, sind auch Rechtsvorschriften der Europäischen Gemeinschaften erforderlich, die einen möglichst hohen, einheitlichen Datenschutzstandard in der Telekommunikation gewährleisten

15.3. Entschließung zur Gewährleistung des Datenschutzes bei der Mobilkommunikation vom 26./27.10.1993

Die Verbreitung mobiler Sprach- und Datenübertragungsdienste hat in jüngster Vergangenheit stark zugenommen. So gibt es bereits jetzt in Deutschland mehr als eine Million Teilnehmer der Funktelefonnetze C und D; mit der Aufnahme des Regelbetriebs von MODACOM ist seit Juni dieses Jahres auch ein öffentlicher mobiler Datenübertragungsdienst in Deutschland verfügbar. Es ist zu erwarten, daß sich die Teilnehmerzahl mobiler Kommunikationsdienste in Zukunft weiter vergrößern wird.

Die mit der Nutzung von Mobilfunkdiensten verbundenen Vorteile gehen mit Gefährdungen für den Datenschutz einher. Neben den auch bei anderen Telekommunikationsdiensten gespeicherten Angaben, wer wann mit wem in Verbindung war, wird bei der Mobilkommunikation auch erhoben, wo sich der mobile Teilnehmer jeweils aufhält. Die Speicherung dieser Daten ermöglicht die Bildung von problematischen Bewegungsprofilen.

Darüber hinaus ist vielfach auch die Vertraulichkeit der Kommunikationsinhalte gefährdet, insbesondere dann, wenn Daten unverschlüsselt per Funk übertragen werden. Dies gilt sowohl für die analogen Funktelefon-Netze B und C als auch für den von der Deutschen Bundespost Telekom betriebenen mobilen Datenübertragungsdienst MODACOM. Bei satellitengestützten Diensten ist es sogar möglich, die übertragenen Daten im gesamten, teilweise viele tausend Quadratkilometer umfassenden Abstrahlbereich des Satelliten unbemerkt abzuhören und aufzuzeichnen.

Von den Herstellern und Betreibern mobiler Kommunikationsdienste ist zu fordern, daß sie diesen Gefahren für das Fernmeldegeheimnis und für den Datenschutz durch eine entsprechende Gestaltung entgegenwirken und technische Vorkehrungen für eine sichere Kommunikation treffen.

Die Teilnehmer mobiler Kommunikationsdienste müssen von den Anbietern, Herstellern und Betreibern über die mit der Nutzung verbundenen Risiken und das erreichte Sicherheitsniveau aufgeklärt werden. Sofern bei bestimmten Diensten Sicherheitsmerkmale realisiert sind - wie z.B. in den digitalen D-Netzen -, muß die Sicherheit für die Aufsichts- und Kontrollorgane auch nachprüfbar sein. Falls durch den Dienstbetreiber nicht die erforderliche Sicherheit gewährleistet werden kann, ist eine Übertragung personenbezogener oder sonstiger sensibler Daten mit dem jeweiligen Dienst nur dann vertretbar, wenn der Benutzer zusätzliche Sicherheitsvorkehrungen trifft, also z.B. die übertragenen Daten anwendungsseitig verschlüsselt.

Zusätzlich kompliziert wird die Datenschutzproblematik bei der Mobilkommunikation dadurch, daß unter Umständen bei verschiedenen Dienst- und Netzbetreibern, aber auch bei anderen Unternehmen - den sogenannten Service-Providern, die lediglich Dienste vermarkten -, personenbezogene Daten gespeichert werden.

Hier muß im Zuge der anstehenden Überarbeitung des Telekommunikationsrechts dafür Sorge getragen werden, daß sich die Verarbeitung der Kommunikationsdaten auf das wirklich erforderliche Maß beschränkt und daß die Nutzer darüber aufgeklärt werden, bei welcher Stelle welche personenbezogenen Daten gespeichert oder sonst verarbeitet werden.

Besonders problematisch ist es, wenn bei der internationalen Mobilkommunikation auch in solchen Staaten personenbezogene Daten gespeichert werden, in denen kein ausreichendes Datenschutzniveau gewährleistet ist oder in denen das Fernmeldegeheimnis nicht

sichergestellt wird. Deshalb ist es erforderlich, auf internationaler Ebene Regelungen zu treffen, die den Datenschutz bei mobilen Kommunikationsdiensten gewährleisten.

Die Konferenz unterstreicht aus diesem Grunde ihre Forderung, die Arbeiten an der EG-Richtlinie über Datenschutz im ISDN und in öffentlichen digitalen Mobilfunknetzen zu einem datenschutzrechtlich befriedigenden Abschluß zu bringen. Auch für den noch gänzlich datenschutzrechtlich ungeregelten Bereich der Satellitenkommunikation müssen endlich völkerrechtlich verbindliche Regelungen getroffen werden.

15.4. Entschließung zur Gefährdung der Vertraulichkeit der Funkkommunikation von Sicherheitsbehörden und Rettungsdiensten vom 26./27.10.1993

Durch die Aufhebung der bisher gültigen Beschränkungen der zulässigen Empfangsbereiche für Rundfunkempfänger zum 30. Juni 1992 werden zunehmend Empfangsgeräte betrieben, die das Abhören des Funkverkehrs ermöglichen. Dies stellt eine erhebliche Bedrohung des Fernmeldegeheimnisses dar.

Die Datenschutzbeauftragten des Bundes und der Länder beobachten die damit verbundene Gefährdung der Vertraulichkeit der Funkkommunikation von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) mit Sorge. Sie erkennen die Bemühungen der Polizeiverwaltungen der Länder an, durch zusätzliche technische Maßnahmen die Sicherheit des Sprechfunkverkehrs zu erhöhen. Sie stellen jedoch fest, daß die erforderliche Vertraulichkeit bisher nicht gewährleistet werden konnte. Auch Sprachverschleierungssysteme erreichen diese nicht hinreichend.

Daher begrüßt die Konferenz die im Rahmen des Schengener Abkommens getroffene grundsätzliche Entscheidung, im BOS-Bereich eine europäische Normierung zu erarbeiten, die die Digitalisierung und eine Verschlüsselung des BOS-Funkverkehrs vorsieht.

Die Konferenz hält es für erforderlich, daß das Normierungsverfahren so zügig wie möglich durchgeführt wird und auch schon vor der Umsetzung dieser Norm alle Möglichkeiten für einen effektiven Schutz der Vertraulichkeit des BOS-Funkverkehrs entsprechend dem jeweiligen Stand der Technik genutzt werden.

Die Konferenz weist weiter darauf hin, daß nicht nur bei den Behörden der Polizei, sondern auch in anderen BOS-Bereichen, wie z.B. dem Rettungswesen, eine Vertraulichkeit des Funkverkehrs zu gewährleisten ist. Daher sind auch in den übrigen BOS-Bereichen frühestmöglich entsprechende Absicherungen zur Vertraulichkeit des Funkverkehrs gefordert.

15.5. Entschließung zu kartengestützten Zahlungssystemen im öffentlichen Nahverkehr vom 26./27.10.1993

Mit der Weiterentwicklung von Chipkarten werden kartengestützte Zahlungssysteme zunehmend auch im Verkehrsbereich eingesetzt. Damit besteht die Gefahr, daß sehr detaillierte Bewegungsprofile entstehen, die den persönlichen Bereich jedes Einzelnen einschränken und z.B. auch für Strafverfolgungsbehörden, Finanzämter und für die Werbewirtschaft von Interesse sein könnten. Da sämtliche Fahrten für einen gewissen Zeitraum aufgelistet werden können, hat jeder Kontoinhaber die Möglichkeit, Fahrten sämtlicher Familienmitglieder jederzeit nachzuvollziehen.

So sind im öffentlichen Nahverkehr zahlreiche sogenannte Postpaid-Verfahren in Erprobung, bei denen dem Fahrgast am Monatsende die aufsummierten Fahrpreise vom Konto abgebucht werden. Diese Zahlungsweise erfordert die Speicherung umfangreicher personenbezogener Daten: Neben der Konto-Nr. und Bankleitzahl des Fahrgastes werden sowohl Datum und Uhrzeit des Fahrscheinkaufs bzw. des Fahrtantritts als auch Automatennummer und Preisstufe der jeweiligen Fahrt erhoben.

Eine solche Vorgehensweise ist umso problematischer, als technische Alternativen existieren, die weitaus datenschutzfreundlicher sind. Im öffentlichen Nahverkehr können - wie skandinavische und auch deutsche Projekte aufzeigen - Wertkartensysteme eingesetzt werden, bei denen im voraus bezahlt wird und die daher gänzlich ohne personenbezogene Daten auskommen.

Die Datenschutzbeauftragten halten es daher für dringend erforderlich, daß mehr als bisher bei der Einführung kartengestützter Zahlungssysteme darauf geachtet wird, die "datenfreie Fahrt" zu ermöglichen. Im öffentlichen Nahverkehr sollte weiterhin auch die datenschutzfreundlichste Lösung angeboten werden: Der Kauf einer Fahrkarte am Automaten mit Bargeld.

Die Konferenz fordert weiter, daß noch vor der Pilotierung der dargestellten Technikvorhaben im Verkehrsbereich eine Untersuchung möglicher Alternativen, eine Analyse der von ihnen ausgehenden Gefahren für das informationelle Selbstbestimmungsrecht und eine Darstellung der technischen und organisatorischen Möglichkeiten zur Gewährleistung des Persönlichkeitsschutzes zu erstellen ist (Technikfolgen-Abschätzung). Nur Verfahren mit dem geringsten Eingriff in das allgemeine Persönlichkeitsrecht sollten eine Chance zur Erprobung erhalten.

15.6. Entschließung zu regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ) vom 26./27.10.1993

Die öffentlich-rechtlichen Rundfunkanstalten drängen seit langem auf die Schaffung einer Rechtsgrundlage für die regelmäßige Übermittlung von Meldedaten aller Einwohner an die gemeinsame Gebühreneinzugszentrale (GEZ). Sie verweisen dazu auf bereits bestehende Regelungen in den Ländern Hessen und Nordrhein-Westfalen. Auf Bitten der Konferenz der Regierungschefs der Länder hat deshalb nunmehr der zuständige Arbeitskreis der Innenministerkonferenz einen Musterentwurf für eine bundesweite Lösung im Melderecht erarbeitet. Der Entwurf sieht vor, daß künftig alle Meldebehörden in der Bundesrepublik im Fall der Anmeldung, Abmeldung oder des Todes eines volljährigen Einwohners bis zu acht Kerndaten an die GEZ übermitteln dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen eine derartige Regelung insbesondere aus folgenden Gründen ab:

Die Regelung könnte im Ergebnis zu einem bundesweiten Melderegister bei Volljährigen führen. Sie könnte außerdem gegen das verfassungsrechtlich garantierte Verhältnismäßigkeitsprinzip verstoßen. Den Rundfunkanstalten stünde möglicherweise der unkontrollierte Zugriff auf Millionen personenbezogener Daten Volljähriger Einwohner der Bundesrepublik zu, obwohl es für die Rundfunkanstalten nur von Interesse ist, welcher Einwohner bei ihnen gebührenpflichtig ist und bislang seine Gebührenpflicht nicht angemeldet hat. Das vorgesehene generelle Übermittlungsverfahren kennt keine Unterscheidung zwischen erforderlichen und nicht erforderlichen Daten, sondern überläßt diese Unterscheidung der GEZ. Über die Frage, ob ein Volljähriger überhaupt gebührenpflichtig ist, geben die Meldedaten keine Auskunft. Das muß nach wie vor im herkömmlichen Verfahren durch Befragung ermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder sind bereit, an geeigneten und verfassungskonformen Lösungen der Landesregierungen zur Sicherung des Gebührenaufkommens der Rundfunkanstalten mitzuwirken.

15.7. Entschließung zum Integrierten Verwaltungs- und Kontrollsystem (InVeKoS) (Verordnungen der EWG Nrn. 3508/92 und 3887/92) vom 26./27.10.1993

Die vom Ministerrat der EG 1992 beschlossene Reform der gemeinsamen Agrarpolitik sieht die Angleichung der gemeinschaftlichen Preise für bestimmte Kulturpflanzen an den

Weltmarkt vor und gewährt auf Antrag als Ausgleich für die dadurch bedingten Einkommenseinbußen flächen- und tierbezogene Zuwendungen an die Erzeuger. Zur Verhinderung einer mißbräuchlichen Verwendung von Fördermitteln hat die EG die Mitgliedsstaaten dabei zur Einführung eines "Integrierten Verwaltungs- und Kontrollsystem (InVeKoS)" verpflichtet. Diese haben danach integrierte Datenbanken mit Angaben über Flurstücke, deren kulturartige Nutzung sowie den Tierbestand einzurichten und in einem Mindestumfang entsprechende Kontrollen durchzuführen.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder hat die EG mit dem "Integrierten Verwaltungs- und Kontrollsystem" den Landwirtschaftsverwaltungen der Länder ein Überwachungssystem verordnet, das dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot, widersprechen kann. Insbesondere legt das EG-Recht für die Kontrolldichte nur ein Mindestmaß an Kontrollen, jedoch keine Obergrenze fest.

Zur Vermeidung unverhältnismäßiger Einschränkungen des informationellen Selbstbestimmungsrechts der betroffenen Landwirte fordern daher die Datenschutzbeauftragten des Bundes und der Länder,

- ortsunabhängige Überwachungsmöglichkeiten (Fernerkundung mittels Satellit oder Flugzeug) nicht für eine flächendeckende Totalüberwachung einzusetzen, sondern auf den von der EG geforderten Stichprobenumfang zu beschränken;

- bei der Nutzung des Kontrollsystems InVeKoS und der darin gespeicherten personenbezogenen Daten den Grundsatz der Verhältnismäßigkeit und insbesondere der Zweckbindung zu beachten;

- nur dezentrale Datenbanken in den einzelnen Bundesländern einzurichten (keine Euro- oder Zentraldatenbank über Landwirte!), und an zentrale Datenbanken keine personenbezogenen Daten zu übermitteln;

- zu beachten, daß die EG-Verordnungen zu InVeKoS keine Rechtsgrundlage für eine Erweiterung der Nutzungen enthalten (z.B. zu Kontrollzwecken bei anderen landwirtschaftlichen Förderungsmaßnahmen oder außerhalb des landwirtschaftlichen Bereichs, z.B. zur Besteuerung).