21. Jahresbericht

des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bremischen Bürgerschaft (Landtag) und dem Präsidenten des Senats meinen 21. Bericht über das Ergebnis meiner Tätigkeit im Jahre 1998 zum 31. März 1999 (§ 33 Abs. 1 Bremisches Datenschutzgesetz – BrDSG).

Dr. Stefan Walz, Landesbeauftragter für den Datenschutz

Redaktionsschluß: 28. Februar 1999

Inhaltsverzeichnis

1. Vorwort

1.1. Modernisierung des Datenschutzes - Erwartungen und Reformbedarf

1.1.1. Erwartungen - Ergebnisse der Demoskopie

Was wissen die Bürgerinnen und Bürger "vom Datenschutz"? Welchen Institutionen und Berufsgruppen vertraut oder mißtraut die Bevölkerung? Welche Risiken ängstigen am meisten? Welche Handlungs- und Informationsdefizite werden beklagt? Wie verhalten sich von - vermeintlichem oder wirklichem - Datenmißbrauch Betroffene?

Wer Daten verarbeitet, wer Datenschutzgesetze macht, wer Datenverarbeiter überwacht - sie alle sollten diese Fragen annähernd zutreffend beantworten können, um das Recht auf informationelle Selbstbestimmung problemadäquat, risikospezifisch und zielgruppengenau sichern zu können. Um so mehr erstaunt, wie wenig Versuche es - jedenfalls in Deutschland - bisher gegeben hat, das große empirische Defizit zum Thema Datenschutz mit professioneller sozialwissenschaftlicher Methodik zu verringern.

Um so gespannter konnte man auf die Ergebnisse der im Juli 1998 vorgelegten repräsentativen **Meinungsumfrage des BAT-Freizeit-Forschungsinstituts** sein ("Der Gläserne Konsument? Multimedia und Datenschutz", Hamburg 1988). Das Institut hat 3000 Bundesbürger ab 14 Jahren nach ihren Kenntnissen, Einstellungen und Erwartungen zu Datenschutz und Datensicherheit befragt und dabei Erstaunliches zu Tage gefördert.

Zwar erscheinen dem professionellen Datenschützer auf der Grundlage seiner Praxiserfahrungen die Vermutungen der Befragten über die Stellen, die am umfangreichsten Daten speichern (z.B. Krankenkassen = 90%, Versicherungen = 87 %) noch durchaus realitätsnah. Auch für die Annahme, dass dem Daten-

umgang des Adreßhandels (8%) weniger zu trauen ist als dem von Ärzten (56 %),spricht, nimmt man die Statistiken der bei Datenschutzbehörden eingehenden Anfragen und Beschwerden zum Maßstab, einiges.

Ebenso überraschend wie besorgniserregend sind dagegen diejenigen Zahlen, die sowohl die große **Hilflosigkeit** des Bürgers im "institutionellen Datendschungel" belegen als auch seine Unkenntnis über praktische Handlungsmöglichkeiten. Wenn 40% der Befragten **Unwissenheit** als Hauptursache für Datenschutzverstöße bezeichnen, wenn 51 % keine Chance sehen oder einfach nicht wissen, wie sie sich gegen Datenmißbrauch wehren können, und das alles nach mehr als 20 Jahren Bestehen der Datenschutzgesetzgebung, ist dringender **Handlungsbedarf** offenkundig. Er trifft den Gesetzgeber genauso wie die datenverarbeitenden Stellen in Staat und Wirtschaft: Die Gesetze müssen verständlicher werden, der Datenumgang von Behörden und Unternehmen muß transparenter gemacht werden. Akzeptanz gewinnt die Informationsgesellschaft nur mit Offenheit.

Kritik und Selbstkritik als Konsequenz aus den Zahlen der Hamburger Untersuchung treffen aber auch und gerade die Datenschutzbeauftragten: Sie müssen intensiver als bisher **Öffentlichkeitsarbeit** betreiben, in Schulungsveranstaltungen auftreten, über die Medien praktische Schutzmöglichkeiten vermitteln. Anders ausgedrückt: Die Umfrageergebnisse lassen nur die Interpretation zu, dass die Datenschutzbehörden die **Aufklärung** über ihre Existenz, Aufgaben und Befugnisse nachhaltig verbessern müssen.

Kurz: Wir brauchen einen **"neuen Datenschutz"**, der praxisnäher, bürgerorientierter, technisch kompetenter, medienbewußter und vernetzt mit anderen Bürgerrechts- und Verbraucherschutzinstitutionen agiert (vgl. dazu die Beiträge in dem vom schleswig-holsteinischen Datenschutzbeauftragten H.

Bäumler herausgegebenen und ebenfalls im Juli 1998 erschienenen Sammelband "Der neue Datenschutz" im Luchterhand-Verlag).

Diese **Umorientierung** ist nicht Selbstzweck, sondern notwendig, um den Erwartungen der Bevölkerung gerecht werden zu können. Denn - und diese Erkenntnis der Studie ermutigt alle Engagierten - diese Erwartungen sind hoch: 47% der Befragten sind der Ansicht, es werde zu wenig auf den Datenschutz geachtet, 44% gehen davon aus, dass die Bedeutung des Datenschutzes in den nächsten Jahren zunehmen wird (18 % gleichbleibende Bedeutung), und 55% wünschen sich einen verstärkten Schutz ihrer persönlichen und geschäftlichen Daten.

Fazit also: Die Hamburger Repräsentativerhebung belegt die Existenz einer eigentümlichen Gemengelage einerseits von Ohnmachtsgefühlen, Befürchtungen und Unkenntnis in bezug auf den Umgang mit den eigenen Daten und andererseits Wünschen nach mehr Information, mehr Hilfen zur Selbsthilfe und wirksamerer Kontrolle. Die Umfrageergebnisse liefern viel Stoff für die Debatte über die Zukunft des Datenschutzes in unserem Land. Die Untersuchung ist vor allem aber eine wichtige Informationsquelle für alle, die an einer (selbst)kritischen Evaluation unseres deutschen Datenschutzsystems interessiert sind.

1.1.2. Reformbedarf und Reforminstrumente

Diese Bewertung von Erfolgen und Defiziten unseres über zwei Jahrzehnte gewachsenen Datenschutzsystems drängt, weil nach dem Regierungswechsel in Bonn die **Novellierung des Bundesdatenschutzgesetzes** (vgl. dazu 19. JB, Ziff. 5.1; 20. JB Ziff. 1.1.1) endlich angepackt werden und dazu die konzeptionelle Grundlage geklärt sein muß.

Wer wissen will, ob die neue Regierung diese Aufgabe, das Datenschutzrecht umfassend zu modernisieren und auf das Internet-Zeitalter hin zu orientieren, erkannt hat, wird bei der Lektüre der Koalitionsvereinbarung nicht fündig. Dort heißt es lediglich: "Effektiver Datenschutz im öffentlichen und im privaten Bereich gehört zu den unverzichtbaren Voraussetzungen für eine demokratische und verantwortbare Informationsgesellschaft. Die notwendige Anpassung des deutschen Datenschutzrechts an die Richtlinie der Europäischen Union soll kurzfristig umgesetzt werden." Diese Sätze sind ebenso richtig wie für das konkrete Politikprogramm wenig aussagekräftig.

Jedenfalls wird nicht deutlich, dass wir im Datenschutzrecht einen **Paradigmenwechsel** haben und daher eine Neuorientierung dringend brauchen. Deren Ziele und Instrumente lassen sich durchaus konkret benennen, wenn es um den Schutz des Persönlichkeitsrechts der Bürgerinnen und Bürger im Zeitalter von Internet, Multimedia und elektronischer Kommunikation geht. Die Datenschutzbeauftragten (vgl. zuletzt dazu die Konferenzentschließung vom 05./06. Oktober 1998, abgedr. u. Ziff. 20.5.), Bürgerrechtsorganisationen und kritische Informatiker, zuletzt auch der Deutsche Juristentag Ende September 1998 in Bremen, haben dafür längst vorgeleistet.

Ausgangspunkt des Reformbedarfs sind die tiefgreifenden Veränderungen der technologischen Rahmenbedingungen. Die **Digitalisierung** und die **Vernetzung** der Informationsübertragung heben die traditionellen Grenzen zwischen Computer, Telefon und Fernseher auf. Der "gläserne Netzbürger" droht unabhängig davon, ob das, was er an seinem Bildschirm tut, von der Telefongesellschaft, vom Pay-TV-Sender oder vom Internet-Provider registriert wird. Neue Kontrolltechniken wie die Videoüberwachung verbreiten sich epidemisch.

Datenschutzrecht kann sich mithin nicht mehr auf die Absicherung vor den Mißbrauchsrisiken der automatisierten Datenverarbeitung in großen Rechnern beschränken. Er ist vielmehr "Querschnittsmaterie": Wir brauchen die gleichen Schutzprinzipien und Schutznormen wie im traditionellen Datenschutzrecht auch im Rundfunk-, Multimedia- und Telekommunikationsrecht. Der vielleicht wichtigste Grundsatz ist die **Datenvermeidung bzw. Anoymisierung**. Wenn z. B. Internet-Anbieter gesetzlich verpflichtet werden, den Zugang zum Netz und die Bezahlung (auch) anonym, d.h. ohne automatische Identifizierung des Nutzers, anzubieten - etwa mit vorausbezahlten Chipkarten - werden von vornherein zu Mißbrauch verführende Datenspuren vermieden.

Dieses Beispiel zeigt die Bedeutung der Allianz von Datenschutz und Technik. Recht nützt nichts, wenn seine Vorgaben technisch nicht umgesetzt werden können. **Datenschutzfreundliche Technologien** wie Chipkarten, Verschlüsselungsprogramme und Firewalls sind längst auf dem Markt und werden laufend verbessert; die staatliche Forschungsförderung muß sich allerdings stärker engagieren.

Die besten rechtlichen Rahmenbedingungen und technischen Schutzmöglichkeiten nützen wiederum nur wenig, wenn der Einzelne zu wenig Rechte hat, seine Rechte nicht kennt oder die Datensicherung seines Gerätes nicht bedienen kann; dies haben die im vorigen Abschnitt (s.o. 1.1.1.) dargestellten Umfrageergebnisse nur zu deutlich gemacht. Die Bürger brauchen daher mehr Information über die Verwendung ihrer Daten, sie brauchen bessere **Auskunfts- und Widerspruchsrechte**. Schutzprogramme müssen einfach handhabbar sein und verständlich erklärt werden. Oder: Wer via Internet Waren bestellt oder Dienstleistungen ordert, muß

vor übereilter Einwilligung "per Knopfdruck" geschützt werden.

Aber: So notwendig es ist, den Bürgerinnen und Bürgern Instrumente für ihren "**Selbstschutz**" gegenüber datenverarbeitenden Stellen zur Verfügung zu stellen, so behält doch der Staat seine Schutzverantwortung für das informationelle Selbstbestimmungsrecht. Die effiziente Überwachung durch handlungsfähige Datenschutzbehörden ist dafür unverzichtbar. Hier gibt es gesetzgeberischen Nachholbedarf: Im neuen Datenschutzrecht muß die **Kontrolle** sowohl der Behörden als auch der Unternehmen in gleicher Weise anlaßfrei, weisungsfrei, unabhängig und mit wirksamen Eingriffs- und Verbotsbefugnissen ausgestaltet werden. Angesichts wachsender Datenmacht in privater Hand und zunehmender Privatisierung bislang öffentlicher Aufgaben spricht ohnehin alles dafür, den Schutzstandard für Verwaltung und Wirtschaft weitgehend zu vereinheitlichen. Nur wer überflüssig gewordene Sonderregelungen beseitigt, kann das derzeitige Regelungsgestrüpp **verschlanken**.

Noch einmal: Die **Neuorientierung** von Datenschutzpolitik und Datenschutzrecht ist weder technologiefeindlicher Luxus noch juristisches Sandkastenspiel. Sie ist notwendig, um den hohen Erwartungen der Bevölkerung an einen wirksamen Schutz ihres Persönlichkeitsrechts im Zeitalter globaler Vernetzung gerecht zu werden. Die Erfüllung dieser Erwartungen hat auch eminente ökonomische Bedeutung für die Wachstumspotentiale im Informations- und Kommunikationsbereich: Nur wenn die Bürger volles Vertrauen haben, dass ihre Daten im Internet zulässig verwendet und technisch sicher übertragen werden, hat **electronic commerce** eine Chance. Auf diesen Zusammenhang haben jüngst wieder die Experten des Deutschen Instituts für Wirtschaftsforschung (DIW) hingewiesen (vgl. Frankfurter Rundschau vom 18.2.1999).

Das jetzige Datenschutzrecht ist in Grundprinzipien wie Regelungskonzept zwanzig Jahre alt. Die Anforderungen für eine grundlegende Reform sind definiert; die Vorschläge liegen auf dem Tisch. Die Politik ist jetzt in der Pflicht, zunächst im Bund, dann auch in Bremen.

1.2. Hinweise zu diesem Bericht: "alte" und neue Themen

Auch dieser 21. Jahresbericht enthält - wie seine Vorgänger - (nur) einen **Ausschnitt** aus dem breiten Spektrum der Aktivitäten des Landesbeauftragten für den Datenschutz. Einige der beschriebenen Konfliktlagen zwischen dem informationellen Selbstbestimmungsrecht der Bürger und den Verarbeitungsinteressen von Verwaltung und Wirtschaft tauchen in jedem Jahr wieder auf. Dazu gehören insbesondere die Themenblöcke "Bekämpfung" des Mißbrauchs von Sozialleistungen und Datenverarbeitung durch die Sicherheitsbehörden.

Doch gibt es auch **Fragestellungen**, die **neu** in den Vordergrund rücken. Dazu zwei Beispiele:

- Die Einführung des **Neuen Steuerungsmodells** in der bremischen Verwaltung, die Umstellung auf Kosten- und Leistungsrechnung führen zu veränderten, tendenziell erhöhten Kontrollerwartungen (vgl. z.B. u. Ziff. 9.8. und 17.3.). "Der Datenschutz" muß dabei darauf achten, dass die notwendige Transparenz behördlicher Kosten und Leistungen nicht gleichzeitig auch die Beschäftigten lückenlos kontrollierbar macht. Sicherlich läßt sich, wie etwa bei der kostenstellenbezogenen Kalkulation, ein Mitarbeiterbezug nicht immer verhindern, auch um Angebote etwa der Eigenbetriebe "marktfähig" zu machen. Doch muß jeweils begründet werden, warum bei Datenverarbeitungsverfahren zu Zwecken der Pro-

jektabwicklung oder des Controlling die Identifizierbarkeit des einzelnen Beschäftigten erforderlich ist.

- Als technisches Kontrollinstrument breitet sich die **Videoüberwachung bzw. –aufzeichnung** (vgl. dazu Ziff. 18.2. und 18.3.) epidemisch aus. Diese Kontrolltechnologie, deren Einsatz bisher auf wenige Unfall- oder Kriminalitätsschwerpunkte (Bahnhöfe etc.) begrenzt war, wird sowohl in der Anschaffung billiger als auch in der Präzision der Aufnahmen immer perfekter. Um "englische Verhältnisse" zu vermeiden, in denen ganze Stadtviertel, Einkaufszentren etc. ohne Differenzierung nach Risikozonen von Videokameras staatlicher Stellen oder privater Unternehmen erfaßt werden, bedarf es dringend einer rechtsstaatlichen Begrenzung durch eine spezielle Regelung im zu novellierenden (dazu o. Ziff. 1.1.2.) Bundesdatenschutzgesetz (BDSG).

Wie wichtig es - bei aller in der Regel vorhandenen und begrüßenswerten Kooperationsbereitschaft der bremischen Behörden - bleibt, dass der Datenschutzbeauftragte **Kontrollen "vor Ort"** durchführt, belegen die Ergebnisse der Prüfungen in ausgewählten Polizeirevieren und bei der polizeilichen Einheit für die Foto- und Videodokumentation (vgl. u. Ziff. 9.1.2. und 9.2.). Diese Kontrollbesuche haben einerseits zum Teil erhebliche Datenschutzmängel aufgezeigt, boten aber andererseits auch die Gelegenheit, die Beamten direkt "an der Basis" über technische und rechtliche Datenschutz- und Datensicherungsanforderungen aufzuklären.

Zuletzt ein **redaktioneller Hinweis:** Erstmals verzichte ich aus Kostengründen auf eine eigene Druckausgabe dieses Berichts, der mithin nur in der vorliegenden Form der Bürgerschaftsdrucksache verbreitet wird (und im Internet unter der Adresse www.datenschutz.de abrufbar ist).

Reaktionen auf und Hinweise zu diesem Bericht sind herzlich willkommen (vgl. folgende Ziff.)

1.3. Anschrift und Kommunikationsdaten des Landesbeauftragten

Der Landesbeauftragte für den Datenschutz ist wie folgt zu erreichen:

Hausanschrift: Arndtstr. 1, 27570 Bremerhaven

Postanschrift: Postfach 10 03 80, 27503 Bremerhaven

Telefon: 0471/92461-0

Telefax: 0471/92461-31

E-mail: office@datenschutz.bremen.de

Sprechstunde für Bürgerinnen und Bürger im Bremer Büro, Pieperstr. 1-3, 28195 Bremen; jeweils donnerstags,
15 – 18 Uhr, Tel. während der Sprechstunde: 0421/361-2010.

1.4. Bremerhaven

Die Bremerhaven betreffenden Beiträge sind dieses Mal nicht in einem eigenen Kapitel ausgewiesen, sondern in die jeweiligen Fachkapitel integriert (vgl. die Abschnitte betr. das Magistratsnetz, Ziff. 6.4., Ziff. 17.1. zur Hundebestandserhebung, sowie Ziff. 12.1. betr. Datenabgleich in der Sozialhilfe).

2. Eingaben und Beschwerden

Schon aus arbeitsökonomischen Gründen ist es nicht möglich, eine vollständige Statistik aller Arbeitskontakte des LfD und seiner Mitarbeiter mit Bürgerinnen und Bürgern zu führen. Daher registriere ich die Zahl der telefonischen Anfragen und Hinweise ebensowenig wie die vielen Einzelgespräche anläßlich von Tagungen oder

Fortbildungsveranstaltungen. Gleiches gilt für die Bitten um Zusendung von Informationsmaterial. Erfaßt und nach Stichworten vermerkt sind lediglich die **schriftlichen Eingaben**. Zahl und Inhalt dieser Schreiben zeigen, worüber sich die Bürgerinnen und Bürger besonders ärgern, in welchen Bereichen sie ihre Individualrechte einfordern und zu welchen Themen Informationsbedarf besteht. Es geht also nicht nur um Beschwerden oder Kritik; manchmal wird auch nur um eine Rechtsauskunft gebeten.

Bis einschl. Januar 1999 habe ich insgesamt 121 Eingaben erhalten. 64 davon betrafen Stellen der **öffentlichen Verwaltung**. Schwerpunkte waren die Bereiche Polizei (10), Meldebehörde (3), Senatskommission für das Personalwesen (3) sowie Justizvollzugsanstalten (3).

57 Anschreiben hatten Datenschutzfragen in **privaten Unternehmen** zum Gegenstand. "Spitzenreiter" waren hier wie in den Vorjahren die **Auskunfteien** (8).

3. Fortbildungs- und Vortragsveranstaltungen

Meine Mitarbeiter und ich haben zahlreiche **Fortbildungsveranstaltungen** sowohl im Rahmen des SKP-Programms als auch aufgrund bilateraler Absprache mit senatorischen Behörden - so etwa bei der Schutzpolizei - abgehalten. Eine besondere Rolle spielt das zum dritten Mal im Rahmen des SKP-Programms für leitende Mitarbeiterinnen und Mitarbeiter durchgeführte Seminar "Datenschutz als Führungsaufgabe". Dieses Kursangebot bietet die Möglichkeit, mit Leitungskräften, d.h. für die Planung und Organisation ihrer Dienststellen verantwortlichen Amts- und Abteilungsleiter/innen, deren Erwartungen und Probleme bei der Umsetzung datenschutzrechtlicher Anforderungen zu diskutieren und die gegenseitigen Wünsche, Erwartungen und Kritikpunkte darzustellen.

Weitere **Referate** von Mitarbeitern meiner Dienststelle und mir betrafen u.a. die Themen "Lauschangriff", Sicherheit im Internet, digitale Signatur, unmittelbare Anwendung der EG-Datenschutzrichtlinie, sowie den Datenschutz in der Schulbegleitforschung, bei Rettungsdiensten/ Feuerwehr, bei der vernetzten Verarbeitung von Gesundheitsdaten und in der Altenpflege.

4. Presse- und Öffentlichkeitsarbeit; e-mail-Anschluß

Die Unterstützung der Medien ist fundamental für die Schaffung von Problembewußtsein für die Belange des Datenschutzes in Politik, Verwaltung und Wirtschaft. Die von Rundfunk und Presse aufgegriffenen aktuellen Themen geben einen guten Überblick über die gerade aus der Sicht des Bürgers und damit des von behördlicher oder geschäftlicher Datenverarbeitung Betroffenen besonders relevanten Fälle und Konflikte.

Meine **Pressemitteilungen** und **Interviews** im Berichtszeitraum betrafen u.a. die Themen "Großer Lauschangriff", Widerspruch gegen Wahlwerbung, rechtsstaatliche Sicherungen bei der zentralen "Gen-Datei", Sozialgeheimnis bei Meldungen an die Polizei sowie die unmittelbare Anwendung der EG-Richtlinie.

Mit mehreren Datenschutzbeauftragten-Kollegen habe ich im November 1998 auf einer **Pressekonferenz** in Bonn einen Appell an die neue Bundesregierung vorgestellt mit dem Titel "10 Punkte für einen Politikwechsel zum wirksameren Schutz der Privatsphäre".

Meine Dienststelle ist seit Mitte 1998 für Bürgerinnen und Bürger auch per **e-mail** zu erreichen. Die Adresse lautet **office@datenschutz.bremen.de**

Bei elektronischen Briefen ist jedoch das Risiko des unsicheren Netzes zu beachten, da noch keine Verschlüsselung eingerichtet ist. Dies soll im Frühjahr 1999 nachgeholt werden.

5. EG-Richtlinie: Direktwirkung und Datenexport

5.1. Direktwirkung - Vorgaben durch EuGH-Rechtsprechung

Da die Novellierung des Bundesdatenschutzgesetzes (BDSG) und des Bremischen Datenschutzgesetzes (BrDSG) nicht bis zum Ablauf der von der Richtlinie 95/46/EG vorgesehenen Umsetzungsfrist am 24. Oktober 1998 erfolgt ist, stellt sich die Frage nach der sog. **unmittelbaren Wirkung** einzelner Normen der Richtlinie. Der Europäische Gerichtshof hat die ständige Rechtsprechung entwickelt, dass sich die Bürgerinnen und Bürger in der Europäischen Union unter bestimmten Voraussetzungen gegenüber den Behörden auf in einer EG-Richtlinie gewährte Rechtspositionen auch dann berufen können, wenn der Mitgliedstaat die EG-Vorgaben (noch) nicht fristgemäß in sein nationales Recht übernommen hat.

Um Grundlagen und Konsequenzen dieser Direktwirkung für die Übergangszeit bis zur Anpassung der Datenschutzgesetze in Bund und Ländern festzustellen, habe ich zusammen mit meiner nordrhein-westfälischen Kollegin am 30. Oktober 1998 eine **Fachtagung** im und mit Unterstützung des Zentrums für Europäische Rechtspolitik an der Universität Bremen (ZERP) veranstaltet.

Grundlage der Beratungen war u.a. ein für die nordrhein-westfälische Datenschutzbeauftragte erstelltes Gutachten von Herrn Christian Haslach, Krefeld, mit dem Titel "Auswirkungen einer fehlenden Umsetzung der EG-Datenschutz-Richtlinie" (abgedr. in DuD 12/1998, 693 ff.).

5.2. Voraussetzungen und Adressaten

Übereinstimmung bestand zunächst hinsichtlich der **generellen Voraussetzungen** der unmittelbaren Wirkung von Richtliniennormen, nämlich Ablauf der Umsetzungsfrist, inhaltliche Unbedingtheit, hinreichende Bestimmtheit und subjektiv-rechtliche Qualität. Die inhaltliche Unbedingtheit entfällt nicht deshalb, weil zwar die Rechtsgewährung an den Bürger eindeutig ist, dem nationalen Gesetzgeber aber Ausnahmen ermöglicht werden. Dies gilt etwa für das Verhältnis zwischen Artt.10 bis 12 (Individualrechte) und Art. 13 (Ausnahmen und Einschränkungen durch den einzelstaatlichen Gesetzgeber möglich) oder zwischen Art. 8 Abs. 1 bis 3 (Rechte mit Einschränkungen, die insgesamt direkt gelten) einerseits und Abs. 4 (Ausnahmetatbestände für den nationalen Gesetzgeber) andererseits.

Adressaten der Richtlinie sind **alle öffentlichen Stellen von Bund, Ländern und Kommunen**, auch wenn sie in privatrechtlicher Form tätig sind, aber Aufgaben der öffentlichen Verwaltung wahrnehmen. Voraussetzung ist, dass sie in Verwaltungsverfahren und -materien agieren, die dem **Anwendungsbereich der Richtlinie** unterfallen. Keine Direktwirkung kann naturgemäß dort bestehen, wo Bereiche von der Richtlinie selbst ausdrücklich ausgenommen sind, etwa aufgrund Art. 3 Abs. 2 die Verarbeitungen betreffend die öffentliche Sicherheit. Die Abgrenzung ist aufgrund der dynamischen Kompetenzordnung des EG-Vertrags nicht immer einfach.

Die unmittelbare Wirkung ist von den Verwaltungen **von Amts wegen** zu beachten und nicht erst, wenn sich Personen auf ihre Rechtsansprüche berufen. Sie ist auch für die Beratungs- und Kontrollpraxis der Datenschutzbeauftragten verbindlich. Sie gilt nur **zugunsten** und nicht zu Lasten von

Privatpersonen. Sie wird nur dort relevant, wo BDSG, Landesdatenschutzgesetze oder bereichsspezifische Vorschriften nicht bereits die Anforderungen der Richtlinie erfüllen.

5.3. Rechtswirkungen

Regelungen des BDSG, die nicht der unmittelbaren Wirkung unterfallen bzw. durch sie nicht ergänzt oder modifiziert werden, sind von den öffentlichen Stellen **richtlinienkonform auszulegen**, um dadurch eine effektive Wirksamkeit des Gemeinschaftsrechts zu erreichen. Beispiel dafür ist die Berücksichtigung der Artt. 25 und 26 betr. die Datenübermittlung in Drittstaaten bei der Interpretation der §§ 28 und 29 BDSG. Bei der Übermittlung in Mitgliedstaaten, die ebenfalls noch nicht umgesetzt haben, ist zu berücksichtigen, dass auch dort die Direktwirkung greift.

Die verschiedenen in der Richtlinie enthaltenen **Meldepflichten** an die EU-Kommission, etwa nach Art. 26 Abs. 3 betr. Genehmigungen von Datenübermittlungen in Drittstaaten, greifen vor der Umsetzung formal nicht, da die gesamte **Genehmigungsprozedur** für die deutschen Unternehmen und Aufsichtsbehörden vor Schaffung einer expliziten Rechtsgrundlage in einem novellierten BDSG noch nicht gilt. Gleichwohl ist es dringend angeraten, dass die Datenschutzbeauftragten/Aufsichtsbehörden die EU-Kommission schon jetzt über ihre einschlägigen Stellungnahmen auf der Grundlage von §§ 28,29 BDSG i.V.m. Art. 26 Abs. 2 informieren. Wer nach dem neuen BDSG endgültig nach Brüssel meldende deutsche Stelle(n) sein wird (werden), ist noch offen.

Die **Direktwirkung einzelner Richtlinienartikel** ist für die Praxis vor allem dort interessant, wo das EG-Recht die Rechtsstellung des Einzelnen gegenüber der geltenden Rechts-

situation verbessert. Die **Erweiterung von Individualrechten** durch die Richtlinie gegenüber der deutschen Rechtslage ergibt sich vor allem aus den Artikeln 8, 10, 11 und 14, also für den besonderen Schutz sensibler Daten sowie die Informations- und Widerspruchsrechte. Wegen des gegenüber dem BDSG **weiteren Verarbeitungs- und Dateibegriffs** der Richtlinie (vgl. Art. 2 lit. b) und c) beziehen sich diese Rechte auf einen weiteren Anwendungsbereich als nach unserem deutschen Recht. Die **Haftung** für immaterielle Schäden läßt sich nach Art. 23 abweichend vom BDSG und § 5 Abs. 1 Satz 2 BrDSG wohl nicht auf schwere Verletzungen des Persönlichkeitsrechts beschränken.

Ich habe dem Senator für Justiz und Verfassung die Ergebnisse dieser Fachtagung zugeleitet.

5.4. Datenexport in Staaten außerhalb der Gemeinschaft - Regelungsinhalt und Verfahren der Aufsichtsbehörden

Die Debatte um die Interpretation und Umsetzung der **Drittstaatenregelung** in der Datenschutzrichtlinie, vor allem im Zusammenhang mit Datentransfers in die USA (vgl. dazu 20. JB, Ziff. 8.3), hat Praktiker in den Unternehmen, betriebliche Datenschutzbeauftragte und Firmenanwälte - nach meinem Dafürhalten überflüssigerweise - verunsichert. Dies gilt sowohl für den Regelungsinhalt der Artikel 25 und 26 der Richtlinie als auch für das in Deutschland bei Vertragsmodellen oder Entwürfen für Verhaltensrichtlinien einzuhaltende Verfahren.

Zum **Inhalt**: Art. 26 Abs. 1 der Richtlinie macht deutlich, dass in zwei großen Fallgruppen die Prüfung der **Angemessenheit des Datenschutzniveaus im Drittstaat** keine Rolle spielt, jedenfalls wenn der nationale Gesetzgeber nicht anders entscheidet. Dies gilt zum einen für Datenflüsse, in die der Betroffene "ohne jeden Zweifel" eingewilligt hat,

zum anderen für Übermittlungen, die zur Erfüllung einer Vertragspflicht des Datenexporteurs gegenüber dem Betroffenen erforderlich sind. Beispielsfälle für die zweite Konstellation sind Hotelreservierungen oder Mietwagenbestellungen im datenschutzlosen oder -schwächeren Ausland. Die Forderung, dass das Datenschutzniveau im Zielland dem in der EG adäquat sein muß, greift also besonders für die Branchen wie **Direktmarketing** und **Kreditauskunfteien**, in denen persönliche Angaben außerhalb eines Vertragsverhältnisses mit dem Betroffenen und ohne seine Kenntnis bzw. Einwilligung auf EG-Territorium erhoben wurden und dann in Drittstaaten weitergeleitet werden.

Die Datenschutzinstanzen der EG-Mitgliedstaaten haben in der **Gruppe nach Art. 29 der Richtlinie** zum grenzüberschreitenden Datenaustausch, d.h. zu den Anforderungen der Artikel 25 und 26, eine an klaren Prinzipien ausgerichtete Dogmatik entwickelt. Die Positionen der Art. 29-Gruppe, an deren Sitzungen ich als Vertreter der deutschen Landesbeauftragten regelmäßig teilnehme, sind zusammengefaßt in der öffentlich zugänglichen und in der datenschutzrechtlichen Fachpresse wiederholt kommentierten **Arbeitsunterlage** "Übermittlungen personenbezogener Daten in Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU" (GD XV D/5025/98, WP12).

Auch was die Anwendung der genannten Artikel in der **aufsichtlichen Praxis** angeht, gibt es klare Abläufe. Der Düsseldorfer Kreis, das Abstimmungsgremium der obersten Aufsichtsbehörden, hat sich auf ein **Verfahren** verständigt für den Fall, dass Unternehmen Datenflüsse in Drittstaaten, die nicht über ein angemessenes Schutzniveau verfügen, mit Hilfe einer Vertragslösung entsprechend Art. 26 Abs. 2 oder mit Einwilligungsklauseln (vgl. Art. 26 Abs. 1 lit a) der Richtlinie) ermöglichen wollen.

Sie müssen sich zur Beurteilung ihres Entwurfs wie für alle anderen Anwendungsfragen des BDSG auch zunächst an die für das Unternehmen örtlich zuständige Aufsichtsbehörde nach § 38 BDSG wenden. Diese bereitet eine Stellungnahme vor und sendet sie an den Berliner Datenschutzbeauftragten, der den Vorsitz in der **Arbeitsgruppe "Internationaler Handelsverkehr"** des Düsseldorfer Kreises führt. Als "Clearingstelle" informiert der Berliner Datenschutzbeauftragte die anderen obersten Aufsichtsbehörden. Gibt es von dort keine Einwände, entscheidet die zuständige Aufsichtsbehörde nach ihrem Votum. Werden Bedenken geäußert, wird der Sachverhalt in der o.a. Arbeitsgruppe besprochen; die zuständige Aufsichtsbehörde entscheidet dann unter Berücksichtigung des Diskussionsergebnisses der AG "Internationaler Handelsverkehr". Falls notwendig, wird das Ergebnis der Arbeitsgruppe auch dem Plenum des Düsseldorfer Kreises vorgelegt. Die endgültige Handhabung der Art. 25/26-Problematik durch die Aufsichtsbehörden hängt natürlich davon ab, wie die künftige BDSG-Novelle diesen Komplex regeln wird.

Dagegen ist es nicht sinnvoll, dass deutsche Unternehmen oder Branchenverbände Vertragsmodelle oder Entwürfe für Verhaltensrichtlinien direkt dem Datenschutzreferat in der Generaldirektion XV der EG-Kommission oder der Art. 29-Gruppe in Brüssel vorlegen. Die Art. 29-Gruppe hat festgelegt, dass sie sich nur mit solchen Texten beschäftigen wird, die von EG-weit tätigen Institutionen oder Verbänden vorgelegt werden bzw. EG-weit gelten sollen. Dazu gehören etwa Modellklauseln des europäischen Direktmarketingverbands FEDMA oder der internationalen Transportorganisation IATA.

Die Unternehmenspraktiker sollten sich mithin nicht von der auf den ersten Blick zugegebenermaßen komplexen Regelungs-

materie abschrecken lassen, sondern bei geplanten Datentransfers in Drittstaaten das **Beratungsangebot** und den Sachverstand der Aufsichtsbehörden in Anspruch nehmen.

6. Datenschutz durch Technikgestaltung und -bewertung

6.1. MEDIA@Komm

Ende Februar 1998 startete der damalige Bundesminister für Bildung, Wissenschaft, Forschung und Technologie Rüttgers "MEDIA@Komm", den **Städtewettbewerb Multimedia**. Ziel des Wettbewerbs ist es, die Anwendungen von Multimedia im Alltag erfahrbar zu machen, "Multimedia zum Anfassen" zu gestalten. Der Wettbewerb wurde vom Ministerium als wichtiger Bestandteil seiner Multimedia-Strategie angesehen. Ein zentrales Augenmerk wurde dabei auf die **digitale Signatur** nach dem Signaturgesetz vom 01.08.1997 gelegt. Bis zum 24. April hatten Städte oder Konsortien (Public-Private-Partnerships) die Gelegenheit, ihre Ideenskizzen einzureichen. Neben der Freien Hansestadt Bremen nahmen noch 135 weitere Städte, Gemeinden, Regionen und Public-Private-Partnerships an diesem Wettbewerb teil. In der ersten Runde wurden die zehn besten Ideenskizzen zur Förderung mit je 150.000 DM ausgewählt.

Am 11. Mai 1998 wurde das Ergebnis der Jury verkündet: Neben Städten wie Berlin, Köln und Leipzig gehörte die Freie Hansestadt Bremen zu den ausgewählten und konnte nun in einer Konzeptionierungsphase, die ich - soweit es die geringen Kapazitäten meiner Dienststelle zugelassen haben - begleitet habe, ein Grobkonzept für die Bewerbung erstellen. Von den vorgesehenen 44,6 Millionen DM der Ausgaben für das Projekt sind 0,466 Mio. DM für den Datenschutz vorgesehen, also ca. 1 Prozent der Ausgaben. Darin enthalten sind die Kosten für das Datenschutzkonzept (66.000 DM), die Evaluation (300.000 DM) und die Überprüfung (DM 150.000). Mit dem letzten Posten sollen die Aktivitäten meiner

Dienststelle im Rahmen des Projekts unterstützt bzw. überhaupt erst ermöglicht werden.

Für mich ist das Vorhaben ein spannendes **Versuchsfeld für Entwicklung und Einsatz datenschutzfreundlicher Technologien in elektronischen Verwaltungsverfahren**. Positiv an dem Konzept ist daher insbesondere zu bewerten, dass bei der geplanten Infrastruktur neben der digitalen Signatur der elektronisch zu übertragenden Dokumente auch deren **doppelte Verschlüsselung** vorgesehen ist. Damit ist nach derzeitigem Kenntnisstand für die nächsten Jahre sichergestellt, dass Unbefugte keinen Zugriff auf die Inhalte haben und diese auch nicht unbemerkt verändert werden können.

Ich habe meine Bereitschaft erklärt, das Projekt im Rahmen meiner begrenzten Kapazitäten zu begleiten und die Überprüfung des Datenschutzkonzepts für das Gesamtsystem sowie für die Anwendungsbündel vorzunehmen. Am 1o. März 1999 hat die Jury entschieden, dass Bremen neben den Städten Esslingen und Nürnberg zu den "Siegern" des Wettbewerbs gehört und damit den Zuschlag für die Förderungssummen aus Bonn erhält.

6.2. bremen.online

Für das Projekt bremen.online war 1998 von der SKP eine Ausschreibung als **"private-public-partnership"** vorbereitet worden (vgl. 20 JB, Ziff. 9.1.3.). Bedingt durch das Projekt MEDIA@Komm (s.o. Ziff. 6.1.) wurde diese Ausschreibung zurückgestellt. Seitens der SKP wird eine enge Koordination zwischen bremen-online und MEDIA@Komm als notwendig erachtet.

Das Problem der ungesicherten Übertragung der Daten zwischen Bürgern und Bürgerinnen auf der einen und der Verwaltung auf der anderen Seite konnte zumindest teilweise gelöst werden. So werden z.B. für die Übermittlung von Kurzbewerbungen an

die SKP (vgl. 20. JB, Ziff. 9.1.2.) standardmäßige **Verschlüsselungsverfahren** verwendet, die eine gewisse Sicherheit bieten. Für die Übertragung sehr sensibler personenbezogener Daten sind diese Verfahren zwar nicht geeignet, aber hierfür können später die im Projekt MEDIA@Komm gefundenen Lösungen verwandt werden.

6.3. Intranet - BVN

Nachdem bereits im März 1998 die Arbeitsgemeinschaft aus ID-Bremen und BreKom ihren Dienst aufgenommen hat, ohne dass zum damaligen Zeitpunkt auch nur der Entwurf eines Datenschutzkonzepts vorgelegen hätte (vgl. 20. JB, Ziff. 9.1.4.), wurde vom Senat zugesichert, dass es zu einem Vertragsabschluß zwischen der Senatskommision für das Personalwesen und der Arbeitsgemeinschaft erst kommen wird, wenn ein mit meiner Dienststelle abgestimmtes Datenschutzkonzept vorliegt. Am 30. Juli 1998 wurde mir die erste Version eines **"Sicherheitskonzepts für das Intranet der bremischen Verwaltung"** vom 19.06.1998 vorgelegt. Eine zur Abstimmung des Sicherheitskonzepts eingerichtete Arbeitsgruppe, an der ich beratend teilnehmen sollte, hat bis Redaktionsschluß dieses Berichts nicht getagt. Mehrere anberaumte Termine wurden seitens der SKP wieder abgesagt. Daher steht ein abgestimmtes Datenschutzkonzept für das Intranet und dessen Anbindung an das Internet nach wie vor aus. Dies ist um so verwunderlicher, als das vorgelegte Sicherheitskonzept eine gute Basis für die Abstimmung darstellt.

Vom TuI-Referat der Senatskommision für das Personalwesen sind "**Empfehlungen für die Erprobungsphase des E-Mail-Systems (elektronische Post) und der elektronischen Informationsordner in der bremischen Verwaltung**" erlassen worden. Wichtiger Bestandteil ist die Regelung, dass, solange keine verwaltungsweite Infrastruktur für digitale

Signaturen und für Verschlüsselung der E-Mails zur Verfügung steht, Dokumente, die eine Unterschrift benötigen, die bestimmten Formen genügen muß, oder die personenbezogene Daten enthalten, nicht per E-Mail zu versenden sind. Nicht unter die Regelung fallen der elektronische Datenaustausch für spezielle Anwendungen, in denen durch sichere Verschlüsselungstechniken die Vertraulichkeit und Integrität der übertragenen Daten sichergestellt ist.

Im November 1998 wurde ein "erster Entwurf einer Anweisung zur Einstellung und Absicherung von Windows-NT-Workstations und Windows-NT-Servern" von der SKP verteilt. Ziel dieser Anweisung ist es, die Windows-NT-eigenen Sicherungsfunktionen so zu konfigurieren, dass sie einen möglichst guten Schutz bieten. Das Schutzniveau, das mit den Sicherungsfunktionen von Windows-NT erreicht werden kann, ist allerdings nicht für alle Anwendungen ausreichend. Für Anwendungen mit sensiblen personenbezogenen Daten sind daher zusätzliche Sicherungsmaßnahmen (z.B. der Einsatz von Sicherheitssoftware, wie sie auch auf der Beschaffungsliste enthalten ist) zu treffen.

6.4. Das Projekt "Magistratsnetz Bremerhaven"

Am 19. März 1998 fand beim Magistrat der Seestadt Bremerhaven ein Projektauftaktgespräch zur Einführung und zum Betrieb des Magistratsnetzes statt. Ziel des Projektes ist es, für die verschiedensten Problematiken, die sich aus der Bildung eines **magistratsweiten Netzes** ergeben, unter Beteiligung der betroffenen Ämter, aber auch von Personalrat und meiner Dienststelle, Lösungen zu finden. Hierzu gehören insbesondere:

- zentrale Dienste im Netz (Intranet- und Internetnutzung, Fax-Server, E-Mail-Dienste),

- Netzwerkmanagement und Administration des Netzes,
- Verkabelungsstrategien,
- Anbindung von Außenstellen sowie
- Einrichtung und Betrieb der Firewalls.

Zu diesen Thematiken wurden Teilprojektgruppen eingerichtet, die - soweit es die knappen Ressourcen meiner Dienststelle zugelassen haben - beratend begleitet wurden. Daneben wurden für einzelne Fachverfahren (wie z.B. Bibliotheken, Ordnungswidrigkeiten) eigenständige Projektgruppen gebildet, deren Aufgabe die Integration dieser Fachverfahren in das Magistratsnetz ist.

Ich verwies schon im Vorfeld des Projektauftaktgesprächs auf die Ausführungen in meinem 20. Jahresbericht zum Bremischen Verwaltungsnetz und zu bremen.online (vgl. 20. JB, Ziff. 9.1.) sowie auf die Orientierungshilfe Internet (vgl. 18. JB., Ziff. 9.2.; zur aktualisierten Version s.u. Ziff. 6.5.).

6.4.1. Teilprojekt Zentrale Netzdienste

Hier gab es bis zum Redaktionsschluß noch keine abschließenden Ergebnisse. Als Aufgabe dieses Teilprojekts stellte sich die Erarbeitung einer **Dienstanweisung für den Umgang mit E-Mail** heraus. Ich habe darauf hingewiesen, dass auch in bezug auf die Nutzung von E-Mail sowie Dienste des Internets der Grundsatz der Erforderlichkeit zu beachten ist. Insbesondere die Möglichkeit, mit E-Mails jede Art von gespeicherter Datei zu versenden, fordert eine genaue Überprüfung, welche Arbeitsplätze mit dieser Möglichkeit ausgestattet werden. Zur Fragestellung, welche Regelungen aus datenschutzrechtlicher Sicht eine Dienstanweisung oder eine

Dienstvereinbarung enthalten sollte, habe ich der Teilprojektgruppe ein Arbeitspapier übergeben.

6.4.2. Teilprojekt Firewall

Ein **Firewallkonzept** soll bis Mitte März ausgearbeitet und dann in der Teilprojektgruppe vorgestellt und diskutiert werden. Ich habe im Rahmen meiner Beratung hierzu insbesondere auf die Anforderungen in der Orientierungshilfe Internet (vgl.u. Ziff. 6.5.) verwiesen. Die weitere Beratung sollte sich u.a. darauf richten, inwieweit die dortigen Anforderungen in dem Konzept umgesetzt worden sind.

6.4.3. Teilprojekt Netzwerkmanagement/Administration

In diesem Teilprojekt lag das Augenmerk insbesondere auf der Auswahl einer Netzwerkmanagementsoftware sowie der Erstellung eines Konzeptes zur Netzadministration. Ein mit mir abgestimmtes **"Basiskonzept" für die Netzadministration** liegt vor, das im März/April 1999 weiter detailliert werden soll. Für das Netzwerkmanagement wurde die Auswahl für ein System getroffen. Auf einem Testserver wurde das Produkt inzwischen installiert. Ab April soll es dann in Betrieb genommen werden. Bei allen Netzwerkmanagement-Diensten ist zu beachten, dass dort die Möglichkeit zur Verhaltens- und Leistungskontrolle der Arbeitnehmer und Arbeitnehmerinnen gegeben ist, da von ihnen personenbezogene Nutzungsdaten gespeichert werden können. Daher ist auch für diesen Bereich ein **Datenschutzkonzept** zu erstellen, aus dem insbesondere hervorgeht, welche Daten für welche Zwecke erforderlich sind, wie sie verarbeitet werden und wann sie wieder zu löschen sind.

6.5. Orientierungshilfe Internet

Zur Anpassung der "Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an

das Internet" (vgl. 18. JB, Ziff. 9.2) an die technische Entwicklung hatte der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Arbeitsgruppe eingerichtet. Ein Mitarbeiter meiner Dienststelle koordinierte diese Arbeitsgruppe, deren Ergebnis im Oktober 1998 von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zustimmend zur Kenntnis genommen wurde. Diese **aktualisierte Version** der Orientierungshilfe hat der Landesbauftragte für den Datenschutz in Mecklenburg Vorpommern als gedruckte Broschüre herausgegeben (Schloß Schwerin; 19053 Schwerin; Tel.: 0385/59494-0; FAX: -58). Sie ist auch **im Internet** unter **http://www.datenschutz-berlin.de/informat/dateien/onet-rtf.gz** zu finden.

7. Bürgerschaft - Die Arbeit des Datenschutzausschusses

7.1. Ergebnisse der Beratung des 20. Jahresberichts

Der **Bericht und Antrag des Datenschutzausschusses** vom 21. Januar 1999 zum 20. Jahresbericht des Landesbeauftragten für den Datenschutz (Drs. 14/1005 vom 21. April 1998) und zur Stellungnahme des Senats vom 29. September 1998 (Drs. 14/1124) mußte von der Tagesordnung der Februarsitzung des Plenums der Bürgerschaft abgesetzt werden. Er wird daher erst in der dritten März-Woche, also nach Redaktionsschluß, im Plenum beraten werden können (Drs. 14/1321). Die Abgeordneten haben dann über folgenden Antrag zu befinden: "Die Bürgerschaft (Landtag) tritt den Bemerkungen des Datenschutzausschusses bei."

Der vom Ausschuß angenommene Text hat folgenden **Wortlaut**:

"Die Bürgerschaft (Landtag) hat in ihrer Sitzung am 14. Mai 1998 den 20. Jahresbericht des Landesbeauftragten für den Datenschutz und in ihrer Sitzung am 22. Oktober 1998 die

Stellungnahme des Senats zur Beratung und Berichterstattung an den Datenschutzausschuß überwiesen.

Der Ausschuß hat bei der Behandlung des Jahresberichts und der Stellungnahme des Senats den Landesbeauftragten für den Datenschutz und Vertreter der betroffenen Ressorts angehört. Die wesentlichen Beratungsergebnisse sind nachfolgend aufgeführt. Die Textziffern in den verwendeten Überschriften sind identisch mit denen des 20. Jahresberichts.

- **Zukunftstrend Teleheimarbeit (Tz. 11.1)**

Die neue Arbeitsform Teleheimarbeit kommt insbesondere den speziellen Bedürfnissen Schwerbehinderter und Familien mit kleinen Kindern entgegen. Der Datenschutzausschuß begrüßt in diesem Zusammenhang, dass zwischenzeitlich eine Dienstvereinbarung zwischen der Senatskommission für das Personalwesen und dem Gesamtpersonalrat für das Land und die Stadtgemeinde Bremen abgeschlossen worden ist, die es ermöglicht, Telearbeitsplätze in Privatwohnungen einzurichten, und die auch die datenschutzrechtlichen Anforderungen an derartige Arbeitsplätze festlegt. So stellt diese Dienstvereinbarung unter anderem sicher, dass sensible Daten nicht in Teleheimarbeit verarbeitet werden dürfen und dass dem Landesbeauftragten für den Datenschutz zur Ausübung seiner Kontrollbefugnisse der Zutritt zu den Privatwohnungen, in denen Teleheimarbeit stattfindet, zu gewähren ist.

- **Geheimschutzbeauftragte (Tz. 12.2)**

Im Zusammenhang mit der Überprüfung von Bediensteten, denen geheimschutzrelevante Aufgaben übertragen sind, üben die Geheimschutzbeauftragten der Dienststellen wichtige Funktionen aus. Bei einer Überprüfung der Tätigkeit der Geheimschutzbeauftragten einiger Dienststellen sind erhebliche Mängel

festgestellt worden. So sind zum Beispiel Unterlagen über Jahrzehnte aufbewahrt worden, obwohl sie seit langem hätten vernichtet sein müssen. Auch ist festgestellt worden, dass keiner der vom Landesbeauftragten für den Datenschutz aufgesuchten Geheimschutzbeauftragten vorher in seine Aufgaben eingewiesen worden ist.

Der Datenschutzausschuß ist der Auffassung, dass für die Wahrnehmung der Aufgaben der Geheimschutzbeauftragten eine entsprechende Schulung dieses Personenkreises insbesondere in Form von Aus- und Fortbildungsmaßnahmen unerläßlich ist. Der Ausschuß geht deshalb davon aus, dass den Geheimschutzbeauftragten die Teilnahme an solchen Veranstaltungen ermöglicht wird.

- **Zugriffsprotokollierung bei der Polizei - Löschungsfrist (Tz. 12.4)**

Im Zusammenhang mit der Behandlung dieser Angelegenheit im Datenschutzausschuß hat das Polizeipräsidium nunmehr die Anregung des Landesbeauftragten für den Datenschutz, Sicherungsbänder mit Protokolldaten beim behördlichen Datenschutzbeauftragten aufzubewahren, aufgegriffen.

Der Ausschuß sieht diesen Punkt damit als erledigt an.

- **Verwaltungsvorschriften zum Ausländergesetz - Bonitätsprüfung (Tz. 12.7)**

Nach § 84 des Ausländergesetzes kann derjenige, der einen Ausländer gastweise aufnimmt, verpflichtet werden, alle mit dem Aufenthalt zusammenhängenden Kosten zu übernehmen, wenn der Ausländer selbst nicht in der Lage ist, seinen Lebensunterhalt während des Aufenthalts in Deutschland zu bestreiten. Bisher geschah dies in Bremen durch eine formlose Verpflichtungserklärung, die der Einladende vor der zuständigen Behörde abgeben konnte.

Im Vorgriff auf eine bundeseinheitliche Verwaltungsvorschrift, deren Entwurf inzwischen dem Innenausschuß des Bundesrats zur Beratung vorliegt, hat der Senator für Inneres mit einem Erlaß geregelt, dass der Gastgeber vor der Abgabe der Verpflichtungserklärung nach § 84 des Ausländergesetzes einer sogenannten Bonitätsprüfung unterzogen wird. Das dazu verwandte Formular enthält unter anderem Rubriken für Angaben zur Frage, ob der Gastgeber Mieter oder Wohnungseigentümer ist sowie für sonstige Angaben zu Einkommens- und Vermögensverhältnissen. Das Original des Formulars erhält der Eingeladene, der es wiederum im Rahmen des Visumsverfahrens bei der zuständigen Auslandsvertretung vorlegen muß.

Der Datenschutzausschuß teilt die Kritik des Landesbeauftragten für den Datenschutz an diesem neuen Verfahren, das dem Gastgeber eine unverhältnismäßig große Anzahl von sensiblen Einzelangaben abverlangt, in die zudem noch Dritte Einsicht nehmen können. Der Ausschuß begrüßt deshalb, dass der Senator für Inneres mit einem Erlaß vom 2. November 1998 an die Ausländerämter verfügt hat, dass auf Angaben zu den vorgenannten Rubriken künftig zu verzichten sei.

- **Novellierung des Bremischen Meldegesetzes (Tz. 12.8.1)**

Das Bremische Meldegesetz ist immer noch nicht an das bereits 1994 geänderte Melderechtsrahmengesetz des Bundes angepaßt worden. Der Datenschutzausschuß hat auf dieses Versäumnis wiederholt hingewiesen, zuletzt in seinem Bericht zum 19. Jahresbericht des Datenschutzbeauftragten. Der Senator für Inneres hat im Ausschuß erneut auf fehlende Arbeitskapazitäten in seinem Haus hingewiesen, gleichwohl aber erklärt, er bemühe sich um die Vorlage eines Entwurfs noch vor Ende der Legislaturperiode. Der Datenschutzausschuß

erwartet, dass der Innensenator diese Ankündigung realisiert und weist auf den bereits jetzt bestehenden Zeitdruck hin. Der Ausschuß geht weiterhin davon aus, dass bei der Erarbeitung des Entwurfs für ein novelliertes Meldegesetz die bisherigen Regelungen über die Übermittlung von Meldedaten an Parteien und Adreßbuchverlage überprüft werden.

- **Sperrvermerke und Wählerverzeichnis (Tz.12.10)**

Bereits anläßlich der Beratungen des 17. Jahresberichts des Landesbeauftragten im Datenschutzausschuß hatte der Senator für Inneres zugesagt, Vorkehrungen dahingehend zu treffen, dass Sperrvermerke, die zum Schutz vor Belästigungen oder Bedrohungen im Melderegister eingetragen worden sind, auch bei der Erstellung des öffentlich auszulegenden Wählerverzeichnisses beachtet werden. Der Senator für Inneres hat nunmehr auf Nachfrage gegenüber dem Datenschutzausschuß erklärt, rechtzeitig bis zur Bürgerschaftswahl am 6. Juni 1999 eine entsprechende Regelung in der Landeswahlordnung vorzusehen.

- **Versorgungswerk der Hanseatischen Rechtsanwaltskammer (Tz. 13.4)**

§ 10 Abs. 2 Nr. 10 des Gesetzes über die Rechtsanwaltsversorgung in der Freien Hansestadt Bremen (RAVG) vom 30. September 1997 sieht vor, die besonderen Bestimmungen über den Datenschutz durch Satzung zu regeln. Der Landesbeauftragte für den Datenschutz hat dazu eine Reihe von Empfehlungen ausgesprochen, die jedoch nicht berücksichtigt worden sind.

Der Vorsitzende des Vorstands der Hanseatischen Rechts-anwaltsversorgung Bremen hat gegenüber dem Ausschuß erklärt, es werde größter Wert darauf gelegt, dass der Datenschutz im

Versorgungswerk im Einvernehmen mit dem Landesbeauftragten geregelt werde. Dessen Empfehlungen hätten damals aus Zeitgründen nicht mehr aufgenommen werden können, da die Satzung am 1. Januar 1998, dem Stichtag für das neue Versorgungsjahr, habe in Kraft gesetzt werden müssen. Anfang 1999 sei eine Überprüfung des Satzungsrechts vorgesehen. In diesem Zusammenhang könnten dann auch Bestimmungen über den Datenschutz aufgenommen werden.

Der Datenschutzausschuß sieht die Angelegenheit damit als erledigt an.

- **Krebsregister des Landes Bremen (Tz. 14.1)**

Zur Erforschung der Ursachen von Krebskrankheiten und letztlich mit dem Ziel der Verhütung und Eingrenzung dieser Krankheiten ist aufgrund entsprechender Vorgaben des Bundes an die Länder durch das am 1. Oktober 1997 in Kraft getretene Gesetz über das Krebsregister der Freien Hansestadt Bremen (BremKRG) ein Krebsregister errichtet worden. Das Krebsregister wird von zwei räumlich, organisatorisch und personell voneinander getrennten Stellen geführt, der Vertrauensstelle, deren Träger die Kassenärztliche Vereinigung Bremen (KV) ist, und der Registerstelle in der Trägerschaft des Bremer Instituts für Präventionsforschung und Sozialmedizin (BIPS). Aufgabe der Vertrauensstelle ist es, Meldungen von Ärzten über Daten von Patienten, die an Krebskrankheiten leiden, entgegenzunehmen, diese auf Schlüssigkeit und Vollständigkeit zu prüfen und den sogenannten epidemiologischen Datensatz (medizinische Daten ohne Personenbezug) an die Registerstelle weiterzugeben. Dieser obliegt die Auswertung der Daten nach bundeseinheitlichen Vorgaben und die Übermittlung an die beim Robert-Koch-Institut eingerichtete "Dokumentation Krebs".

Der Datenschutzausschuß hat sich ausführlich mit der besonderen datenschutzrechtlichen Problematik des Krebsregisters befaßt. Er teilt die Auffassung des Landesbeauftragten für den Datenschutz, dass bei der Verarbeitung dieser höchst sensiblen Daten geeignete Vorkehrungen getroffen werden müssen, um zu verhindern, dass die Daten zu anderen als zu den gesetzlich vorgesehenen Zwecken genutzt werden. Der Ausschuß hat in diesem Zusammenhang zur Kenntnis genommen, dass sowohl die Registerstelle als auch die Vertrauensstelle inzwischen Datenschutzkonzepte vorgelegt haben. Er erwartet, dass bei der Führung des Krebsregisters nunmehr die dafür notwendigen datenschutzrechtlichen Vorgaben hinsichtlich der Zweckbegrenzung der Daten und der Datensicherheit unverzüglich umgesetzt werden.

- **Kindergarteninformationssystem (Tz. 14.4.2)**

Der Senator für Frauen, Gesundheit, Jugend, Soziales und Umweltschutz hat ein Kindergarteninformationssystem (KIS) entwickelt, mit dem Daten von Eltern und Kindern für die Aufnahme und die Beitragsberechnung sowie für statistische und für pädagogische Zwecke verarbeitet werden können.

Der Landesbeauftragte für den Datenschutz kritisiert, dass bereits Probeläufe in einigen Kindertagesheimen durchgeführt worden seien, obwohl seinerzeit noch kein Datenschutzkonzept vorgelegen habe.

Der Datenschutzausschuß weist darauf hin, dass nach den Bestimmungen des Bremischen Datenschutzgesetzes Datenverarbeitungssysteme generell erst dann zum Einsatz kommen dürfen, wenn die datenschutzrechtlichen Anforderungen geklärt sind. Letzteres ist, wie der Landesbeauftragte für den Datenschutz und das Jugendressort vor dem Ausschuß übereinstimmend erklärt haben, beim KIS inzwischen der Fall, so dass der

Anwendung des Systems datenschutzrechtliche Bedenken nicht mehr entgegenstehen.

- **Sozialpsychiatrischer Dienst - Keine umfassende Automation ohne Rechtsverordnung (Tz. 14.7)**

Nach dem seit 1995 in Kraft befindlichen Gesetz über den Öffentlichen Gesundheitsdienst im Lande Bremen ist eine Rechtsverordnung zu erlassen, die unter anderem einen Katalog der Daten, die im Bereich der Gesundheitsämter gespeichert werden dürfen, bestimmen muß. Diese Rechtsverordnung liegt bisher nicht vor mit der Folge, dass die Möglichkeiten der automatisierten Datenverarbeitung in der Gesundheitsverwaltung nicht in dem gewünschten Umfang genutzt werden können, was insbesondere beim Sozialpsychiatrischen Dienst zu Problemen führt. Der Datenschutzausschuß hatte sich bereits in seinem Bericht vom 11. März 1998 (Drs. 14/981) mit dieser Angelegenheit befaßt und dabei die Erwartung geäußert, dass die Rechtsverordnung bis zur Sommerpause 1998 vorliegen werde.

Der Ausschuß hat sich über die für die Verzögerung ursächlichen Gründe informiert. Er ist danach zu der Auffassung gelangt, dass es aufgrund der Komplexität der zu regelnden Materie und anderer von niemandem zu vertretender Umstände bisher nicht zum Erlaß der Rechtsverordnung gekommen ist. Der Ausschuß wird die weitere Entwicklung dieser Angelegenheit begleiten.

- **Renten an "Kriegsverbrecher" im Ausland (Tz. 16.1.1)**

In den Medien wurde darüber berichtet, dass an ehemalige, jetzt im Ausland lebende Mitglieder der Waffen-SS Kriegsbeschädigtenrenten gezahlt würden, wobei zwei Fälle aus den USA im Vordergrund standen. Die öffentliche Kritik traf dabei insbesondere das Versorgungsamt Bremen, das zentral

für auf dem gesamten amerikanischen Kontinent lebende Versorgungsberechtigte zuständig ist.

Der Senator für Arbeit übersandte entsprechend einer Aufforderung des Bundesministeriums für Arbeit und Sozialordnung (BMA) diesem eine Liste der Empfänger von Versorgungsleistungen in Nord- und Südamerika, die das BMA zwecks Abgleichung mit dortigen Unterlagen über Kriegsverbrechen an die Justizbehörden der Wohnsitzstaaten weiterleiten wollte.

Der Landesbeauftragte für den Datenschutz hat dazu angemerkt, dass - ungeachtet der rechtspolitisch zu begrüßenden Aktion - Bedenken bestünden, wenn ohne Vorprüfung mehrere tausend Namen von Versorgungsempfängern ausländischen Behörden zur Prüfung der Beteiligung an Kriegsverbrechen übermittelt würden.

Der Datenschutzausschuß teilt diese prinzipielle Kritik. Er sieht sie jedoch als ausgeräumt an, nachdem der Senat in seiner Stellungnahme vom 29. September 1998 (Drs. 14/1124, Nr. 7, Seite 11) ausgeführt hat, dass das BMA inzwischen versichert habe, eine unkontrollierte Weitergabe der Daten erfolge nicht. Vielmehr würden die datenschutzrechtlichen Vorgaben beachtet. Insbesondere müsse vor jeder Weitergabe gewährleistet sein, dass dadurch keine schutzwürdigen Interessen der Leistungsempfänger beeinträchtigt werden. In Zweifelsfällen unterbleibe eine Übermittlung der Daten.

7.2. Aktuelle Themen

Der Datenschutzausschuß befaßt sich neben der Beratung des Jahresberichts mit einer Reihe aktueller Fragen, die teils von den Abgeordneten gestellt, teils von mir aufgeworfen werden. Vielfach sind Presseberichte Ausgangspunkt der Behandlung im Ausschuß. Die von der Ausschußassistenz geführte "Restantenliste" sorgt dafür, dass Bitten und

Anregungen an die Verwaltung nicht ohne Reaktion bleiben, sondern ggf. erneut auf die Tagesordnung gesetzt werden.

Dieser Beharrlichkeit bedurfte es beispielsweise im sog. **Stradivari-Fall** (ausführl. berichtet im 20. JB, Ziff. 10.2.2.2), der nicht weniger als fünf Mal im Datenschutzausschuß aufgerufen werden mußte. Als positives Ergebnis kam heraus, dass der Innensenator Richtlinien für die Erteilung von Drehgenehmigungen bei TV-Reportagen erlassen hat, die einen ausgewogenen Ausgleich zwischen der Pressefreiheit und dem Persönlichkeitsrecht der Opfer, Zeugen und Verdächtigen anstreben. Der Justizsenator hat erklärt, diese Richtlinien auch der Staatsanwaltschaft zur Kenntnis zu geben.

Weitere aktuelle Themen waren u.a.

- die bundesweite **Gendatei** beim Bundeskriminalamt, deren Funktionsweise und rechtliche Grundlagen (vgl. dazu unter Ziff. 10.1.),
- die **Video-Aufnahmen** einer Dokumentationseinheit der Bremer Polizei bei der Demonstration am 1. Mai 1998 (vgl. dazu u. Ziff. 9.1.),
- die Aktivitäten des "Tele-Info-Verlags" im niedersächsischen Garbsen zur Errichtung einer bundesweiten **Häuserdatenbank**,
- der Datenschutz beim Informationsaustausch zwischen Sozialarbeitern und wirtschaftlicher **Jugendhilfe**,
- das Schweigerecht bzw. die Auskunftspflicht von **Therapeuten** gegenüber der Anstaltsanleitung in **Gefängnissen**.

7.3. Haushalt 1999 - keine Aufstockung für technische Fortbildung

In der Beratung des Entwurfs des speziell für den LfD bestimmten Kapitels im Haushalt 1999 hat der Datenschutzausschuß meine bescheidene, zweckgebunden für die technische Fortbildung der Mitarbeiterinnen und Mitarbeiter gestellte Mehrforderung von 11.000 DM anerkannt und einen entsprechenden Antrag an den Haushaltsausschuß weitergeleitet.

Der **Haushaltsausschuß** hat mir diese Summe jedoch zu meinem Bedauern nicht zusätzlich bewilligt, sondern mich auf meine ohnehin vorhandenen Rücklagen verwiesen, die ich allerdings zur Deckung anderer Budgetlücken benötige. Ich muß das Parlament an dieser Stelle darauf hinweisen, dass ich außerstande bin, die quantitativ wie an Komplexität zunehmenden DV- und Netzprojekte der bremischen Behörden im bisherigen Umfang zu betreuen, wenn die technische Fortbildung meiner zuständigen Mitarbeiter finanziell nicht gesichert ist. Bei komplexeren Einzelvorhaben müssen ggf. in der jeweiligen Projektfinanzierung spezielle Mittel für die Erstellung und Überprüfung des Datenschutzkonzepts ausgewiesen werden (vgl. o. Ziff. 6.1.).

Da ich entgegen früherer Praxis im Haushaltsausschuß der Finanzdeputation zur Sitzung des jetzt parlamentarischen Haushaltsausschusses nicht eingeladen worden war, konnte ich meine Budgetsituation persönlich auch nicht erläutern.

8. Personalwesen

8.1. Telearbeit - Zulässigkeitsrahmen und Kontrollbefugnis

In meinem letzten Jahresbericht habe ich unter Ziff. 11.1. erstmals über den Trend zu vermehrter Einführung von Teleheimarbeit auch in der bremischen Verwaltung berichtet. Senat und Gesamtpersonalrat haben im Mai 1998 eine **Dienstvereinbarung zum Modellversuch "Alternierende Tele-**

arbeit" abgeschlossen. Danach werden "Tätigkeiten, bei denen überwiegend personenbezogene Daten (z. B. Personalaktenverarbeitung, Beihilfebearbeitung) verarbeitet werden, nicht im Modellversuch vergeben." Außerdem ist festgelegt worden, dass personenbezogene Daten der Teilnehmer/innen am Modellversuch, die in behördeninternen Anwendungsrechnern oder Telekommunikationsanlagen protokolliert werden, ausschließlich zum Zwecke der Wahrung ihrer Betriebssicherheit oder zur Datenschutzkontrolle und nicht zu Leistungs- und Verhaltenskontrollen ausgewertet werden, und die Einrichtung der Telearbeitsplätze in jedem Einzelfall in Abstimmung mit mir erfolgt. Des weiteren ist eine **Mustervereinbarung über die "Einrichtung, Nutzung und Auflösung einer häuslichen Arbeitsstätte in einer Wohnung"** als Anlage zur Dienstvereinbarung erstellt worden.

Die Modellversuche sollen durch eine Arbeitsgruppe "Tele-arbeit" begleitet werden, der auch ein Vertreter bzw. eine Vertreterin meiner Dienststelle angehören. In der ersten Sitzung dieser Arbeitsgruppe ist vereinbart worden, dass abweichend von der Dienstvereinbarung, an deren Erstellung ich nicht beteiligt worden bin, Telearbeit nicht stattfinden soll, wenn personenbezogene Daten verarbeitet werden, die Berufs- und besonderen Amtsgeheimnissen unterliegen (z. B. Sozial-, Personal- und Steuerdaten sowie medizinische Daten).

Da die Mustervereinbarung keine Klausel über meine **Kontroll-befugnis** enthält, habe ich im September 1998 auf Bitten der Arbeitsgruppe als Ergänzung folgende Formulierung vorgeschlagen: "Der/die Bedienstete stimmt zu, dass der Landesbeauftragte für den Datenschutz bzw. seine Mitarbeiter/-innen die Privaträume betreten und die dienstliche Datenverarbeitung dort überprüfen dürfen. Wird

die Zustimmung später widerrufen, hat dies zur Folge, dass die Telearbeit jedenfalls mit personenbezogenen Daten beendet wird."

In der Sitzung des Datenschutzausschusses der Bremischen Bürgerschaft am 03. Dezember 1998 hat die SKP nur einen bisher eingerichteten Tele-Arbeitsplatz, und zwar für einen Schwerbehinderten, benannt, an dem jedoch keine personenbezogenen Daten verarbeitet würden. Bei ID Bremen nehmen vier Mitarbeiter/innen am Modellversuch teil. Vereinzelt sind Anträge von den Dienststellenleitungen nicht befürwortet worden.

Für Ende Februar 1999 hat die SKP zu einer neuen Sitzung der Arbeitsgruppe "Telearbeit" eingeladen, auf der die weitere Vorgehensweise festgelegt werden soll, um die bisher relativ geringe Resonanz der Beschäftigten auf das Angebot von Telearbeit zu verbessern. Zu erarbeiten ist dann auch ein **Technikkonzept**, das einen sicheren Fernzugriff von Telearbeitsplätzen auf Datenbestände innerhalb des Bremischen Verwaltungsnetzes gewährleistet.

8.2. PuMa: Komprimierung ersetzt nicht Kryptierung

Das Datenschutzkonzept für das landesweit zur Personalverwaltung und für das Personalmanagement eingesetzte Verfahren PuMa (vgl. 18. JB, Ziff. 10.1.3.) sieht vor, in Ausnahmefällen ein Schreiben auf Diskette zu ermöglichen, wenn auf diesen Geräten ein Programm zur Verschlüsselung der Daten installiert wird. Bei einer Prüfung des Verfahrens beim Senator für Frauen, Gesundheit, Jugend, Soziales und Umweltschutz - Bereich Gesundheit, Jugend und Soziales - habe ich entgegen dieser Vorgabe PCs mit Schreibzugriff auf das Diskettenlaufwerk, aber ohne Kryptierungs-Software, vorgefunden.

Ich habe die fehlende Verschlüsselung bei der SKP angemahnt. Nach mehrfacher Bitte um Antwort hat die SKP das Komprimierungsprogramm WinZip empfohlen. Das Programm bietet die Möglichkeit der **paßwortgeschützten Datenkomprimierung**. Eine Dekomprimierung der Daten ist zwar nur durch Paßworteingabe möglich; der Zugriff Unbefugter durch Herausfinden des Paßwortes ist jedoch nicht auszuschließen. Ich habe die SKP darauf hingewiesen, dass die Komprimierung die Verschlüsselung nicht ersetzen und lediglich als Übergangslösung bis zum Einsatz einer adäquaten Verschlüsselungssoftware akzeptiert werden kann.

8.3. Türöffnungssystem nur ohne Zeiterfassung

Mehrere Beschäftigte des Senators für Häfen, überregionalen Verkehr und Außenhandel, die im neuen Hafenhaus in Bremerhaven arbeiten, hatten mich darüber informiert, dass dort ein Türöffnungssystem installiert war, das gleichzeitig für die Kontrolle der Arbeitszeit geeignete Zugangsdaten wie Datum und Uhrzeit, bezogen auf die Ausweisnummer und damit auf die Ausweisinhaber, speicherte.

Nicht zuletzt da die Dienstvereinbarung über die Grundsätze für die gleitende Arbeitszeit eine **Koppelung der Arbeitszeiterfassung mit anderen EDV-Systemen** ausschließt, hat das für das Türöffnungssystem verantwortliche Hansestadt Bremische Hafenamt auf meine Intervention hin erklärt, Zugangsdaten würden nicht mehr gespeichert, und das Modul "Auswertungen" sei deaktiviert worden. Ich habe das System vor Ort überprüft und mich von der Richtigkeit der Erklärung überzeugt.

8.4. KIDICAP: Datenschutzkonzept ist fertig

Im 20. JB habe ich unter Ziffer 11.5 über die Ablösung des bisher von der SKP eingesetzten Bezügeabrechnungsverfahrens

PAADIS durch das neue Verfahren KIDICAP 2000 berichtet. Hingewiesen habe ich auf die in KIDICAP fehlende Differenzierung der Zugriffsmöglichkeiten je nach Zuständigkeitsbereich des Sachbearbeiters. Das Datenschutzkonzept sieht vor, den Zugriffsschutz von PAADIS weiterzuverwenden.

Die im Vorjahresbericht dargestellte zeitlich begrenzte organisatorische Übergangslösung für den fehlenden Zugriffsschutz ist entfallen, da der Einsatz von KIDICAP im Echtbetrieb erst Anfang 1999 aufgenommen wurde.

Das rechtzeitig vorgelegte Datenschutzkonzept einschließlich der von mir angeforderten Anlagen (Übersicht der Listenausgaben, Schnittstellen und regelmäßigen Übermittlungen) ist insgesamt in Ordnung.

Ich gehe davon aus, dass ich über die weiteren Entwicklungsschritte, z.B. die Verbindung der Verfahren KIDICAP und PuMa, wie bisher rechtzeitig informiert werde.

8.5. Rechtsreferendare: Verzicht auf Einstellungsuntersuchung

Ein angehender Rechtsreferendar hat moniert, dass er sich wie Beamtenanwärter auf Lebenszeit einer Einstellungsuntersuchung unterziehen solle, obwohl er nur für den zweijährigen Vorbereitungsdienst in das Beamtenverhältnis auf Widerruf berufen werde.

Die Senatskommission für das Personalwesen (SKP) hat sich zunächst formal darauf berufen, weil die Berufung in das Beamtenverhältnis gem. § 9 Bremisches Beamtengesetz (BremBG) nach Eignung, Befähigung und fachlicher Leistung vorzunehmen sei und der Begriff der Eignung die gesundheitliche Eignung umfasse, könne auf eine Einstellungsuntersuchung von Bewerbern für den juristischen Vorbereitungsdienst nicht verzichtet werden.

Ich habe gegenüber der SKP angezweifelt, ob mit dieser Interpretation eine **obligatorische Regeluntersuchung** für den gesamten genannten Personenkreis begründet werden kann. Um beurteilen zu können, ob die mit dieser Praxis verbundene Speicherung von Gesundheitsdaten aller Bewerber dem Grundsatz der Erforderlichkeit und damit den Vorgaben des § 93 BremBG entspricht, habe ich die SKP gebeten mitzuteilen, ob und ggf. in wievielen Fällen Bewerber mangels gesundheitlicher Eignung abgelehnt worden sind.

Nachdem sich herausgestellt hat, dass es in den letzten Jahren keinen einzigen derartigen Fall gab, bat ich die SKP, die Möglichkeit zu prüfen, künftig anstelle der Einstellungsuntersuchung die Bewerber/-innen lediglich danach zu **fragen**, ob akute oder chronische Gesundheitsstörungen oder Behinderungen vorliegen, die den Beginn des Ausbildungsverhältnisses verhindern bzw. verzögern oder eine entsprechende Rücksichtnahme oder Hilfe am Ausbildungsplatz erfordern könnten.

Daraufhin hat die SKP erklärt, im Einvernehmen mit dem Senator für Justiz und Verfassung sei sie damit einverstanden, dass bei der Einstellung von Rechtsreferendaren auf die Einstellungsuntersuchung verzichtet und entsprechend meiner Anregung verfahren werde.

8.6. Arbeitsmedizinische Untersuchungen: Abrechnung ohne individuellen Bezug

Die Fachdienste für Arbeitsschutz haben mich gebeten zu prüfen, ob es zulässig sei, wenn der Eigenbetrieb "Justiz-Dienstleistungen" (JUDIT) die arbeitsmedizinischen Untersuchungen für Justizvollzugsbeamte einzelfallbezogen abgerechnet haben wolle, und zwar einschließlich der **Untersuchungsbefunde und Diagnosen**. Diese unterliegen der ärztlichen Schweigepflicht nach § 8 Abs. 1 Satz 2 Arbeitssicher-

heitsgesetz (ASiG) und dürfen ohne besondere gesetzliche Befugnis oder Einwilligung der Betroffenen dem Arbeitgeber bzw. Dienstherrn nicht bekanntgegeben werden.

JUDIT hat auf meine Anfrage erklärt, die Angabe der Untersuchungsbefunde und Diagnosen sei nicht mitarbeiterbezogen erforderlich, jedoch müsse einzelfallbezogen abgerechnet werden, weil sonst die nach Nrn. 11 ff. der Verwaltungsvorschrift zu § 70 Landeshaushaltsordnung vorgeschriebene sachliche und rechnerische Richtigkeit nicht ausreichend nachweisbar sei.

Nach gemeinsamen Beratungen und Rücksprache des Eigenbetriebs mit dem Senator für Finanzen ist daraufhin ein Abrechnungsmuster für JUDIT erstellt worden, auf dem die durchgeführten arbeitsmedizinischen Vorsorgeuntersuchungen und weitere Leistungen (Impfungen etc.) nur **getrennt** als Listen der Mitarbeiter und Listen der erbrachten Leistungen, die nicht individuell einander zugeordnet werden können, dargestellt werden.

8.7. Beihilfeverfahren BABSY: indirekte Speicherung von Diagnosen

Im Jahre 1994 ist das automatisierte Beihilfeverfahren BABSY eingeführt worden, worüber ich in meinem 17. Jahresbericht unter Ziff. 8.3. berichtet habe. Eine im Berichtszeitraum erfolgte **Prüfung** hat ergeben, dass die Beihilfefestsetzungsstelle der Senatskommission für das Personalwesen die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat, um insbesondere zu gewährleisten, dass die zur Benutzung des Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und ein unbefugter Zugriff auf die Beihilfedaten verhindert wird.

Bei der Prüfung habe ich jedoch festgestellt, dass neben den Grunddaten des Beihilfebescheides (Name des Anspruchsberechtigten und Datum des Bescheides) auch **Hinweisnummern** für die Dauer von fünf Jahren im System gespeichert werden, wenn der Beihilfebescheid einen Hinweis für den Anspruchsberechtigten enthält. Hinweise werden dann in den Bescheid aufgenommen, wenn Erläuterungen über die Gewährung der Beihilfe erforderlich sind.

Ich habe mir die Liste der Hinweisnummern vorlegen lassen und festgestellt, dass die insgesamt über 500 Hinweise in fast allen Fällen **Rückschlüsse auf Diagnosen bzw. Krankheiten** zulassen. Beispiele dafür sind die Hinweise darauf, dass nur unter bestimmten Voraussetzungen Aufwendungen für kieferorthopädische Leistungen, prothetische Behandlungen, Psychotherapie, für Herz-, Wirbelsäulen- oder Hüftgelenkoperationen oder für die Behandlung einer anderen schweren Erkrankung wie Herzinfarkt, Krebs oder Suchtkrankheiten beihilfefähig sind.

Die Beihilfestelle hat erklärt, sie halte die Speicherung der jeweiligen Hinweisnummer im automatisierten Verfahren für evtl. Rückfragen von Anspruchsberechtigten und bei Behandlungen, die einen mehrjährigen Verlauf haben, für erforderlich.

Ich habe dementsprechend wegen der hohen Sensibilität der mit diesen Ziffern erschließbaren Gesundheitsdaten eine Differenzierung dahingehend vorgeschlagen, die Hinweisnummern **in der Regel spätestens ein Jahr nach Bescheiderstellung**, und nur bei mehrjährigen Behandlungen später, und zwar spätestens nach fünf Jahren, zu **löschen**.

Die SKP hat zugesagt, meine Anregungen im Zuge der Erstellung eines Löschprogramms im Jahre 1999 zu

berücksichtigen, weil dann die nach § 93h Abs. 2 Bremisches Beamtengesetz vorgesehene fünfjährige Aufbewahrungsfrist auch für automatisiert verarbeitete Beihilfedaten erstmals abläuft.

9. Inneres

9.1. Videoaufzeichnungen durch die Polizei

9.1.1. Überwachung der 1. Mai-Demonstration

In der Bremer Presse wurde berichtet, dass die Demonstration des Deutschen Gewerkschaftsbundes am 1. Mai 1998 aus einem Café von Polizeibeamten mittels Videokamera gefilmt worden sei. Ich wurde daraufhin von Abgeordneten der Bremischen Bürgerschaft gebeten, den Vorgang unter datenschutzrechtlichen Gesichtspunkten zu prüfen, und zwar insbesondere, wie lange und was genau gefilmt wurde, wie das Material ausgewertet wurde und was damit passiert sei. Das Thema war auch Gegenstand einer öffentlichen Sitzung des Datenschutzausschusses am 16.07.1998. In diesem Jahresbericht schildere ich wegen des breiten öffentlichen Interesses Hintergrund, Ablauf und Bewertung der Polizeiaktion sowie die Ergebnisse der zusätzlichen Prüfung der Videoarchive ausführlich.

Aufgrund der Presseberichte und der Anfrage der Abgeordneten habe ich einen Bericht des Polizeipräsidiums angefordert, der die Entscheidungsfindung zum Einsatz der Videoaufzeichnung dokumentiert, und die polizeiliche Dienststelle aufgesucht, die die Maßnahme durchgeführt hat.

Dieser **Bericht** schildert die **angenommene Gefahrenlage** wie folgt: Nach Darstellung der Schutzpolizei waren Störungen gegen den Aufzug aufgrund der Lageeinschätzung nicht auszuschließen. Bereits 1997 habe eine Gruppe von ca. 60 Personen versucht, in die Marschsäule des DGB einzudringen. Auch zum 1. Mai 1998 gab es Erkenntnisse über die Beteiligung

autonomer Kräfte. Auch das zuvor erlassene Verbot des Kurdisch-Deutschen Solidaritätsvereins e. V. durch den Innensenator sowie Plakate und Flugblätter zu diesem Thema gaben Anlaß zur Annahme, dass es zu Störungen kommen könne. Daraufhin habe sich die Einsatzleitung entschlossen, die polizeiliche Einheit, die mit der Durchführung von Foto- und Videodokumentation betraut ist (BEDO-Trupp), einzusetzen. Als dann eine verbotene Fahne der PKK offen im Aufzug gezeigt worden sei, habe der polizeiliche Einsatzleiter den BEDO-Beamten den Auftrag zum Filmen erteilt. In erster Linie habe hierbei der tatverdächtige Fahnenträger aufgezeichnet werden sollen. Man habe dann mit der Videokamera nur innerhalb geschlossener Blöcke einen Film von insgesamt 4 bis 5 Minuten angefertigt.

Darüber hinaus sei es der Schutzpolizei gelungen, den genannten Fahnenträger der PKK nach Abschluß der Kundgebung festzunehmen. Gegen ihn wurde dann Strafanzeige erstattet. Nach Beendigung der Maßnahme sei dann die Filmkassette – da auf ihr keine weiteren Straftatbestände erkennbar gewesen seien – vernichtet worden.

Zur **rechtlichen Bewertung**: Die **Versammlungsfreiheit** genießt Verfassungsrang (Art. 8 GG). Das **Bundesverfassungsgericht** hat in seiner **Brokdorf-Entscheidung** festgestellt, dass das Recht auf freie Meinungsäußerung, das Demonstrationsrecht und das Persönlichkeitsrecht beeinträchtigt würden, wenn Bürger damit rechnen müßten, behördlicherseits registriert und aufgezeichnet zu werden sowie Sanktionen befürchten zu müssen, wenn sie diese Rechte ausüben. 1989 wurde in das **Versammlungsgesetz** der § 12a eingefügt, der Bild- und Tonaufnahmen durch die Polizei in öffentlichen Versammlungen zuläßt, aber auch einschränkend regelt. Nach dieser Vorschrift darf die Polizei Bild- und Tonaufnahmen von

Teilnehmern bei oder im Zusammenhang mit öffentlichen Versammlungen nur anfertigen, wenn **tatsächliche Anhaltspunkte** die Annahme rechtfertigen, dass von ihnen **erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung** ausgehen.

Nach den mir vorgelegten Unterlagen konnte die Polizei aufgrund ihrer Informationen und der daraus abgeleiteten Gefahrenprognose davon ausgehen, dass die Voraussetzungen von § 12 a Versammlungsgesetz erfüllt waren.

Nach § 12 a Abs. 2 des Versammlungsgesetzes sind die Unterlagen nach Beendigung der öffentlichen Versammlung oder zeitlich und sachlich damit unmittelbar in Zusammenhang stehender Ereignisse **unverzüglich zu vernichten**, soweit sie nicht u. a. für die Verfolgung von Straftaten von Teilnehmern benötigt werden. Da es im weiteren Verlauf der 1.-Mai-Demonstration zu keinerlei Ausschreitungen gekommen war und der einer Straftat verdächtige Fahnenträger vorübergehend festgenommen worden war, bestand keine Rechtsgrundlage mehr, die Videoaufzeichnung länger aufzubewahren.

Der Bericht des Polizeipräsidiums bzw. die Einsatzdokumentation wiesen dementsprechend die **Löschung des Filmmaterials** aus, was ich in den Räumen bzw. im Archiv des BEDO-Trupps vor Ort überprüft habe. Ich konnte daher auch nicht mehr feststellen, ob der dargestellte Umfang der Aufzeichnung von 4 bis 5 Minuten zutraf und angemessen war.

9.1.2. Überprüfung des polizeilichen Filmarchivs

Da ich bei meinem ersten Besuch einige Dutzend Videobänder ab dem Jahr 1985 mit Schwerpunkt ab dem Jahr 1991 vorfand, war dies Anlaß dafür, bei der Beobachtungs- und Dokumentationseinheit (kurz "BEDO-Trupp") eine **umfassende Datenschutzprüfung** vorzunehmen.

Dabei mußte ich feststellen, dass dort eine größere Anzahl von Filmen und Bildmaterial, das nicht aus aktueller Bearbeitung stammte, aufbewahrt wurde. So gab es z.B. Fotos von Demonstrationsteilnehmern, ohne dass Ausschreitungen oder verbotene Gegenstände oder vermummte Personen zu erkennen waren. Die **Erforderlichkeit der Aufbewahrung** konnte **nicht begründet** werden.

Gleiches gilt für eine großen Teil der bis zum Anfang der neunziger Jahre zurückreichenden ca. 130 Videobänder. Deren **Verwaltung** und **Archivierung** war in einem **schlechten Zustand**. Zwar war in der Regel noch zu erkennen, welche Dienststelle den Auftrag zur Dokumentation gewisser Ereignisse gegeben hatte. Vielfach war aber nicht nachvollziehbar, ob und in welchem Umfange von dem Fotomaterial Abzüge gefertigt bzw. von den Videoaufnahmen Kopien gefertigt und an welche Stellen diese ausgehändigt wurden. Auch fehlte es häufig an klaren Anweisungen der auftraggebenden Stellen, wie nach Abschluß der Maßnahme mit dem Material verfahren werden solle. Auf diese Mängel angesprochen, wurde darauf hingewiesen, dass es zwar einen Vordruck gebe, das mitgelieferte PC-Programm aber nicht einsatzfähig sei.

Bereits während der Prüfung habe ich zum Ausdruck gebracht, dass dieser Zustand nicht länger hinnehmbar sei und dringend eine generelle Bereinigung erfolgen müsse. Einen Monat später wurde mir mitgeteilt, dass die fraglichen Fotos vernichtet worden seien. Zwei Monate später erhielt ich eine komplette Liste aller ursprünglich vorhandenen **Videobänder**, woraus sich ergibt, dass rund 90% von ihnen **gelöscht** worden sind.

Die beim BEDO-Trupp festgestellten **Datenschutzmängel**, insbesondere der Verstoß gegen das Löschungsgebot nach § 12a Versammlungsgesetz, waren so **erheblich**, dass eine förmliche

Beanstandung hätte ausgesprochen werden können. Lediglich die schnelle Kooperation der zuständigen Hauptabteilung der Schutzpolizei und die **konsequente Löschaktion** (wobei das Material dem Staatsarchiv hätte angeboten werden können bzw. müssen) sowie das erkennbare Bemühen, den Anforderungen des Datenschutzes gerecht zu werden, haben es ermöglicht, von einer Beanstandung abzusehen.

Allerdings müssen jetzt weiterreichende Konsequenzen gezogen werden, zu denen ich die Schutzpolizei aufgefordert habe. So habe ich z.B. festgestellt, dass Rechtsgrundlagen und Rechtsprechung zur Zulässigkeit polizeilicher Filmaufnahmen nicht oder nicht ausreichend bekannt sind; es besteht mithin ein **Schulungsdefizit**. Weiter bedarf es einer klaren Festlegung, welche Stellen berechtigt sind, einen Auftrag an den BEDO-Trupp zu erteilen. Dabei müssen Ziel, Zweck und Rechtsgrundlage der Maßnahme klar beschrieben werden.

Weiterhin muß klar dokumentiert werden, wann und wo, in wessen Auftrag und in welchem Umfang Fotos, Videoaufzeichnungen oder mit anderen technischen Mitteln gefertigte Aufzeichnungen hergestellt wurden, ob und in welchem Umfang Vervielfältigungen angefertigt wurden bzw. an wen das Material ausgehändigt wurde. Soweit Materialien bei dem BEDO-Trupp verbleiben, sind Löschprüffristen vorzusehen. Bei der beauftragenden Stelle ist dann nachzufragen, ob das Material vernichet werden kann. Werden durch den BEDO-Trupp erstellte Materialien für die Durchführung von Strafverfahren benötigt, ist in jedem Fall sicherzustellen, dass nach Abschluß des Verfahrens und nicht erst dann, wenn die Kriminalakte zur Löschung ansteht, die nicht im Verfahren benötigten Fotos und Bänder gelöscht bzw. vernichtet werden. Die für das Strafverfahren selbst gebrauchten Aufzeichnungen werden ohnehin Bestandteil der staatsanwaltschaftlichen Ermittlungsakte.

Meine **Empfehlungen zur Neuorganisation des Verfahrens** habe ich Anfang des Jahres an das Polizeipäsidium gerichtet. Eine Stellungnahme steht noch aus.

9.2. Querschnittsprüfung in Polizeirevieren

Im letzten Jahr habe ich ausgewählten Polizeirevieren in Bremen und Bremerhaven Kontrollbesuche abgestattet. Die geprüften Reviere weisen überwiegend ähnliche Organisationsstrukturen auf, d.h. sie sind aufgeteilt in die Bereiche Führung, Wache und Ermittlungsdienst.

Von den Revieren werden u.a. Straftaten und Ordnungswidrigkeiten verfolgt, verkehrs- und veranstaltungsbezogene Maßnahmen ergriffen; je nach stadtteilbezogener Problemlage wird in unterschiedlicher Ausprägung auch die präventive Tätigkeit durch Datenverarbeitung unterstützt. Bei den Prüfungen bin ich nach einem ähnlichen Schema vorgegangen; auch habe ich mich vorher angemeldet, um eine umfassende Information sicherzustellen.

Zunächst muß festgestellt werden, dass sich mit dem Einsatz des rechnergestützten Vorgangsverwaltungssystems die Datenschutzsituation in den Revieren erheblich verbessert hat. **Gravierende Mängel** habe ich allerdings vor allem in zwei Bereichen festgestellt: Bei der Datenaufbewahrung in den Archivräumen und beim Einsatz von Hard- und Software. Dabei handelt es sich teils um Einzelfälle, teils aber auch um häufiger auftretende Schwachstellen.

Bei der **Aufbewahrung der Altvorgänge** waren die **Löschfristen** zum Teil weit **überschritten**, z. T. sogar über die maximale Aufbewahrungsdauer von 10 Jahren hinaus. Nur zum Teil waren die Vorgänge nach Jahrgängen geordnet, was die Einhaltung von Aussonderungs- und Löschfristen zusätzlich erschwert. Hinzu kam mangelnde Kenntnis über Aufbewahrungsfristen und

über die Verpflichtung, Akten vor der Vernichtung dem Staatsarchiv anzubieten. Nicht immer beachtet wurde bei den Löschfristen die "Doppelspeicherung" in Papierform und in der automatisierten Datei. In einem Revier hatten alle Bediensteten des Reviers Zugang zu Personalunterlagen.

Die Schwerpunkte bei den **Mängeln im technischen Bereich** lagen beim Einsatz der **Vorgangsverwaltungssysteme** und bei der Benutzung der **Magnetkarten**. So steckten z.B. Karten für die Berechtigung zu Abfragen im ISA-D-System in den Lesegeräten, obwohl die Karteninhaber abwesend bzw. sogar ausser Haus waren. Jeder berechtigte Polizeibeamte verfügt jedoch über eine eigene Karte für die von ihm getätigten Abfragen, die er herausziehen muß, wenn er das Gerät nicht benutzt.

Schwachstellen der Datensicherung ergaben sich u.a. daraus,

- dass ein Bootpaßwort ganz fehlte oder von unzureichender Länge (z.B. nur zwei Zeichen) war, was leicht zu "knacken" ist,
- dass Dateien mit personenbezogenen Angaben, z.T. auch Personaldaten, ohne ausreichenden Zugriffsschutz auf den PCs gespeichert waren,
- dass Abfragen im Rahmen von ISA-D für Kollegen ohne Angabe des Veranlassers vorgenommen wurden, und
- dass die Anwender die Archivierungsfunktion der Vorgangsverwaltung nicht genug kennen.

Ich habe die bei der Prüfung festgestellten Mängel sowie Anregungen zu ihrer Beseitigung den Polizeileitungen in Bremen und Bremerhaven mitgeteilt. Dazu gehören die Klarstellung der **Aufbewahrungsfristen** sowohl für papierne Unterlagen als auch für automatisiert gespeicherte Daten, die Notwendigkeit

des Angebots zur Abgabe an das Staatsarchiv für einzelne Unterlagen vor deren Vernichtung, Regelungen für die Vergabe von BIOS-**Paßwörtern** sowie verbindliche Anweisungen für den Umgang mit der Mail-Funktion in ISA.

Auch die geprüften Reviere habe ich schriftlich über die bei ihnen festgestellten Mängel informiert und um Beseitigung gebeten. Ich erwarte, dass meine in den Schreiben enthaltene Mängelliste zum Anlaß genommen wird, auch die nicht geprüften Reviere auf die genannten Fehler bei der Datenverarbeitung hinzuweisen, so dass diese in die Lage versetzt werden, Rechtsverstöße und Schwachstellen selbst zu beseitigen. Ich gehe davon aus, dass die Mängel im ersten Halbjahr 1999 abgestellt werden und schliesse eine Nachkontrolle nicht aus.

9.3. Datenspeicherung bei Polizei und Verfassungsschutz: Eingaben und Prüfergebnisse

Ebenso wie in den Vorjahren haben sich wieder viele Bürger teils selbst, teils über einen beauftragten Rechtsanwalt an mich gewandt und um Überprüfung der zu ihrer Person gespeicherten Daten bei Polizei, Staatsanwaltschaft und Verfassungsschutz gebeten. Einige Petenten hatten sich bereits vorher direkt bei den speichernden Stellen um Auskunft bemüht und waren mit der Antwort nicht zufrieden, entweder weil die Auskunft verweigert wurde oder weil sie mit der Tatsache oder dem Umfang der Datenspeicherung nicht einverstanden waren.

Ich nenne die Ergebnisse hier nur summarisch: Meine Überprüfungen beim **Landesamt für Verfassungsschutz** führten zu keinerlei Beanstandungen. Anders bei den Speicherungen im **polizeilichen Informationssystem ISA**: Dort führte meine Intervention zu einer Reihe von Löschungen, teils des gesamten Datensatzes des Eingebers, teils einzelner Angaben.

Gründe waren vor allem Überschreitungen der Speicherfrist oder die Änderung der polizeilichen Bewertung in bezug auf die Notwendigkeit weiterer Aufbewahrung.

9.4. INPOL-Neu - die Umstrukturierung und ihre Konsequenzen

9.4.1. Neukonzeption des bundesweiten Informationssystems INPOL beim BKA

Seit mehr als 10 Jahren wird beim Bundeskriminalamt (BKA) daran gearbeitet, das zentrale Informationssystem der Polizei des Bundes und der Länder weiter zu entwickeln und neuen technischen Entwicklungen anzupassen. Bekannt ist das System unter dem Kürzel INPOL, was für den Begriff "**Informationssystem der Polizei**" steht. INPOL unterstützt mit seinen zentralen Dateien die Personen- und Sachfahndung und gibt überregionale Auskünfte in den Bereichen Erkennungsdienst, Daktyloskopie, Haftdatei, Kriminalaktennachweis und aus verschiedenen Falldateien unter anderem in den Bereichen Rauschgift, Waffen, Falschgeld und Organisierte Kriminalität.

1992 wurde von dem BKA den Ländern erstmalig der Entwurf einer Gesamtkonzeption zur Umstrukturierung von INPOL vorgestellt. Das Projekt trägt den Namen **INPOL-Neu**.

Die Entscheidungsfindung ging in den fünf Jahren nach 1992 nicht so recht voran; erst ab Ende 1997 wurde an der Umsetzung und Einführung von INPOL-Neu mit Hochdruck gearbeitet. Das BKA hat dessen Einführung auf den 01. Januar 2000 festgelegt. Die bisherige INPOL-Dateistruktur wird durch einen Datenpool auf der Grundlage eines **relationalen Datenbanksystems** mit verschiedenen Verknüpfungs- und Auswertungsfunktionen abgelöst. INPOL-Neu wird zu einem komplexen Datenbanksystem weiterentwickelt, das mit multifunktionalen Verknüpfungs-, Auswertungs- und Recherchetools eine **qualitativ und quantitativ neue Dimen-**

sion darstellen wird. Allein die Liste der sog. Entitäten-Typen und Attribute umfaßt rund 100 DIN-A4-Seiten und reicht von "A" wie Adresse über "D" wie DNA und "K" wie Konto bis "Z" wie Zahnbeschreibung. Die Informationen aus den Ländern sollen nach vorgegebenen Mustern – häufig verbunden mit der Möglichkeit der Eingabe von Freitexten – direkt in INPOL-Neu eingespeist werden. Dabei ist beabsichtigt, die Entscheidung darüber, ob ein Datensatz in INPOL-Neu eingestellt werden soll, nach einem Muß-, Regel- und Kann-Fall-Konzept zu unterstützen.

Die Teilnahme an INPOL-Neu bedingt für die Polizeien der Länder die Teilnahme an einer **einheitlichen Kommunikationsschnittstelle**, die nach dem derzeitigen Planungsstand mit 168 Funktionalitäten ausgestattet sein soll. Die Kommunikationsschnittstelle regelt den Aufruf der erforderlichen Funktionen, über die der Zugriff auf den INPOL-Neu-Datenbestand realisiert werden soll. Der **Zugriffsschutz** soll über eine spezielle Software gewährleistet werden und über die Definition von **Benutzerklassen**, denen die Anwender gemäß einer Errichtungsanordnung zugeordnet werden, benutzerspezifische Sichten auf den INPOL-Neu-Datenpool ermöglichen. Das **Berechtigungskonzept** ist noch nicht entwickelt.

9.4.2. Auswirkungen auf die polizeiliche Informationsverarbeitung im Lande Bremen

Die Folgen für die polizeiliche Informationsverarbeitung in Bremen sind gravierend. INPOL-Neu ist so konzipiert, dass mit ihm weder die Datenbank ISA noch das Dialogsystem ISA-D als Landesverfahren kompatibel sind. Auch das als Eigenentwicklung des Landes laufende Datenaustauschverfahren zwischen Polizei und Staatsanwaltschaft (ISA-SIJUS-STRAF) wird betroffen sein. **Die gesamte DV-Struktur der Polizei im**

Lande Bremen muß umgestellt werden. Bremen wird es allein schon aus Kostengründen nicht möglich sein, zu dem vorgesehenen Stichtag alle DV-Anwendungen komplett auf INPOL-Neu umzustellen.

Auch gibt es hier derzeit noch keine hinreichend entwickelten Konzeptionen und Softwarelösungen. Dies gilt auch für andere Bundesländer. Man hat sich daher auf Länderseite darauf verständigt, das Verfahren schrittweise einzuführen und dazu eine Arbeitsgruppe eingerichtet. Auch im Lande Bremen wurden zur Anpassung an INPOL-Neu ein **Lenkungs**- und ein **Koordinierungsausschuß** gebildet; letzterer ist beim Polizeiführungsstab (Führungsstab 24) angebunden.

Da INPOL-Neu vorgangsbezogen aufgebaut ist, muß auch die gesamte **Erfassungsstruktur** bei den Länderpolizeien geändert werden. Langfristig hat dies zur Folge, dass – da INPOL-Neu aktuell im Dialog laufen muß – alle Sachbearbeiter mit entsprechender **Hardware** auszurüsten sind. Zur Zeit gibt es in Bremen ca. 150 bis 170 ISA-D-Rechner, die aller Voraussicht nach aufgrund ihres technischen Standards den Anforderungen von INPOL-Neu nicht entsprechen und daher nicht weiter verwendet werden können. Folge einer umfassenden Einführung von INPOL-Neu wäre für Bremen, dass - so die Schätzung von PFSt 24 - ca. 600 bis 800 Endgeräte neu beschafft werden müßten, die vernetzt werden müßten mit einem **neuen Landesrechner**, auf dem das künftige Landesinformationssystem gefahren wird, sowie mit einem Knotenrechner als Schnittstelle zu INPOL-Neu. Hinzu kommt, dass ein Vorgangsbearbeitungssystem (VBS) neu eingeführt werden müßte.

Ich befinde mich mit dem PFSt 24 in einem regelmäßigen Informationsaustausch über die datenschutzrechtlichen und datensicherungstechnischen Auswirkungen des neuen Systems. Dabei hat sich gezeigt, dass eine Beeinflussung der

Datenschutzkomponenten auf Bundesebene bei der Gestaltung von INPOL-Neu nur in geringem Umfang möglich ist. Aber auch auf Landeseite scheinen mir die Spielräume für datenschutzgerechte Lösungen relativ gering, weil Bremen anders als im Falle ISA-D keine Eigenentwicklung beabsichtigt, sondern die Übernahme einer externen Komplettlösung favorisiert.

Auf der anderen Seite gestatten die neuen Programmentwicklungen aufgrund vieler vorhandener technischer Möglichkeiten, dass in Teilbereichen auch im Nachhinein spezifische, auf die besonderen Verhältnisse der Polizei im Lande Bremen zugeschnittene Lösungen ab der Schnittstelle zwischen Bund und Land möglich sind.

9.4.3. Zugriffsbeschränkungen und Protokollierungsverfahren

Ich bin mir mit dem PFSt 24 einig darüber, dass bei der Umstrukturierung der Datenverarbeitung nicht hinter die bereits im Lande Bremen erreichten Datenschutzstandards zurückgegangen werden soll. Daher habe ich frühzeitig meine Anforderungen an das **Protokollierungsverfahren** mitgeteilt. Auch die neuen Verfahren müssen so ausgestaltet sein, dass sie die Funktionen, die bereits jetzt realisiert sind, unterstützen, d.h. u. a. die **automatisierte Rückmeldung des Ausgangs des Verfahrens** von der Staatsanwaltschaft an die Polizei sowie ein automatisationsunterstütztes **Löschverfahren** mit Löschfristenverwaltung. Darüber hinaus sollte auch die ermittelnde bzw. mit der Bearbeitung eines Vorgangs beauftragte Polizeidienststelle über den Ausgang des Verfahrens unterrichtet werden. Der **Zugangsschutz** zu den Systemen (Chipkartenlösung) kann und sollte verbessert werden.

Ich stehe im engen Kontakt mit den anderen Datenschutzbeauftragten, um das Projekt INPOL-neu auf Bundesebene so

intensiv, wie es die personellen Ressourcen erlauben, zu begleiten und die mit der Umsetzung beauftragten Stellen im Lande Bremen bei der Ausgestaltung des Datenschutzes zu beraten.

Doch liegt auf der Hand, dass eine ausreichende datenschutzrechtliche Begleitung eines derart umfangreichen Projekts, das sich in über 200 Arbeitspakete mit über 6000 Unterprojekten gliedert, die Möglichkeiten selbst der gebündelten Kapazitäten aller Datenschutzbeauftragten des Bundes und der Länder übersteigt. Die Eile, mit der das Verfahren jetzt bis zum Jahr 2000 realisiert werden soll, gibt zur Befürchtung Anlaß, dass nicht alle aus datenschutzrechtlicher Sicht relevanten Fragen hinreichend bedacht und geklärt werden können. Zu befürchten ist auch, dass angesichts der derzeit noch vielen unfertigen Teile von INPOL-Neu vor dessen Einführung kaum ausreichende Möglichkeiten bestehen werden, die Anwender für das neue Verfahren hinreichend zu schulen. Insgesamt birgt die Umstellung auf das neue Verfahren noch **erhebliche Risiken für Datenschutz und Datensicherung**.

9.5. Neue Volkszählung - EG-weiter Zensus 2001?

9.5.1. Bundesmodell versus Landesmodell

Für das Jahr 2001 ist beabsichtigt, erneut eine Volkszählung durchzuführen. Das Vorhaben ist zurückzuführen auf den Vorschlag einer **gemeinschaftsweiten Volks- und Wohnungszählung** in der Europäischen Union und eine hierzu vom Statistischen Amt der Europäischen Gemeinschaft Ende 1997 vorgelegte “Leitlinie für das gemeinschaftliche Programm der Volks- und Wohnungszählung im Jahre 2001”. Aus Kosten- und Akzeptanzgründen soll die Zählung allerdings nicht wie die im Jahre 1987 als Primärerhebung direkt bei allen Einwohnern, sondern vor allem durch die Nutzung bei den Behörden vorhandener Datenbestände wie z.B. der

Melderegister durchgeführt werden. Die beim Statistischen Bundesamt eingerichtete Arbeitsgruppe "Gemeinschaftsweiter Zensus 2001” hat in der Zwischenzeit zwei Modelle zur Durchführung der neuen Volkszählung erarbeitet, die sich derzeit noch in der Diskussion befinden. Es handelt sich hierbei um ein sogenanntes "Bundesmodell” und ein sogenanntes "Ländermodell”.

Zum **Bundesmodell** gehören ein demographischer Teil, bei dem aus dem Einwohnermelderegister demographische Grunddaten wie z. B. Alter, Geschlecht, Familienstand, Staatsangehörigkeit, Religionszugehörigkeit gewonnen werden, ein erwerbsstatistischer Teil, bei dem aus Dateien der Bundesanstalt für Arbeit (z. B. Beschäftigtendateien, Arbeitslosendateien), Dateien anderer Behörden sowie vorhandenen Statistiken vielfältige Daten über Erwerbstätigkeit erhoben werden sollen, sowie ein **erweiterter Mikrozensus**, bei dem durch die stichprobenartige Befragung von 1% der Bevölkerung ausführliche Informationen über Haushalte, Wohnungen und Gebäude sowie den Bildungsstand erfragt werden sollen. Das Bundesmodell sieht keine flächendeckende Datenerhebung bei der Bevölkerung vor; statt dessen werden stichtagsbezogen **vorhandene Verwaltungsregister ausgewertet** und eine ergänzende Stichprobenbefragung durchgeführt. Im Unterschied zum Ländermodell sind keine personenbezogenen bzw. einzelfallbezogenen Verknüpfungen zwischen den in den Zensus einbezogenen Dateien und Statistiken und demgemäß auch keine entsprechenden Auswertungen, d. h. Merkmalskombinationen der Dateien aus den verschiedenen Quellen, vorgesehen. Bei diesem Modell sollen die einzelnen Erhebungsteile nicht personenbezogen miteinander verknüpft werden.

Auch das sog. **Ländermodell** sieht **keine flächendeckende Befragung** der Bevölkerung vor. Es besteht aus einem Grundmodul zur Gewinnung demographischer Grunddaten, gebäude- und wohnungsstatistischer Daten sowie Angaben über die Haushaltssituation, und einem Ergänzungsmodul zur Gewinnung erwerbsstatistischer Daten. Für das Grundmodul sollen Daten aus dem Einwohnermelderegister wie beim Bundesmodell gewonnen, eine postalische Gebäude- und Wohnungszählung durch die Befragung von Gebäudeeigentümern und Hausverwaltungen und im Anschluß hieran eine personenbezogene Zusammenführung mit den Melderegisterdaten zu einer Grunddatei durchgeführt werden. Für das Ergänzungsmodul sollen Daten aus den Dateien der Bundesanstalt für Arbeit und aus Erwerbsstatistiken und Dateien anderer Behörden in Bund, Ländern und Kommunen gewonnen sowie ergänzend hierzu eine **postalische primärstatistische Stichprobenerhebung** bei Personengruppen, für die keine Erwerbstätigendaten vorliegen, durchgeführt werden. Eine personenbezogene bzw. einzelfallbezogene Verknüpfung der gewonnenen Datensätze ist bei diesem Modell vorgesehen, so dass die Kombination und Auswertung von Merkmalen und Daten unterschiedlicher Herkunft möglich wird.

9.5.2. Datenschutzrechtliche Aspekte

Gemein ist beiden Modellen die große Bedeutung der **Einwohnermelderegister**. Der Erfolg beider Modelle ist mit der Qualität der Melderegister eng verbunden, so dass Bemühungen verstärkt wurden (auch in Bremen), die Qualität der Melderegister zu verbessern (z.B. Berichtigung und Fortschreibung von Amts wegen, Unterrichtung der Meldebehörden durch die Empfänger von Meldedaten, Überprüfung von Haupt- und Nebenwohnungen, beschleunigte Rückmeldungen und Fortschreibungen des Registers).

Ob letztendlich das Bundes- oder das Ländermodell durchgeführt wird, ist offen. Hier treffen derzeit noch die

unterschiedlichen Informationsbedürfnisse von Bund, Ländern und Kommunen sowie der EU zum Teil konträr aufeinander. Festzustellen unter Datenschutzgesichtspunkten ist jedoch die Tatsache, dass die neue Volkszählung nicht mehr in Form einer Totalerhebung bei allen Einwohnern, sondern hauptsächlich in Form einer Registerauswertung vorgenommen werden soll, insofern also ein "Paradigmenwechsel", d.h. **die Umstellung von einer Primär- auf eine Sekundärstatistik**, erfolgt. Dadurch können sicherlich die Widerstände in der Bevölkerung gegen eine Totalerhebung vermieden werden. Ob allerdings der informationelle Eingriff des Staates in die geschützte Rechtssphäre des Bürgers dadurch geringer ausfällt, hängt vom gewählten Modell und vom gewünschten Datenvolumen ab.

Der Senator für Inneres hat mir im Oktober 1998 in einem Schreiben mitgeteilt, dass er unter Berücksichtigung der angespannten bremischen Haushaltslage für seinen Verantwortungsbereich das wesentlich kostengünstigere und wohl auch "datenschutzfreundlichere" Bundesmodell vorziehen würde. Hierbei ist allerdings zu sehen, dass kommunalstatistische Bedürfnisse aufgrund der besonderen stadtstaatlichen Struktur im Bundesland Bremen eine geringere Bedeutung haben.

Zwingende Voraussetzung für eine neue Volkszählung ist aus meiner Sicht ein den datenschutzrechtlichen Anforderungen entsprechendes **neues Volkszählungsgesetz**, aus dem klar hervorgeht, welche Daten bei welchen Betroffenen erhoben oder aus welchem Register übermittelt werden dürfen, wo und durch wen sie mit welchen Verknüpfungen gespeichert und wann sie gelöscht werden sowie welche Daten weitergegeben bzw. übermittelt werden dürfen. In das Recht auf informationelle Selbstbestimmung darf dabei nur so gering wie möglich eingegriffen werden. Personenbezogene Daten, die für die

Statistik erhoben werden, dürfen von den Statistischen Ämtern nicht an die Verwaltung zurückfließen. Dies schließt auch aus, dass andere Behörden, z.B. die Meldebehörden, mit statistischen Aufgaben betraut werden, wie es zeitweilig geplant war. Ich hoffe, dass diese datenschutzrechtlichen Anforderungen bei der bevorstehenden Gesetzgebung zum Zensus 2001 beachtet werden.

9.6. Stagnation im Melderecht

In meinem letzten Jahresbericht hatte ich ausführlich (vgl. Ziffer 12.8.1.) über die auch aus datenschutzrechtlicher Sicht bestehende Notwendigkeit zur **Änderung des Bremischen Meldegesetzes** und über den Verstoß Bremens gegen die Verpflichtung aus Art. 75 Abs. 3 Grundgesetz zur Angleichung an das Melderechtsrahmengesetz berichtet. Leider hat der Senat in seiner Stellungnahme zu meinem 20. Jahresbericht zu diesem Punkt nichts gesagt. Der **Datenschutzausschuß** der Bremischen Bürgerschaft hat in seinem Abschlußbericht für das Plenum (Drucks. 14/1321, S. 2, abgedr. oben Ziff. 7.1.) die Erwartung geäußert, dass noch in dieser Legislaturperiode ein Gesetzentwurf zur Novellierung des Bremischen Meldegesetzes vorgelegt wird, wofür aber bis zum Redaktionsschluß keine Anzeichen erkennbar waren. Die Novellierung dieses Gesetzes bleibt bis zur Verabschiedung einer Gesetzesänderung in der Bremischen Bürgerschaft weiterhin auf der politischen Tagesordnung.

Berichtet hatte ich auch über die erfolgte Änderung der Bremischen **Meldedatenübermittlungsverordnung** und die zurückgestellten Änderungswünsche zu dieser Rechtsverordnung (20. JB, Ziff. 12.8.2.). Mit dem Senator für Finanzen habe ich zwischenzeitlich eine Abstimmung über seinen Änderungswunsch betreffend die Einbeziehung der Steuerfahndung in den Kreis der regelmäßigen Datenempfänger mit einem etwas erweiterten Datenkatalog herbeigeführt.

Abstimmungsgespräche mit anderen Senatsbereichen zu dieser Thematik haben im Berichtsjahr nicht stattgefunden. Doch gibt es immer wieder neue Begehrlichkeiten für online-Zugriffe weiterer Behörden auf das gesamte (!) Melderegister. Die rechtlichen Voraussetzungen für die Zulassung neuer Direktabrufe werde ich aber wie bisher restriktiv bewerten.

Auch die Übermittlung von **Meldedaten an Parteien und an Adressbuchverlage** beschäftigt mich, nicht zuletzt wegen immer wiederkehrender Bürgerbeschwerden, seit Jahren, in diesem Jahr (1999) wegen der mehrfachen Wahlen im Bundesland Bremen sicher wieder besonders (vgl. zuletzt hierzu 20. Jahresbericht, Ziff. 12.8.1.2. und 12.8.1.3.). Der Senat hatte in seiner Stellungnahme zu meinem 20. Jahresbericht erklärt, dass die Datenübermittlung an Adressbuchverlage im Zusammenhang mit der Novellierung des Bremischen Meldegesetzes diskutiert werden sollte, die aber noch nicht abesehbar ist. Zur Datenübermittlung an politische Parteien hatte der Senat erklärt, dass er es nicht für erforderlich halte, die Weitergabe der Daten ausschließlich an Parteigliederungen im Lande Bremen gesetzlich zu regeln. Zur zentralen Frage, die Meldedatenübermittlung an politische Parteien an die **Einwilligung** der Betroffenen zu knüpfen, hat der Senat nicht Stellung genommen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in einer Entschließung vom 5./6.10.1998 für diese Einwilligungslösung ausgesprochen (abgedr. unten Ziff. 20.4.).

Der **Datenschutzausschuß** der Bremischen Bürgerschaft hat in seinem Bericht an das Plenum (vgl. oben Ziff. 7.1.) seine Erwartung geäußert, dass bei der Erarbeitung des Entwurfs für ein novelliertes Meldegesetz die bisherigen

Übermittlungsregelungen für Parteien und Adreßbuchherausgeber überprüft werden.

9.7. Gewerbemeldungen: Übermittlung nicht gegen Widerspruch

Nach § 14 der Gewerbeordnung (GewO) sind Gewerbetreibende verpflichtet, sich bei der zuständigen Gewerbemeldestelle an- und abzumelden bzw. Veränderungen mitzuteilen. Diese Daten werden in das Gewerbemelderegister aufgenommen. In anderen Ländern bestehen zu dieser gesetzlichen Vorschrift bereits entsprechende Erlasse, die Ausführungshinweise für die zuständigen Behörden geben. Im Sommer 1998 hat jetzt auch der Senator für Wirtschaft, Mittelstand, Technologie und Europaangelegenheiten einen **Erlaßentwurf** vorgelegt.

Darin wird insbesondere im einzelnen bestimmt, an welche öffentlichen Stellen zu welchem Zeitpunkt Daten aus diesen Meldungen zu übermitteln sind. In diesem Zusammenhang soll auch die automatisierte Datenübermittlung (Abrufverfahren) an dritte Behörden geregelt werden.

Eine weitere vorgesehene Regelung könnte den Anlaß für eine Reihe von Beschwerden beseitigen: Nach § 14 Abs. 8 GewO können die Grunddaten der Gewerbetreibenden bei Vorliegen eines glaubhaft gemachten berechtigten Interesses grundsätzlich an private Stellen, d.h. insbesondere Berufsverbände, Markt- und Meinungsforschungsunternehmen, Adressbuchverlage und Versicherungen, übermittelt werden. Ich vertrete seit langem die Auffassung, dass auch bei Vorhandensein berechtigter, zumeist kommerzieller, Interessen der Datenempfänger der einer Übermittlung entgegenstehende Wille einzelner Gewerbetreibender, d. h. ihr **Widerspruch gegen die Datenweitergabe**, zu beachten ist. Dieser Auffassung hat sich der Senator für Wirtschaft, Mittelstand, Technologie und Europaangelegenheiten nunmehr angeschlossen. Tritt der Erlaß in Kraft, was ich mir möglichst bald wünsche, können

zukünftig Gewerbetreibende darauf vertrauen, dass ihre Daten nicht gegen ihren Einspruch für geschäftliche Zwecke Dritter übermittelt werden.

9.8. ID Cash - Haushaltskontrolle mit Bürgerdaten

Mit dem Verfahren ID Cash (Control Access System Haushalt) wird der Senator für Inneres in die Lage versetzt, alle Zahlungsbewegungen seines senatorischen Bereichs, also einschließlich der nachgeordneten Ämter, laufend zu beobachten. Die im Zugriff stehenden Datensätze enthalten jedoch auch **personenbezogene** Daten von Bürgerinnen und Bürgern, und zwar immer dann, wenn sie eine Zahlung von der Landeshauptkasse erhalten oder an sie leisten. Die Daten sollen über sechs Jahre aufbewahrt werden.

Zu ID Cash wurden bereits im Juli 1998 in der Innendeputation kritische Fragen gestellt. Auch der Datenschutzausschuß hat sich damit befaßt und sich vorgemerkt, dieses Thema erneut aufzugreifen.

Ich habe den Innensenator darauf hingewiesen, dass ich für einen derart umfassenden zentralen Zugriff auf eine Unmenge personenbezogener Angaben über Bürger und Mitarbeiter **keine Rechtsgrundlage** sehe. Viele der Zahlungsvorgänge, die über die Landeshauptkasse abgewickelt werden, enthalten sensible persönliche Informationen (z.B. Zahlung von Geldbußen).

Allerdings hat mir der Innensenator bis heute nicht dargelegt, welchen genauen Zwecken die Anwendung überhaupt dienen soll. Sollte sie für **Controlling- bzw. Berichtszwecke im Sinne von § 7 LHO** gedacht sein, kann auf personenbezogene Daten weitgehend verzichtet werden, wie dies die Ausgestaltung des Kosten- und Leistungsrechnungsverfahrens des Senators für Finanzen (KLR) deutlich belegt (vgl. u. Ziff. 17.3.).

Ich habe den Innensenator aufgefordert, zur Rechtsgrundlage Stellung zu nehmen und ein **Datenschutzkonzept** vorzulegen. Falls die Frage nach dem Zweck von ID Cash und seiner Rechtsgrundlage nicht befriedigend beantwortet oder der Personenbezug der abgerufenen Datensätze nicht beseitigt wird, kann das Verfahren nicht weiter benutzt werden.

10. Justiz

10.1. DNA-Analysedaten für die Zwecke der Strafverfolgung

10.1.1. Neue Rechtsgrundlage für die zentrale "Gendatei"

Im Berichtszeitraum sind vor allem im Rahmen der Suche nach Tätern von Kinderschändungen und –morden, aber auch im Zusammenhang mit anderen Gewaltdelikten wie z.B. Vergewaltigungen zahlreiche "Gentests" durchgeführt bzw. "genetische Fingerabdrücke" erhoben worden. Die öffentliche Aufmerksamkeit und das Interesse der Medien für dieses neue Ermittlungsinstrument waren und sind hoch. Der Gesetzgeber hat kurz vor Ende der letzten Legislaturperiode mit dem sog. DNA-Identitätsfeststellungsgesetz (BGBl. 1998/I, 2646) reagiert.

Allerdings wurden die für die Durchführung von DNA-Analysen **im Strafverfahren** erforderlichen gesetzlichen Voraussetzungen zum Teil bereits im Frühjahr **1997** geschaffen. Der Deutsche Bundestag hat am 17.03.1997 mit einem **Strafverfahrensänderungsgesetz** (vgl. BGBl. I, S. 534 f.) die Voraussetzungen und Grenzen molekular-genetischer Untersuchungen (in Fachkreisen kurz DNA-Analyse genannt) geregelt.

Die Vorschriften der **§§ 81 e und f** StPO, die durch das damalige Gesetz in die Strafprozeßordnung eingefügt worden sind, regeln die Zulässigkeit von molekular-genetischen Untersuchungen an Körpermaterial, das durch körperliche Eingriffe nach §§ 81a oder 81c StPO bei Verfahrensbeteiligten gewonnen

worden ist. § 81e StPO gestattet darüber hinaus die Vornahme entsprechender Untersuchungen an Spurenmaterial, das die Strafverfolgungsorgane ohne körperlichen Eingriff erlangt haben. § 81f StPO sieht vor, dass entsprechende Untersuchungen nach § 81e StPO nur durch den Richter angeordnet werden dürfen, und trifft weitere organisatorische und technische Maßnahmen für die Durchführung der DNA-Analyse durch Sachverständige. Schließlich führte die Neuregelung eine anlaßunabhängige (verdachtsunabhängige) Datenschutzkontrolle bei den die DNA-Analyse durchführenden Instituten vor.

Diese Regelungen, die ich zusammen mit den anderen Datenschutzbeauftragten des Bundes und der Länder kritisch begleitet habe (vgl. die Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, abgedruckt im 20. JB, Ziff. 22.2.), lassen aber nur zu, dass Blutproben und sonstige Körperzellen, die dem **Beschuldigten** entnommen worden sind, für Zwecke des der Entnahme zugrundeliegenden oder eines anderen anhängigen Strafverfahrens verwendet werden dürfen. Die Untersuchung ist daher nur insoweit zulässig, als sie in einem **anhängigen Strafverfahren** erforderlich ist. Die Untersuchungen des Materials dürfen sich dabei nur darauf beschränken, festzustellen, ob aufgefundenes Spurenmaterial von dem Beschuldigten oder dem Verletzten stammt oder ob es einer anderen Person zugerechnet werden muß. Eine **weitere Aufbewahrung und Verwendung** der mittels DNA-Analyse gewonnenen Informationen ist damit **nicht vorgesehen**. Die Materialien müssen unverzüglich vernichtet werden, sobald sie für das jeweilige anhängige Strafverfahren nicht mehr erforderlich sind.

Eine völlig neue Dimension bedeutete die Absicht des damaligen Bundesinnenministers Kanther und des Bundeskriminalamts, eine bundesweite **zentrale DNA-Datenbank** aufzubauen, in die alle in den Ländern bisher und in Zukunft gewonnenen DNA-Analysedaten eingespeichert und zum Abruf bereitgehalten werden sollten. Hierzu erließ der Bundesinnenminister im Sommer 1998 ohne gesetzliche Absicherung eine sog. Errichtungsanordnung. Wegen der hohen Eingriffsintensität einer solchen zentralen Registrierung sensibler Daten habe ich mich zusammen mit meinen Kollegen von vornherein nachdrücklich gegen eine solche bundesweite "Gendatei" ohne eine gesetzliche und damit parlamentarisch verantwortete Rechtsgrundlage gewandt.

Die neue Dimension ergibt sich aus der Zielsetzung, die einmal gewonnenen Vergleichsdaten nicht nur im ursprünglichen Strafverfahren, sondern auch zu **präventiv-polizeilichen Zwecken** sowie zur **Vorbeugung und Aufklärung späterer Straftaten** nutzen zu können. Dies sind die Regelungszwecke des **DNA-Identitätsfeststellungsgesetzes**, das am 07.09.1998 in Kraft getreten ist. Das Gesetz fügt in die Strafprozeßordnung den **§ 81g** ein. Er enthält Regelungen zur Entnahme von Körperzellen zur Erstellung eines DNA-Identifizierungsmusters bei Straftatbeschuldigten ebenso wie bei bereits rechtskräftig Verurteilten, und erlaubt die Speicherung dieser DNA-Identifizierungsmuster in einer Datei beim Bundeskriminalamt. Hinsichtlich der Verwendung dieser Daten wird allerdings nur auf die Regelungen des BKA-Gesetzes verwiesen.

Die Datenschutzbeauftragten des Bundes und der Länder hatten die Mindestanforderungen an eine solche Regelung frühzeitig formuliert (vgl. die o.a. Konferenzentschließung). Anläßlich der Beratung des Gesetzentwurfs im Rechtsausschuß des

Bundesrates habe ich vor allem eine Beachtung folgender Punkte angemahnt:

Für die Anordnung der Abnahme eines genetischen Fingerabdrucks muß ein **klarer Katalog schwerer Straftaten** gelten. Die Öffnungsklausel "sonstige Straftaten von erheblicher Bedeutung" ist konturlos und verstößt angesichts der Eingriffstiefe in das Persönlichkeitsrecht der Betroffenen gegen das Verhältnismäßigkeitsprinzip.

Voraussetzung für Gen-Tests muß **in jedem Fall eine Prognoseentscheidung** des anordnenden Richters sein, wonach wegen der Tatausführung oder der Persönlichkeit des Täters die Begehung weiterer schwerer Straftaten zu erwarten ist.

Die **Verwendung** der gespeicherten genetischen Daten kann nicht nur durch pauschale Verweisungen auf das Bundeskriminalamtsgesetz geregelt werden. Auszuschließen ist insbesondere, dass die DNA-Ergebnisse – wie es das BKA-Gesetz zuließe – an Behörden übermittelt werden, die nichts mit der Strafverfolgung zu tun haben.

Ein grundsätzliches **Verbot der Speicherung** solcher Analyseergebnisse, die inhaltliche **Aussagen über Erbanlagen** ermöglichen, also der sogenannten codierenden Bereiche, ist gesetzlich festzuschreiben.

Einige, aber nicht alle diese Punkte sind vom Gesetzgeber berücksichtigt worden.

10.1.2. Umsetzungsprobleme in der Praxis

Das DNA-Identitätsfeststellungsgesetz läßt ein ganzes Bündel von **Umsetzungsfragen für die Praxis** offen. Hierzu zählt vor allem die Handhabung der Regelungen durch die **Staatsanwaltschaft** in erledigten Strafverfahren, in denen es zur Verurteilung gekommen ist. Das DNA-Identitätsfeststellungsgesetz

verpflichtet nämlich auch bei abgeschlossenen und somit zurückliegenden Strafverfahren, in bestimmten Fällen eine nachträgliche DNA-Analyse und eine rückwirkende Erfassung dieser Daten in der Zentraldatei des BKA vorzunehmen. Um geeignete Fälle zu finden, hat man sich auf Bundesebene auf eine entsprechende Auswertung des Bundeszentralregisters verständigt. Dazu muß das geltende Bundeszentralregistergesetz allerdings noch geändert werden, was bereits in die Wege geleitet worden ist.

Weiter ist die Staatsanwaltschaft als Strafvollstreckungsbehörde in Zusammenarbeit mit den **Justizvollzugsanstalten** im Zuge des Gesetzesvollzuges gehalten, in geeigneten Fällen vor Entlassung von Strafgefangenen sicherzustellen, dass diesen entsprechendes molekular-genetisches Material entnommen wird.

Ergänzend zu den gesetzlichen Regelungen hat der Senator für Justiz und Verfassung für seinen Bereich die in einer länderübergreifenden Arbeitsgruppe des Strafrechtsausschusses erarbeiteten **"vorläufigen Hinweise zum DNA-Identitätsfeststellungsgesetz"** mit Stand vom 08.10.1998 gegenüber der Staatsanwaltschaft in Kraft gesetzt und die Strafgerichte hierüber unterrichtet. Bedauerlicherweise wurde nach meinen Informationen keinem Datenschutzbeauftragten die Möglichkeit gegeben, zu diesen Hinweisen eine Stellungnahme abzugeben. Nicht zuletzt deshalb ist eine Reihe von Fragen aus datenschutzrechtlicher Sicht nicht oder nicht zufriedenstellend behandelt worden.

So bleiben z. B. die folgenden Fragen klärungsbedürftig:

Wer entscheidet über die Einleitung eines Verfahrens zur Durchführung von DNA-Analysen? Welche Behörde ist örtlich zuständig? Ist an den Wohnort, den Ort der Vollstreckung oder den Ort der Verurteilung anzuknüpfen?

Welche Dateien dürfen zur Gewinnung von Daten über Personen herangezogen werden, denen nachträglich eine DNA-Materialprobe entnommen werden soll?

Wer entscheidet über die Aufnahme von DNA-Identifizierungsdaten, die bereits früher zum Zwecke der Aufklärung einer bestimmten Straftat erlangt worden sind, in die Zentraldatei des BKA, und ist hierzu ein besonderer richterlicher Beschluß erforderlich?

Nicht nur bei der Justiz, auch bei der **Polizei** bedarf es noch vergleichbarer Entscheidungen bzw. Regelungen zur Durchführung des neuen Gesetzes.

Ein Teil dieser Fragen ist bereits im **Datenschutzausschuß** mit Vertretern des Senators für Justiz und Verfassung und des Senators für Inneres behandelt worden. Der Vertreter des Senators für Inneres hat mir zugesichert, mich über die weitere Entwicklung auf dem laufenden zu halten und mir die Möglichkeit zur Stellungnahme einzuräumen.

Dies gilt auch für die endgültige Festlegung der Bedingungen für den Aufbau der zentralen DNA-Identitätsdatei beim Bundeskriminalamt. Hierfür muß das Bundeskriminalamt eine **Errichtungsanordnung** erlassen, in der u.a. die aufzunehmenden Personen, Inhalt und Umfang der Datensätze, Aufbewahrungsdauer und Löschungsprüffristen zu bestimmen sind. Der Senator für Inneres hat mir den Entwurf einer Errichtungsanordnung zugeschickt. Meine dazu abgegebene Stellungnahme hat er an das Bundeskriminalamt weitergeleitet.

Zusammenfassend ist festzustellen, dass einige der jetzt auftretenden Probleme nicht Polizei und Justiz der Länder anzulasten, sondern Ausfluß der nicht ausreichend durchdachten Gesetzgebung sind. Ich habe mir für den

laufenden Berichtszeitraum zur Aufgabe gesetzt, die Umsetzungsmaßnahmen auf Landesebene kritisch zu begleiten und zu überprüfen.

10.2. JVA Blockland - Besucherregelung jetzt datenschutzgerecht

Eine Forderung, die ich aus der umfassenden Datenschutzprüfung der JVA Oslebshausen im Jahr 1993 (vgl. 16. JB, Ziff. 6.1.3) abgeleitet hatte, sah vor, die Kontrollprozedur für Besucher von Häftlingen nicht mehr stattfinden zu lassen, ohne dass die Betroffenen überhaupt von ihrer beabsichtigten Einladung wußten. Das inzwischen geänderte Verfahren der Überprüfung zur Erlangung einer Besuchserlaubnis, die Aufbewahrung der Besucheranträge sowie die Dokumentation durchgeführter Besuche habe ich vor Ort in der Teilanstalt Blockland geprüft.

Jetzt stellt zunächst der Besucher einen Antrag auf Eintragung in die Besucherkartei. Der Antrag wird dann dem Gefangenen zur Einverständniserklärung vorgelegt. Der Gefangene teilt dem Besucher telefonisch oder schriftlich das Ergebnis (erteilte/abgelehnte Besuchserlaubnis) mit. Die Anträge werden in der **Gefangenenpersonalakte** abgelegt und bis fünf Jahre nach Entlassung aufbewahrt.

An der Pforte werden alle Besuche anstaltsfremder Personen mit Datum, Name, Vorname, Begehren und Verweildauer in einem **Passagebuch** eingetragen. Es enthält Eintragungen über einen Zeitraum von ca. sechs Monaten. Die Bücher werden 5 Jahre aufbewahrt und dann vernichtet. Besuche werden zusätzlich in der **Besucherkartei** dokumentiert. Die Kartei wird nach Entlassung des Gefangenen an die Vollzugsgeschäftsstelle weitergeleitet und dort vernichtet.

Damit ist die Forderung nach einem datenschutzgerechteren Antragsverfahren für JVA-Besucher erfüllt.

10.3. Bundeszentralregister - Schuldunfähigkeit "ewig" gespeichert?

Aufgrund einer Eingabe bin ich auf die Rechtslage aufmerksam geworden, dass die Einstellung eines Strafverfahrens wegen Schuldunfähigkeit nach § 11 Abs. 1 Nr. 1 Bundeszentral-registergesetz (BZRG) in das Bundeszentralregister einzutragen ist und diese Eintragungen ohne jede weitere Differenzierung nach Deliktsart o.ä. nach § 24 BZRG nicht vor dem 90. Lebensjahr oder dem Tod des Betroffenen aus dem Register entfernt werden. Während also Verurteilungen schuldfähiger Täter nach differenzierten Fristen getilgt werden, bleibt der Schuldunfähige gleichsam **"lebenslänglich"** in der Datei. Im konkreten Fall wurde dem überraschten Eingeber, der von der Tilgung ausgegangen war, die Eintragung mehrere Jahrzehnte nach ihrer Aufnahme in das BZR vorgehalten.

Allerdings kann der Generalbundesanwalt nach § 25 Abs. 1 BZRG auf **Antrag** des Betroffenen oder von Amts wegen im Benehmen mit der Stelle, welche die Entscheidung getroffen hat, insbesondere im Interesse der **Rehabilitation** des Betroffenen anordnen, dass derartige Eintragungen entfernt werden, soweit nicht das öffentliche Interesse einer solchen Anordnung entgegensteht. Vor seiner Entscheidung soll der Generalbundesanwalt einen in der Psychiatrie erfahrenen medizinischen Sachverständigen anhören.

Ich habe den Betroffenen über diese Rechtslage unterrichtet und ihm anheimgestellt, einen entsprechenden Antrag beim Generalbundesanwalt zu stellen. Im übrigen hat mir der Bundesbeauftragte für den Datenschutz auf Anfrage mitgeteilt, das Bundesjustizministerium bereite eine Gesetzesänderung in bezug auf die Dauer der Speicherung vor. Bei dieser Gelegenheit solle auch vorgesehen werden, dass die Registerbehörde den Betroffenen über eine derartige

Eintragung und sein Antragsrecht auf Tilgung bei Vorliegen der in § 25 Abs. 1 BZRG geregelten Voraussetzungen zu **unterrichten** hat.

11. Gesundheit/Krankenversicherung

11.1. Bremisches Krebsregister - Einführungsprobleme

11.1.1. Datenverarbeitungskonzept zu spät fertiggestellt

Zum 1.10. 1997 trat das **Bremische Krebsregistergesetz (BremKRG)** in Kraft. Damit war die Grundlage dafür gelegt, entsprechend der Vorgabe des Krebsregistergesetzes des Bundes (KRG) spätestens zum 01.01.1999 ein Bremisches Krebsregister einzurichten. In meinem 20. Jahresbericht habe ich unter Ziff. 14.1 ausführlich dargestellt, dass gerade die in Bremen gewählte Ausgestaltung des Registers, wenn auch aus mir plausiblen Gründen, in Abweichung von dem bundesgesetzlichen Modell die dauerhafte Speicherung der Identitätsdaten der Betroffenen in der Vertrauensstelle vorsieht und deshalb besondere Anforderungen an die zum Schutz der Persönlichkeitsrechte der registrierten Krebspatienten zu treffenden technischen Vorkehrungen stellt. Es standen jedoch immerhin 15 Monate zur Verfügung, um das anspruchsvolle und sensible Projekt durch Entwicklung eines Datenverarbeitungskonzepts vorzubereiten. Leider wurde diese Zeit nicht in vollem Umfang genutzt. Zwar wurde bereits im Januar 1998 verkündet, in Bremen sei man soweit, rückwirkend zum Beginn des Jahres die Daten krebskranker Bremer zu registrieren. Trotz meiner Hinweise aus dem Herbst 1997, dass man **rechtzeitig** mit den Vorbereitungen der Registrierung von Patientendaten beginnen müsse, tat sich vor der Besetzung der Stellen für die Vertrauensstelle zum 01.04.1998 durch die mit deren Betrieb beauftragte Kassen-ärztliche Vereinigung nichts.

Zwar lag mir dann bereits Ende Mai 1998 der 1. Entwurf eines Datenverarbeitungskonzepts vor. Dieser genügte aber in wichtigen Punkten noch nicht den gesetzlichen Anforderungen. Dies scheint mir zum einen daran zu liegen, dass man noch nicht im vollen Umfang akzeptieren wollte, dass das BremKRG einen **besonders hohen Sicherheitsstandard** fordert. Zum anderen aber ergaben sich erst jetzt bei der "Feinarbeit" immer neue Detailprobleme, für deren Lösung das Gesetz keine klaren Vorgaben machte.

Man hatte mir aber bereits im August angekündigt, man müsse auch ohne Datenverarbeitungskonzept beginnen, Daten für das Register zu erheben. Dies hieß, die Ärzte aufzufordern, Patienten zu melden, obgleich die Vertrauensstelle mangels technischer Voraussetzungen die Meldungen lediglich lagern, aber nicht im Sinne der BremKRG verarbeiten konnte und durfte. Ich wies die Beteiligten darauf hin, dass man damit gegen das Gesetz verstoße, das von der Vertrauensstelle verlange, die Meldungen unverzüglich durch Trennung der medizinischen Daten von den Identitätsdaten und Weiterleitung der erstgenannten Datenart an die Registerstelle zu bearbeiten. Ich konnte von einer **formellen Beanstandung** nur **absehen**, weil ich auf Grund der im übrigen guten Kooperation keine Zweifel an Bereitschaft und Fähigkeit der zuständigen Stellen zur Erstellung eines angemessenen Konzepts und damit zur Behebung des Verstoßes hatte.

Nachdem die **Vertrauensstelle** die Erstellung des Konzepts extern vergeben hatte, liegt jetzt seit Dezember 1998 eine **Konzeption** vor, deren Umsetzung eine gesetzmäßige Verarbeitung der dem Krebsregister gemeldeten Patientendaten in angemessenem Maße gewährleistet. Ich musste allerdings darauf hinweisen, dass eine Darstellung der installierten

Sicherheitskonfiguration nachzureichen sei. Die Steuerung und die Kontrolle des Rechnerzugangs über Chipkarten sowie einen maximal möglichen Schutz der Schnittstellen konnte ich nicht durchsetzen. Es fehlen noch Regelungen der zuständigen Stellen für die Aktualisierung der Identitätsdaten durch Abgleich mit dem Melderegister und vor allem zur Nutzung der Registerdaten für Forschungsvorhaben. Das **Datenverarbeitungskonzept der Registerstelle** ist noch nicht vollständig abgestimmt. Gleichwohl habe ich signalisiert, dass ich keine Einwände mehr gegen den Beginn der Meldungen an die Vertrauensstelle erhebe. Ohnehin wird es meine Aufgabe sein, die Umsetzung der Datenverarbeitungskonzepte vor Ort beratend und falls erforderlich kritisch zu begleiten.

Der **Datenschutzausschuß** hat sich bei der Beratung des 20. Jahresberichts mit der Entwicklung beim Bremischen Krebsregister befaßt und seine Erwartung geäußert, dass die datenschutzrechtlichen Vorgaben unverzüglich umgesetzt werden (vgl. o. Ziff. 7.1.).

11.1.2. Schwierigkeiten bei Meldung und Erfassung

Kurz vor Redaktionsschluss konnte ich mich bei einem Besuch der Vertrauensstelle davon überzeugen, dass man inzwischen damit begonnen hatte, die von behandelnden Ärzten eingesandten **Dokumentationsbögen elektronisch zu erfassen**. Damit sind endlich die Voraussetzungen geschaffen worden, die Meldungen gesetzmäßig zu verarbeiten. Ich gehe davon aus, dass letzte noch offene Fragen im Zusammenhang mit den Datenverarbeitungskonzepten von Vertrauens- und Registerstelle in Kürze einvernehmlich geklärt werden können.

Zugleich aber sind **neue Probleme** offenkundig geworden, wegen derer ich mich jetzt schriftlich an die Stellen des Krebsregisters und an das Gesundheitsressort gewandt habe.

Nicht alle Kliniken, die krebskranke Patienten behandeln, haben für ihre Meldungen die vom Senator für Gesundheit vorgegebenen Dokumentationsbögen benutzt, sondern der Vertrauensstelle sind auch in größerer Zahl Kopien der eigentlich für die nachbehandelnden Ärzte bestimmten **Arztbriefe**, die Klinikärzte über den gesundheitlichen Zustand von ihnen behandelter Patienten bei deren Entlassung verfasst haben, eingereicht worden. Dies ist natürlich nicht im Sinne des Gesetzes. Die Arztbriefe sind nicht standardisiert und enthalten zwangsläufig eine Fülle von Daten, deren Registrierung das BremKRG nicht vorsieht. Die Vertrauensstelle wäre gezwungen, aus den Arztbriefen mühsam die für sie relevanten Daten herauszufiltern, wollte sie sie für ihre Zwecke auswerten. Dies wäre aber ohnehin **unzulässig**: Weder berechtigt das BremKRG die Ärzte, der Vertrauensstelle die in den Unterlagen enthaltenen "Überschussdaten" zu übermitteln, noch berechtigt es die Vertrauensstelle, diese Daten zur Kenntnis zu nehmen. Die Vertrauensstelle hat mir versichert, sie "schreddere" derartige Arztbriefe unverzüglich nach ihrem Eingang. Zudem werde sie Ärzte und Krankenhäuser noch einmal ausdrücklich darum bitten, ihr Meldungen nur mit den gesetzlich zulässigen Patientendaten einzureichen.

Sowohl Vertrauensstelle als auch Registerstelle sehen es als ihre Aufgabe an, durch Rücksprache mit den meldenden Ärzten **Widersprüche zwischen mehreren** ein und denselben Patienten betreffenden **Meldungen** aufzuklären. Das Gesetz schreibt weder der einen noch der anderen der beiden Stellen diese Aufgabe ausdrücklich zu. Vielleicht mit gutem Grund: Die

Vertrauensstelle soll die medizinischen Daten unverzüglich an die Registerstelle weiterleiten, dieser wiederum ist es verwehrt, die Identität der jeweiligen Patienten zur Kenntnis zu nehmen. Die angestrebte Aufklärung der Widersprüche setzt aber die Kenntnis sowohl der widersprüchlichen medizinischen Daten als auch der Identität des jeweiligen Patienten voraus. Ein mit dem Gesetz vereinbares Verfahren setzt daher die Kooperation beider Stellen voraus. Stellt die Registerstelle Widersprüche zwischen zwei Meldungen zu ein und demselben Patienten fest - und dies ist ihr anhand der durch die Vertrauensstelle vergebenen Registernummer möglich - , so teilt sie dies der Vertrauensstelle mit, die sich wiederum nach Rücksprache mit den Meldern um Klärung bemüht, das Ergebnis der Registerstelle mitteilt und danach umgehend die in diesem Zusammenhang bei ihr gespeicherten medizinischen Daten löscht.

11.2. Das Patientengeheimnis in der Psychotherapie

11.2.1. Gefährdungen vor Inkrafttreten des Psychotherapeutengesetzes

Wer Hilfe in einer Psychotherapie sucht, vertraut in besonderem Maße darauf, dass der Therapeut seine **berufliche Schweigepflicht** wahrt. Viele Patienten tragen die Kosten selbst, damit Krankenkassen (oder bei Beamten die Beihilfestellen) keine Kenntnis davon erhalten. Psychotherapie ist jedoch teuer. Deshalb sind die Patienten meist darauf angewiesen, dass die Kosten von der Krankenkasse übernommen werden. Diese wiederum hat angesichts der hohen Kosten ein Interesse daran, auf der Grundlage ärztlicher Bescheinigungen und Dokumentationen des Therapeuten die Notwendigkeit und Effektivität der Therapie beurteilen zu können, genauer gesagt, durch externe Gutachter bzw. durch ihren medizinischen Dienst beurteilen zu lassen.

Die Eingabe eines Rechtsanwalts, der Psychotherapeuten vertritt, veranlasste mich, zu prüfen, ob das praktizierte Verfahren den Vertrauensschutz im gebührenden Maße beachtet. Dabei stellte ich fest:

Für die Therapien, die ein Arzt an einen Psychotherapeuten delegierte (Voraussetzung: bestimmte formale Qualifikationen des Therapeuten), war zwischen den Verbänden der Kassen und der Vertragsärzte ein Verfahren vereinbart, das den Anforderungen genügte. Die Kassen erhielten lediglich die gesetzlich vorgesehenen Unterlagen. Gutachten und Dokumentationen im übrigen erhielt die Kasse zur Weiterleitung an den Gutachter in verschlossenem Umschlag. Der Gutachter wiederum erhielt die für ihn bestimmten Unterlagen unter Kennziffer, d.h. ohne Identitätsdaten des Patienten.

Ganz anders aber sah es für die Therapien aus, deren Kosten die Kassen erstatteten, ohne dass die Therapeuten die Voraussetzungen für eine Delegation erfüllten (sog. "Erstattungstherapeuten" im Gegensatz zu den "Delegationstherapeuten"). Mir wurde vorgetragen und im Einzelfall auch durch Schrift-stücke belegt, dass die Kassen selbst Dokumentationen zur Kenntnis nahmen und der hier eingeschaltete Medizinische Dienst auch die **Identität des betroffenen Patienten** erfuhr.

Die von mir deshalb angeschriebenen Kassen antworteten auf meine entsprechenden Fragen deshalb nicht mehr, weil inzwischen das **Psychotherapeutengesetz (PsychThG) verabschiedet** worden war. Dies hat zum Ziel, dass die sog. "Erstattungstherapie" nicht mehr erforderlich ist, sondern dass alle erforderlichen Psychotherapien durch approbierte und zugelassene Therapeuten erbracht werden können. Es besteht Anlass zu der Erwartung, dass die datenschutzgerechten Regelungen für die Bewilligung von Therapien der sogenannten

"Delegationstherapeuten" in das Verfahren auf der Grundlage des neuen Gesetzes übernommen werden.

11.2.2. Psychotherapeutengesetz: Anonymisierung der Nachweise

Vorübergehend ergaben sich aber neue Probleme: In den Verfahren der Approbation durch die Landesgesundheitsverwaltungen bzw. der Zulassung als Vertragsärzte durch die von Kassen, Kassenärztlichen Vereinigungen und Berufsverbänden der Psychotherapeuten gebildeten Zulassungsausschüsse können bereits praktizierende Psychotherapeuten ihre Qualifikation nicht nur durch Nachweis des geforderten Ausbildungsabschlusses, sondern für eine Übergangszeit auch durch Vorlage von Dokumentationen über eine bestimmte Anzahl von Behandlungsfällen bzw. Behandlungsstunden nachweisen. § 12 PsychThG bzw. § 95 SGB V machen keine Aussage über die Art dieses Nachweises im einzelnen.

Die Gefahr bestand, dass die antragstellenden Therapeuten ihre Qualifikation durch **Vorlage patientenbezogener Unterlagen** nachweisen würden. Zeitlich war Eile geboten, da die **Approbationsverfahren** bis Anfang 1999 und die **Zulassungsverfahren** im unmittelbaren Anschluss daran "durchgezogen" werden sollten. Es war von vornherein beabsichtigt, für den Nachweis von Therapien, deren Kosten Kassen bzw. Beihilfestellen übernommen hatten, deren Bescheinigungen ("Fremdbescheinigungen") anzuerkennen. Demgegenüber zeichnete sich ab, dass gerade die Patienten, die die Kosten ihrer Therapie selbst getragen hatten ("Selbstzahler"), mit den vorgelegten Unterlagen den Approbationsbehörden bekannt würden - angesichts dessen, dass ein Teil dieser Patienten gerade um der Vertraulichkeit willen die Therapie selbst bezahlt hat, ein absurdes Ergebnis.

Die Datenschutzbeauftragten von Bund und Ländern wiesen übereinstimmend die Verbände der Psychotherapeuten und die Landesgesundheitsverwaltungen darauf hin, dass § 12 PsychThG die antragstellenden Therapeuten nicht befuge, ihre berufliche Schweigepflicht zu durchbrechen, sie daher Unterlagen mit den Identitätsdaten ihrer Patienten nur mit deren Einwilligung vorlegen dürften. Den Therapeuten solle empfohlen werden, **Kopien der Unterlagen ohne Identitätsdaten** vorzulegen. Allerdings werde man akzeptieren, wenn in Einzelfällen aus begründetem Anlass die Vorlage patientenbezogener Unterlagen verlangt würde.

Der Senator für Gesundheit hat daraufhin wie die Approbationsbehörden anderer Bundesländer eine entsprechende Empfehlung abgegeben und versichert, er werde patientenbezogene Unterlagen ohne vorgelegte Einwilligung der Patienten den Antragstellern zurückgeben. Meine Überprüfung der bis Mitte Oktober eingegangenen Unterlagen ergab nichts Gegenteiliges.

Ebensowenig darf dem Zulassungsausschuss für Psychotherapeuten die Identität von Patienten der antragstellenden Psychotherapeuten bekannt werden. Der Zulassungsausschuss für das Land Bremen entwickelte deshalb in Abstimmung mit mir **Vordrucke** und Erläuterungen, die eine **Anonymisierung** der Unterlagen, darunter auch der Falldokumentationen, vorsehen.

11.3. Schmerztherapie: Anonymisierung der Behandlungsdokumentationen

Ein Arzt machte mich mit seiner Eingabe auf eine der im vorigen Abschnitt dargestellten vergleichbare Problematik aufmerksam: Auch Ärzte können veranlasst sein, die Behandlung ihrer Patienten gegenüber einem gemeinsam von Vertragsärzten und Kassen gebildeten Gremium an Hand von **patientenbezogenen Unterlagen** zu dokumentieren. Ein

Beispiel: Die Kassenärztliche Bundesvereinigung hat mit den Spitzenverbänden der Krankenkassen vereinbart, die ambulante Behandlung chronisch Schmerzkranker durch besonders dafür qualifizierte Vertragsärzte sicherzustellen. Ein Arzt, der sich daran (mit der Folge, die entsprechenden Leistungen abrechnen zu können) beteiligen will, muss u.a. der Kassenärztlichen Vereinigung (KV) gegenüber die qualifizierte Therapie von 50 schmerzkranken Patienten dokumentieren. Über die Zulassung entscheidet dann eine von der KV gebildete Kommission.

Ebensowenig wie im Approbations- und im Zulassungsverfahren für Psychotherapeuten werden hier patientenbezogene Behandlungsunterlagen benötigt. Eine gesetzliche Befugnis für die Durchbrechung der Schweigepflicht des Arztes fehlt ebenso wie eine entsprechende Einwilligung der Patienten. Auf meinen entsprechenden Hinweis hat die KV Bremen erklärt, die Ärzte, die sich an der qualifizierten Schmerztherapie beteiligen wollten, könnten die eingereichten Unterlagen **anonymisieren**. Man berate die Ärzte auch entsprechend. Auf meine Anregung, durch einen Hinweis in den Antragsunterlagen die Ärzte schriftlich darüber zu informieren, habe ich bislang leider keine Antwort erhalten.

11.4. Sozialpsychiatrischer Dienst - Vorentwurf einer Datenschutzverordnung

Einerseits soll der Sozialpsychiatrische Dienst (SPsD) des Gesundheitsamts einen Teil seiner Kosten durch Abrechnung mit den Krankenkassen decken. Hierfür muss er die Abrechnungsunterlagen automationsgerecht einreichen. Andererseits ist die in § 33 Abs.3 des Bremischen **Gesetzes über den Öffentlichen Gesundheitsdienst (ÖGDG)** vorgesehene Rechtsverordnung über Art und Umfang der Datenverarbeitung im Gesundheitsamt als Grundlage für die Verarbeitung von Patientendaten noch nicht erlassen worden.

In Fortschreibung meiner ausführlichen Darstellung unter Ziff. 14.7 meines 20. Jahresberichts teile ich zur weiteren Entwicklung im Berichtszeitraum folgendes mit: Zur Überbrückung des zeitlich begrenzten Dilemmas war vereinbart, dass das Gesundheitsamt trotz Erwerbs von Software mit umfassenden Funktionen bis zum Erlass der Verordnung die EDV im SPsD durch technische und organisatorische Vorkehrungen auf Textverarbeitung und Abrechnung mit den Krankenkassen begrenzt. Im übrigen sollte das Sicherheitssystem mit dem Betriebssystem WINDOWS NT konfiguriert sein.

Zu meiner Verblüffung musste ich jedoch im Berichtsjahr bei einer Prüfung in einer regionalen Beratungsstelle des SPsD feststellen, dass die konzeptionell festgelegten und abgestimmten **Sicherheitsfeatures** technisch gar nicht **umgesetzt** worden waren. Nur die Zusicherung, den Mangel umgehend zu beheben, erlaubte es mir, von einer Beanstandung abzusehen. Inzwischen konnte ich mich bei einer erneuten Prüfung vor Ort davon überzeugen, dass Konzept und Umsetzung nunmehr sowohl miteinander als auch mit den mit mir getroffenen Absprachen übereinstimmen.

Der Zeitpunkt, zu dem die Datenverarbeitung im SPsD umfassend automatisiert werden darf, ist aber bereits abzusehen. Das Gesundheitsressort bereitet derzeit in Abstimmung mit den Gesundheitsämtern Bremen und Bremerhaven sowie mit mir die **Rechtsverordnung** nach § 33 Abs.3 ÖGDG vor. Ein erster **Vorentwurf** als Arbeitsgrundlage lag bei Redaktionsschluss bereits vor. Mir kommt es vor allem auch auf die Umsetzung des **Trennungsgebots** des § 32 Abs.1 ÖGDG an. Danach hat etwa der Sozialpsychiatrische Dienst die Daten, die er im Zusammenhang mit Beratungsangeboten erhebt, getrennt von den Daten zu speichern, die er im Zusammenhang

mit seinen Aufgaben bei der Zwangseinweisung psychisch Kranker erhebt (vgl. unten Ziff. 11.5.). Nach Erlass der Rechtsverordnung kann der Funktionsumfang des EDV-Programms für den Sozialpsychiatrischen Dienst im Gesundheitsamt Bremen um weitere in der Rechtsverordnung erlaubte Vorgänge der Datenverarbeitung erweitert werden. Ich gehe davon aus, dass das Amt mich bei Fortschreibung seines Datenverarbeitungskonzepts erneut beteiligen wird.

Der **Datenschutzausschuß** hat bei der Beratung meines 20. Jahresberichts angekündigt, die weitere Entwicklung der Erarbeitung der Rechtsverordnung zu begleiten (s.o. Ziff. 7.1.).

11.5. PsychKG: Mitteilung psychiatrischer Gutachten an Ordnungsbehörden

Das Gesundheitsressort bereitet ein **neues Bremisches Gesetz über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG)** vor, das die alte Regelung aus dem Jahre 1983 ablösen soll. Ich begrüße das Vorhaben, denn § 47 des mit mir abgestimmten Entwurfs unterwirft die Daten, die, sei es im Rahmen freiwilliger Inanspruchnahme seiner Beratungsangebote vom Sozialpsychiatrischen Dienst (vgl. hierzu Ziff. 11.4.), sei es in einem Verfahren zur zwangsweisen Unterbringung in einem psychiatrischen Krankenhaus von diesem Dienst selbst oder von einer anderen beteiligten Stelle erhoben wurden, einer - auch im Vergleich zu den Vorgaben des § 32 Abs. 2 ÖGDG - besonders **strengen Zweckbindung**. Nur wenn die betroffene Person darin eingewilligt hat oder wenn eine gegenwärtige Gefahr für ihr Leib oder Leben oder für Leib oder Leben Dritter nicht anders abgewendet werden kann, dürfen die Daten für andere Zwecke verarbeitet werden.

Zu den Aufgaben der Sozialpsychiatrischen Dienste der Gesundheitsämter bzw. der Psychiatrischen Kliniken gehört es, Gutachten zu erstellen, auf deren Grundlage die

Ortspolizeibehörden bei Gericht beantragen können, eine Person unter Entzug ihrer Freiheit unterzubringen bzw. deren Unterbringung zu verlängern. Der Inhalt dieser Gutachten kann aber auch von erheblichem Interesse für die Ordnungsbehörden sein, die über die Eignung zum Führen von Kraftfahrzeugen oder zum Umgang mit Waffen zu befinden haben. Diese forderten denn auch eine Regelung, die es den **Ortspolizeibehörden** erlauben sollte, ihnen die genannten **Gutachten** zur Verfügung zu stellen. Dies aber hätte der im Entwurf angestrebten strengen Zweckbindung widersprochen.

Inzwischen hat man sich auf einen **Kompromiss** einigen können: Nicht die Ortspolizeibehörde, sondern nur die Stelle selbst, die das Gutachten erstellt hat, also der Sozialpsychiatrische Dienst oder die Psychiatrische Klinik, ist befugt, die zuständige Ordnungsbehörde zu unterrichten, wenn die betroffene Person infolge ihrer Krankheit oder Behinderung sich oder andere durch das Führen von Kraftfahrzeugen oder durch den Umgang mit Waffen gefährden würde (so ein neu eingefügter § 48). Der Kompromiss ist auch für mich akzeptabel, denn er schwächt die Zweckbindung gegenüber der oben zitierten Regelung in § 47 des Entwurfs zwar ab, stellt aber jedenfalls auf den Einzelfall ab und belässt die Verantwortung für die Unterrichtung bei der ärztlichen Seite. Nach Informationen aus dem Gesundheitsressort strebt man dort die Verabschiedung des Gesetzes in dieser Fassung noch in der laufenden Legislaturperiode an.

11.6. Narkosevorfall: Unzulässige Datenbeschaffung für Arzthaftpflichtprozess

1988 verabschiedete die Bremische Bürgerschaft ein allgemein als vorbildlich angesehenes **Krankenhausdatenschutzgesetz** (KHDSG). Patientendaten sollten nur nach Maßgabe dieses Gesetzes verarbeitet werden. Besonderes Gewicht wurde u.a.

darauf gelegt, dass nach Entlassung eines Patienten aus der Klinik zwar seine Unterlagen aufbewahrt werden, aber **gesperrt** bleiben sollten. Dies heißt, die Patientenunterlagen sind vom Krankenhaus zu archivieren und dürfen nur in einem besonderen Verfahren nach Einwilligung des Patienten oder zum Zwecke weiterer Behandlung vom Archivpersonal entsperrt und für bestimmte Zwecke, hauptsächlich für weitere Behandlungen, zur Verfügung gestellt werden.

Der folgende Fall, der auf einer **Eingabe** beruht, zeigt, dass diese Vorgabe nicht immer beachtet wird. Die Klinik B hatte sich vertraglich vereinbart, der Klinik A für Operationen ihre Anästhesieärzte zur Verfügung zu stellen. Auch die Aufsicht über diese sollte die Klinik B ausüben. Nun wurde ein Patient zunächst in der Klinik A und einige Jahre später in der Klinik B operiert. Anschließend erhob er wegen eines Narkoseunfalls während der Operation in der Klinik B Haftungsklage gegen deren beteiligte Anästhesieärzte und deren Träger, die Stadtgemeinde Bremen. In der mündlichen Verhandlung vor dem Landgericht berief sich der Anwalt der Beklagten darauf, der Kläger habe vor der Operation die Anästhesieärzte auf die besonderen in seiner Person liegenden Umstände, die den Unfall bedingt hätten, nicht hingewiesen. Man habe die Unterlagen über die vorherigen Operationen in der Klinik A durchsehen lassen. Auch in ihnen fehlten entsprechende Hinweise. Zum Beweis wurde die Vorlage der Unterlagen aus der Klinik A angeboten.

Nachdem der klagende Patient sich im Sommer 1996 an mich gewandt hatte, bat ich zunächst die Klinik A um Stellungnahme und wies darauf hin, dass **eine Freigabe gesperrter Krankenunterlagen für die Prozessführung einer anderen Klinik nicht zulässig** sei. Von dort hieß es, ein im Hause tätiger Oberarzt habe die Akte aus dem Archiv angefordert und sie,

ohne dass dies dem Archivpersonal bekannt gewesen sei, dem Leiter der Anästhesieabteilung der Klinik B weitergegeben. Damit sei gegen den Datenschutz verstoßen worden, was man den beteiligten Ärzten und der Leitung der Klinik B mitgeteilt habe.

Im Verlauf eines langwierigen, sich bis in den Sommer 1998 hinziehenden Schriftwechsels mit der Klinik B und dem Senator für Gesundheit beanstandete ich im Oktober 1997, dass die Klinik B, indem sie sich ohne Wissen des Patienten dessen Akte aus dem Archiv der Klinik A besorgte und zu Prozessführungszwecken weitergab, diese Daten zu Unrecht erhoben und damit die Rechte des Patienten verletzt habe. Ich habe nach wie vor den Eindruck, dass angesichts der "Beweisnot" eines Haftungsprozesses die Archivierungsbestimmungen des KHDSG nicht oder doch nicht mit dem gebotenen Gewicht neben den Interessen der prozessführenden Partei beachtet wurden.

Der Senator für Gesundheit bestreitet, dass in der Anforderung der Unterlagen ein Rechtsverstoß gelegen habe. Um für die Zukunft vergleichbare Konflikte zu verhindern, hat er jedoch eine **Ergänzung der vertraglichen Regelungen der beiden beteiligten Krankenhäuser** angeregt. Dies begrüße ich, zumal Kooperationen von Kliniken untereinander zwecks Qualitätssicherung und Kostensenkung zunehmen. Die nach Presseberichten geplante umfassende Kooperation zwischen den beiden betroffenen Kliniken ist hierfür ein Beispiel. Ich werde mich in diesem Zusammenhang vor allem dafür einsetzen, dass die Datenflüsse zwischen kooperierenden Kliniken für die betroffenen Patienten transparent sind.

11.7. Ärztekammer - Vorlage der Steuerbescheide zur Beitragsberechnung

Die Staffelung der Beitragshöhe nach Einkommen entspricht einerseits dem Empfinden für soziale Gerechtigkeit, hat

jedoch andererseits zur Konsequenz, dass der Erhebungsstelle Belege für die Einkommenshöhe vorzulegen sind, da eine Selbstveranlagung vielfach weder zu Gerechtigkeit noch zu ausreichendem Beitragsaufkommen führt.

1997 beschloss die Mitgliederversammlung der Ärztekammer, der Höhe der Kammerbeiträge künftig das Einkommen ihrer Mitglieder zugrundezulegen. Eine Reihe von an mich gerichteten **Eingaben** von Ärzten bzw. deren Rechtsanwälten belegt, dass nicht alle Kammermitglieder mit der **Offenlegung ihrer Einkommen gegenüber der Kammerverwaltung** einverstanden waren. Ich musste ihnen allerdings mitteilen, dass ich wie der Senator für Gesundheit, der die Beitragsbestimmungen in der neuen Kammersatzung genehmigt hatte, der Auffassung bin, die neue Regelung bewege sich im Rahmen der durch das Bremische Heilberufsgesetz den Ärzten eingeräumten **Selbstverwaltung** ihrer Berufsangelegenheiten. Darüber hinaus konnte ich feststellen, dass die Ärztekammer von ihren Mitgliedern nicht verlangte, den gesamten Steuerbescheid vorzulegen, sondern sie darüber informierte, welche Teile der Bescheide sie benötige, und ihnen nahelegte, die Bescheide im übrigen zu **schwärzen**. Es sei daran erinnert, dass der Senator für Jugend sich erst nach langem Hin und Her bereit fand, bei der Berechnung der Kindertagesheimgebühren ähnlich datenschutzgerecht zu verfahren (vgl. hierzu 20. JB, Ziff. 14.4.1.2.).

Ich musste allerdings zugleich feststellen, dass die Kammer die für die automatisierte Verarbeitung der Beitragsdaten erforderlichen Zugriffsregelungen und Sicherheitsvorkehrungen nicht wie gesetzlich geboten in einem Datenverarbeitungskonzept festgelegt hatte. Die Kammer holte dies auf meine Intervention hin nach.

In mehreren Eingaben wurde weiter moniert, dass über Widersprüche gegen Gebührenbescheide der Vorstand entscheide,

d.h. ein ehrenamtliches Gremium, in dem Kollegen bzw. Konkurrenten der Widerspruchsführer sitzen. Meinen Vorschlag, dem Vorstand die für die **Entscheidung über den Widerspruch** erheblichen Unterlagen in anonymisierter Form vorzulegen, wollte die Kammer nicht aufgreifen.

11.8. Verkauf der Arztpraxis - Wahrung der Schweigepflicht

1991 entschied der Bundesgerichtshof, ein Arzt müsse vor Übergabe seiner Behandlungsunterlagen an seinen Praxisnachfolger die **Einwilligung seiner Patienten** einholen. In meinem 20. Jahresbericht hatte ich unter Ziff. 14.3. ausführlich darüber berichtet,

- dass die Ärzte- und die Zahnärztekammer Bremen nicht etwa ihre Mitglieder verpflichten wollten, entsprechend der BGH-Rechtsprechung die Einwilligung ihrer Patienten einzuholen, sondern in ihren **Berufsordnungen** lediglich regeln wollten, dass der Praxisnachfolger die ihm - ohne Einwilligung der Patienten - übergebenen Unterlagen unter Verschluss halten müsse und nur mit Einwilligung des Patienten, die dieser auch durch Aufsuchen des Praxisnachfolgers erklären könne, einsehen dürfe,

- dass der Senator für Gesundheit unter Berufung auf das höchstrichterliche Urteil diesen Passus der Berufsordnungen der beiden Kammern bislang **nicht genehmigt** habe und

- dass er den Kammern als praktikablen Kompromiss vorgeschlagen habe, diejenigen ihrer Mitglieder, die - anders als z.B. Laborärzte ohne Patientenkontakt - behandelnde Ärzte im eigentlichen Sinne sind, zu verpflichten, die Patienten, die nach Verkauf, aber vor Übergabe die Praxis aufsuchen, mündlich, und die Patienten, die im Verlauf der vergangenen zwei Jahre die

Praxis aufgesucht hatten, schriftlich um ihre Einwilligung zu bitten. Werde die Einwilligung ausdrücklich verweigert, müsse der Arzt die Unterlagen weiterhin aufbewahren. In allen übrigen Fällen sollten die durch die Berufsordnungen getroffenen Regelungen Bestand haben.

Inzwischen haben beide Kammern **Widerspruch** gegen die betreffenden Bescheide des Senators für Gesundheit eingelegt und in erster Linie damit begründet, dass erstens der Praxisnachfolger Eigentum an den Unterlagen erst erlange, sobald er in erlaubter Weise Einsicht nehme, und dass zweitens eine Verpflichtung aller Ärzte, die Einwilligung aller Patienten einzuholen, die ihre Praxis übergebenden Ärzte mit untragbaren Kosten belaste.

Dem ist entgegenzuhalten, dass der Bundesgerichtshof nicht auf den Eigentumsübergang, sondern auf die **Übergabe** der Unterlagen abstellt, d.h. auf die Überlassung der Möglichkeit, tatsächlich auf sie einzuwirken, und daran die Verletzung der Schweigepflicht durch den abgebenden Arzt knüpft. Anscheinend haben die Kammern den **Kompromissvorschlag** des Senators für Gesundheit nicht zur Kenntnis genommen.

Leider wurden in der Mehrzahl der Bundesländer Berufsordnungen der Ärzte- bzw. Zahnärztekammern genehmigt, ohne dass die Aufsichtsbehörden darauf bestanden, durch Umsetzung des höchstrichterlichen Urteils die Einhaltung der ärztlichen Schweigepflicht beim Verkauf von Arztpraxen zu gewährleisten. Es ist zu hoffen, dass der Senator für Gesundheit dennoch mit Hilfe seiner guten Argumente die **Widersprüche ablehnt** und ggf. eine verwaltungsgerichtliche Entscheidung herbeiführt. Ich habe ihm Beratung und argumentative Unterstützung angeboten.

12. Jugend und Soziales

12.1. Datenabgleich bei Sozialhilfeempfängern - viel Lärm um wenig

Dass die Bekämpfung des Mißbrauchs von Sozialleistungen dazu führen kann, das Persönlichkeitsrecht der auf die Hilfe der Solidargemeinschaft angewiesenen Bürger in unverhältnismäßiger Weise einzuschränken, habe ich in den letzten Jahresberichten immer wieder thematisiert (vgl. zuletzt ausführlich 20. JB, Ziff. 14.9). Jeder neue oder erweiterte Datenaustausch bedeutet Abbau des in § 35 des Ersten Buchs des Sozialgesetzbuchs geschützten Sozialgeheimnisses und muß sich daher an den Kriterien der Verhältnismäßigkeit von Eingriffen in Grundrechte messen lassen. Die Entwicklung im Berichtszeitraum hat meine Befürchtungen nicht widerlegt.

In Bremen hat man die ersten Erfahrungen mit dem automatisierten Datenabgleich nach § 117 des Bundessozialhilfegesetzes (BSHG) gesammelt, mit dessen Hilfe die Sozialämter (hier: Amt für Soziale Dienste bzw. Ortsämter) in Erfahrung bringen sollen, ob Hilfeempfänger ihnen Einkünfte oder vorrangige Sozialleistungen (vor allem der Arbeitsämter und der Rentenversicherung) verschwiegen haben. In einer Vorlage des Sozialressorts für die Deputation für Soziales hieß es im Oktober 1998, die Erfahrungen aus dem ersten Abgleich zeigten, dass der sehr hohe Verwaltungsaufwand in einem **Mißverhältnis zu dem tatsächlich festgestellten mißbräuchlichen Leistungsbezug** stehe. Sollten künftig noch mehr Hilfeempfänger einbezogen werden, sei zu befürchten, dass der Verwaltungsaufwand noch steige.

Tatsächlich läßt auch die Veröffentlichung der ersten Auswertungen des Sozialressorts in der Mitteilung des Senats an die Bremische Bürgerschaft vom 12.01.99 (Drs. 14/770S) erkennen, dass selbst positive Rückmeldungen aus dem Abgleich nur in der Minderzahl der Fälle beweisen, dass

ungerechtfertigt Leistungen bezogen wurden. In der Anhörung der verdächtigten Leistungsempfänger läßt sich offenbar häufig der Vorwurf ausräumen. Man kann sich vorstellen, wieviel Unruhe und Ängste bei den zu Unrecht Verdächtigten hervorgerufen wird und wieviele Spannungen und Auseinandersetzungen zwischen Sachbearbeitern und Hilfeempfängern daraus resultieren.

Die zahlreichen **"Fehlmeldungen"** und der daraus resultierende überflüssige Befragungs- und Bearbeitungsaufwand beruht auf einem Strukturfehler des neuen Datenabgleichs. Einem großen Teil der positiven Rückmeldungen liegt nämlich eine dem Sozialamt gegenüber nicht angegebene geringfügige Beschäftigung zugrunde. Gerade diese Rückmeldungen aber sind - wovor Datenschutzbeauftragte schon während der Gesetzgebung gewarnt haben und wie jetzt auch das Sozialressort erkennen mußte - nicht zuverlässig. Denn die Arbeitgeber unterlassen es allzu oft, ein angemeldetes geringfügiges Beschäftigungsverhältnis bei dessen Beendigung abzumelden. Da nur das Vierteljahr vor dem Abgleich gesetzlicher Abgleichszeitraum ist, erfahren die Sozialämter auf diese Weise von z.T. schon Jahre zurückliegenden Beschäftigungen, die ihnen der Verband der Rentenversicherungsträger, der bundesweit die Meldungen über geringfügige Beschäftigungsverhältnisse registriert, bei aktueller Datenlage in seiner Datei gar nicht hätte melden dürfen.

Eine derart unzulängliche und **inaktuelle Datenlage** darf sich aber nicht entgegen den Intentionen des Gesetzgebers zum Nachteil der Betroffenen auswirken. Das Sozialressort hat auf meine entsprechenden Hinweise hin inzwischen die Sozialhilfesachbearbeiter/innen angewiesen, insoweit die Rückmeldungen nicht zum Nachteil der Hilfeempfänger/innen auszuwerten. Deutlich wird erneut, wie wichtig es ist, Daten

nicht hinter dem Rücken von Betroffenen zu verwenden, sondern die Hilfeempfänger in die Aufklärung der Sachverhalte einzubeziehen, d.h. ihnen Gelegenheit zur Stellungnahme und Aufklärung zu geben, bevor aus dem Abgleich ihnen nachteilige Konsequenzen gezogen werden.

Der Magistrat **Bremerhaven** hat erkennen lassen, dass in seinem Zuständigkeitsbereich wie in der Stadtgemeinde Bremen verfahren werden soll. Zugleich bereitet er die Ausdehnung des automatisierten Abgleichs auf Abfragen bei anderen kommunalen Dienststellen und Gesellschaften, zunächst bei der Kfz-Zulassungsstelle, vor. Der Gesetzgeber hatte nachträglich die Rechtsgrundlage für derartige Abgleiche geschaffen, deren Rahmenbedingungen jedoch leider nicht präzise genug festgelegt. Die beteiligten Bremerhavener Stellen haben mir aber zugesagt, dass sie bei den kommunalen Abgleichsverfahren die Regularien, die für Abgleiche der Sozialleistungsträger untereinander gelten, entsprechend einhalten werden. Ob diese Absichten in der "Dienstanweisung zum Umgang mit den Daten, die auf der Grundlage des § 117 BSHG erhoben wurden" vom 10. Februar 1999 realisiert worden sind, konnte ich noch nicht bewerten; sie ist mir erst nach Redaktionsschluß zugegangen.

12.2. PUTOG - Nutzung von Klientendaten für Controlling

In zunehmendem Umfang erfassen und nutzen öffentliche Stellen personenbezogene Daten, die sie zu dem Zweck erhoben und gespeichert haben, den Betroffenen gegenüber Maßnahmen zu ergreifen (Eingriffsverwaltung) oder über Leistungen an sie zu entscheiden (Leistungsverwaltung), auch zum Zweck der **Kosten-Leistungs-Rechnung**, der **Produktplanung** und/oder des **internen Controlling** (vgl. dazu meine Bemerkungen im Vorwort unter Ziff. 1.2). Nun sind solche Verfahren ohne Zweifel für eine leistungsfähige und kostengünstige Verwaltung

unerlässlich. Selbstverständlich ist gleichfalls, dass eigens hierfür entwickelte automatisierte Verfahren eingesetzt werden.

Doch geht es in diesen Verfahren um auf die Aktivitäten der Behörden bezogene aggregierte Zahlen und Rechengrößen, **nicht um die Identität** der betroffenen Bürger bzw. "Kunden" der Verwaltung, an die sich die Leistungen und Maßnahmen richten. Anders ausgedrückt: Mit Hilfe von Software, die für Controlling-Zwecke bestimmt ist, müsste man eigentlich in der Lage sein, den **Personenbezug**, der ja für die Zwecke dieser Verfahren nicht erforderlich und damit **unzulässig** ist, von vornherein zu vermeiden oder doch möglichst umgehend zu löschen. Aus anderen Zusammenhängen, z.B. aus EDV-gestützten Forschungsprojekten, sind durchaus Verfahren bekannt, die es trotz Anonymisierung erlauben, Daten aus unterschiedlichen Quellen einander zuzuordnen. Auch die Verwaltung sollte sich im Interesse des Persönlichkeitsschutzes der Bürger zum sparsamen Umgang mit deren Daten derartige technische Instrumente zu Nutze machen. Das nachfolgende Beispiel ist illustrativ für die schwierigen Abstimmungsprozesse, die ich zuweilen mit senatorischen Behörden wegen oder auch trotz aus meiner Sicht klarer rechtlicher und DV-technischer Vorgaben habe; daher ist der Ablauf ausführlicher geschildert.

Unter dem Kürzel **PUTOG** stellte mir das Ressort zu Anfang 1997 erstmals ein EDV-Projekt zur Pflege des Produktplans, zur Erfassung der Aufgaben, zur Berechnung der Pflegesätze und zur Auswertung der Ausgaben, kurz gefasst zur Produkt-Aufgabenplanung vor. Nicht für die Aufgabe selbst, aber zwecks ggf. sich daraus ergebender Rückfragen und Aktenüberprüfungen müsse es möglich sein, erfasste Einzelfälle zu reidentifizieren. Ich erklärte daraufhin, dass 67c Abs.3 SGB X die Nutzung von Sozialdaten zu

Aufsichts- und Kontrollzwecken nur erlaube, soweit und solange dies erforderlich sei. Jedenfalls seien die Daten zu anonymisieren, sobald der Erfassungszweck es gestatte.

Nach hartnäckigem Drängen legte man mir im März 1998 endlich ein **Datenverarbeitungskonzept** für PUTOG vor. Dieses sah die Erfassung der Aktenzeichen von Zuwendungsempfängern vor. Die Einzelfälle sollten mit Hilfe der Kombination Aktenzeichen/Amt/Region/Stadtteil reidentifiziert werden können. Es fehlten eine Begründung dafür, warum dies erforderlich sei, die Festlegung von Vorkehrungen, die es den Auswertern unmöglich machen, auf die Identität einzelner Hilfeempfänger zu schließen, sowie Fristen und Verfahren für die Löschung der Aktenzeichen. Zudem wurden mir von anderer Seite im Juni 1998 Belege dafür zur Verfügung gestellt, dass inzwischen die Sachbearbeiter des Amtes für Soziale Dienste für PUTOG nicht mehr nur, wie in dem mir vorgelegten Konzept dargestellt, das **Aktenzeichen**, sondern darüber hinaus auch die **Namen der Hilfeempfänger** erfassen sollten.

Nach vielfachen Fragen und Erinnerungen meinerseits sowie wiederholten Zusagen auf baldige Erledigung von Seiten des Ressorts wurde mir schließlich Anfang 1999 bestätigt, dass im Amt für Soziale Dienste sowohl Aktenzeichen als auch Namen der Hilfeempfänger erfasst würden. Dies sei zur Kontrolle der Richtigkeit der Eingaben durch die Sachbearbeiter/innen und durch deren Vorgesetzte erforderlich: Die Namen seien nur auf den Ausdrucken zu lesen, die anschließend zwecks Nachprüfung an die Sachbearbeiter zurückgingen. Da deren **Organisationskennzeichen** nicht erfasst werde, sei eine schnelle Zuordnung nur über den Namen des Hilfeempfängers möglich. In meiner Stellungnahme an das Ressort wies ich darauf hin, dass dies keine Begründung für die Erfassung der Klientendaten sei,

sondern vielmehr zu erwägen sei, die Organisationskennzeichen der Sachbearbeiter statt der Aktenzeichen oder gar Namen der Hilfeempfänger zu erfassen.

Zudem, so kündigte man mir an, solle den dezentralen Auswertern ermöglicht werden, Ungereimtheiten in den erfassten Daten aufzuklären. Zu diesem Zweck sollten auch sie Aktenzeichen der Hilfeempfänger lesen können. Dies sei schon deshalb unbedenklich, weil sie zugleich die Vorgesetzten der Erfassungskräfte/Sachbearbeiter seien und in dieser Funktion Zugriff auf die Akten hätten, aus denen die Daten übernommen seien. Ich habe dem entgegengehalten, auch ohne Zugriff auf Aktenzeichen, sondern anhand einer eigens hierfür vergebenen **Kennziffer** könnten die Auswerter bei Auffälligkeiten der zu einem Fall erfassten Daten die Erfassungskräfte/Sachbearbeiter bitten, die von ihnen erfassten Daten erneut zu überprüfen.

Den zentralen Auswertern in der senatorischen Dienststelle soll, wie es etwas unklar heißt, "ein direkter Einblick in die Erfassungsdaten....nicht möglich" sein; sie könnten über die Auswertungssoftware lediglich die anonymisierten Daten einsehen. Ich habe das Ressort gebeten, diese Aussage zu präzisieren und die noch fehlenden Festlegungen zu Termin und Verfahren der Löschung von Sozialdaten zu treffen.

Unmittelbar vor der immer wieder hinausgezögerten Absendung der an mich gerichteten Stellungnahme hatte das Ressort eine **Dienstanweisung** für das Verfahren erlassen. Ob diese auffällige zeitliche Abfolge Absicht war, entzieht sich meiner Kenntnis. Jedenfalls vermitteln die Unterlagen zur Produkt-Aufgaben-Planung PUTOG und der Verlauf des Abstimmungsverfahrens mit mir nicht den Eindruck, als habe man mit dem gebotenen Nachdruck versucht, das von mir frühzeitig erläuterte **gesetzliche Gebot** umzusetzen, **die Erfassung von Sozialdaten zu Kontrollzwecken möglichst zu**

vermeiden, zumindest aber frühzeitig zu anonymisieren. Vielmehr schien es vor allem das Bestreben zu sein, Wünschen aus der Praxis, zur Verfahrenserleichterung auf Sozialdaten zurückgreifen zu können, zu entsprechen. Im Gegensatz zu den an Konzept und Umsetzung von PUTOG beteiligten behördlichen Stellen und Mitarbeiter/innen konnten die betroffenen Hilfeempfänger sich nicht zu Worte melden. Hinzukommt, dass die Abstimmung mit mir hinausgezögert wurde, bis vollendete Tatsachen geschaffen waren.

Erst kurz vor Redaktionsschluss erhielt ich vom **Ressort** die erbetene **Stellungnahme**. Sie vermittelt als ersten Eindruck, dass man sich mit meinen Bedenken ernsthaft auseinandergesetzt hat. Abgesehen davon, dass man die angemahnte Löschungsregelung - welchen Inhalts? - nachträglich einfügen will, soll das Verfahren aber nicht modifiziert werden. Ich werde nach sorgfältiger Prüfung der Stellungnahme die Angelegenheit weiter verfolgen.

12.3. Kindergarten-Informationssystem KIS - Datenschutzkonzept liegt vor

Im 20. Jahresbericht mußte ich unter Ziff. 14.4.2.2 darüber berichten, dass in einigen städtischen Kindertagesheimen mit der automatisierten Verarbeitung der Sozialdaten von Eltern und Kindern für das **Aufnahmeverfahren** und für **Planungszwecke** begonnen worden sei, ohne dass die gesetzlich gebotenen Festlegungen zur Sicherung der Zweckbindung und des Schutzes der Daten vor unbefugten Zugriffen dokumentiert worden seien. Nachdem mir das Ressort für Jugend nach mehreren vergeblichen Erinnerungen ein unzulängliches Konzept vorgelegt hatte, sprach ich im April 1998 eine **formelle Beanstandung** nach § 29 BrDSG aus. Nach einigem Hin und Her erlaubten es mir ein neues Konzept und ergänzende Festlegungen des Ressorts im Dezember 1998, zu erklären, dass zwar noch einige zusätzliche Präzisierungen geboten,

dass nunmehr jedoch die der Beanstandung zugrunde liegenden **Mängel behoben** seien. Trotz dieses Sachstands (vgl. dazu den Bericht des Datenschutzausschusses, o. Ziff. 7.1., zu Tz. 14.4.2) sollen in diesem Bericht diejenigen Aspekte der Auseinandersetzung, die von exemplarischer Bedeutung sind, noch einmal unterstrichen werden.

Alle Datenschutzgesetze schreiben vor, dass vor Aufnahme der automatisierten Verarbeitung personenbezogener Daten die installierten Vorkehrungen zum Datenschutz und zur Datensicherung zu dokumentieren sind (vgl. § 8 i.V.m. § 7 BrDSG). Auf eine Kurzformel gebracht: **Ein dokumentiertes Datenschutzkonzept ist unerläßlicher Bestandteil von EDV-Projekten.** Dies gilt auch für einen sog. **Testbetrieb**, sofern er mit Echtdaten, d.h. personenbezogenen Daten, läuft. Und dies gilt auch und gerade für **eigenprogrammierte Anwendungen**: Die rechtzeitige Dokumentation mag zwar angesichts knapper Personalausstattung zusätzlich zum ohnehin beträchtlichen Personalaufwand gerade hier besonders lästig sein, sie ist aber um so erforderlicher, als gerade Eigenentwicklungen der datenverarbeitenden Stelle besonders sorgfältiger interner und externer Kontrolle bedürfen. Insbesondere ist auf der Ebene des Betriebssystems und der Applikation die Sicherheitsstruktur zu dokumentieren. Es ist unerläßlich, bereits vor der Entscheidung für die Eigenentwicklung Zeit- und Personalressourcen für Entwicklung und Dokumentation von Datenschutzvorkehrungen vorzusehen. Ist dies nicht möglich, sind Standard-Produkte einzusetzen. Dies habe ich z.B. auch in meiner wiederholten kritischen Berichterstattung zur eigenentwickelten EDV im Zentralkrankenhaus Bremen-Ost deutlich gemacht (vgl. zuletzt 21. JB, Ziff. 14.5: Die Probleme dort wurden bezeichnenderweise überwiegend durch die Ersetzung der eigenentwickelten durch Standard-Software gelöst).

Meine Aufgabe ist es nicht nur, Hinweisen auf Mißbrauch persönlicher Daten nachzugehen, sondern auch **präventiv** die datenverarbeitenden Stellen zu veranlassen, von vornherein die Vorkehrungen zu treffen, die eine Datenverarbeitung im gesetzlichen Rahmen gewährleisten. In diesem Sinne ist es wichtig, folgende **Festlegungen im Datenverarbeitungskonzept für KIS** erreicht zu haben:

- Begrenzung auf die für die Aufnahmeentscheidung relevanten Daten,
- Trennung von Anwendung und Systemadministration, und
- Darstellung der Grobstruktur des Sicherheitssystems und des Protokollierungsverfahrens.

Da die im Aufnahmeverfahren erhobenen **Sozialindikatoren** zum Ende eines jeden Kindergartenjahres gelöscht werden und derzeit weder Daten für die Beitragsberechnung noch für pädagogische Zwecke in KIS gespeichert werden sollen, habe ich meine Beanstandung trotz einiger vorgeschlagener Differenzierungen und Präzisierungen nicht aufrechterhalten.

Sobald KIS um **zusätzliche Funktionen** erweitert wird, wird ggf. zu gewährleisten sein, dass auf Datenbankebene die **Zugriffsberechtigungen und Löschungsfristen** je nach dem mit der Speicherung verfolgten Zweck **differenziert** werden. Ich erwarte, dass die Konzeption von KIS diesmal rechtzeitig fortgeschrieben wird und dass ich rechtzeitig beteiligt werde. In einer auf den 20.11.1998 datierten ressortinternen Mitteilung, die ich Ende Januar 1999 zur Kenntnis erhielt, hieß es, zu dem letztgenannten Zeitpunkt solle eine Testversion für die **Beitragsberechnung** - bislang noch nicht in KIS einbezogen - vorliegen. Im Hinblick darauf, dass für diese Aufgabe **Einkommensdaten** des überwiegenden Teils der

Eltern erhoben werden (vgl. hierzu 20. JB, Ziff. 14.4.1.2.), sind hier besonders sorgfältige Datenschutzvorkehrungen, insbesondere Zugriffsbegrenzungen, geboten. Bei Redaktionsschluß hatte ich noch keine Antwort auf die Bitte erhalten, mir die Fortschreibung des Datenverarbeitungskonzepts für KIS rechtzeitig vorzulegen.

Derselben ressortinternen Mitteilung entnahm ich, dass ein Programm zur **Qualifizierung** der Leitungskräfte der städtischen Kindertagesheime zum technischen Umgang mit KIS vorbereitet werde. Das Thema Schutz der Sozialdaten der Kinder und deren Eltern wurde in diesem Zusammenhang nicht vorgesehen. Deshalb habe ich bei der Senatskommission für das Personalwesen ein entsprechendes Fortbildungsangebot angemeldet und dem Jugendressort vorgeschlagen, miteinander zu kooperieren.

12.4. Werkstatt Bremen - Mängel weitgehend beseitigt

Im 20. Jahresbericht hatte ich unter Ziff. 14.8 die von mir definierten datenschutzrechtlichen Anforderungen für den Einsatz eines Personalinformationssystems geschildert, in dem sowohl Daten von Arbeitnehmern der Einrichtung als auch der Schwerbehinderten (Beschäftigten) verarbeitet werden und damit unterschiedliche gesetzliche Vorschriften (BrDSG, Sozialgesetzbuch) zu beachten sind.

Im Berichtszeitraum habe ich die in der Stellungnahme der Werkstatt Bremen zu meinem **Prüfbericht** genannten Maßnahmen bewertet. Dabei konnte ich feststellen, dass die von mir festgestellten **Mängel weitgehend ausgeräumt** bzw. nach meiner Antwort auf die Stellungnahme **nachgebessert** worden sind. So ist z.B. die sog. **Mandantentrennung** weiter differenziert worden, **Auswertungen** werden in halbjährlich aktualisierten Listen dokumentiert und dem betrieblichen Datenschutzbeauftragten zur Verfügung gestellt. Des weiteren wird die **Proto-**

kollierung durchgeführter Abfragen regelmäßig durch den betrieblichen Datenschutzbeauftragten eingesehen. In Bezug auf die Größe der Kostenstellen (Identifizierbarkeit) und die Löschung der Historiendaten wurde die Erforderlichkeit nochmals dargelegt.

13. Arbeit

13.1. Informationsverbund illegale Beschäftigung - noch Abstimmungsbedarf

13.1.1. Ausgangspunkt Senatskonzept

Auf Seite 8 seines "Konzepts zur nachhaltigen Bekämpfung von illegaler Beschäftigung und Schwarzarbeit im Lande Bremen" (Drs. Bürgerschaft (Landtag) 14/1086 vom 20.07.98) kündigte der Senat die Einrichtung eines EDV-gestützten Informationsverbundes beim Senator für Arbeit an und erklärte, er werde die datenschutzrechtlichen Belange mit mir abklären.

In der **Zentraldatei** bzw. dem **Informationsverbund** sollen personenbezogene Daten, d.h. Daten von Einzelunternehmern und Arbeitnehmern, sowie Betriebsdaten gespeichert und genutzt werden. Letztere sind als Sozialdaten personenbezogenen Daten gleichgestellt. Die Speicherung personenbezogener Daten bzw. von Sozialdaten durch eine öffentliche Stelle ist ein Eingriff in die Rechte der davon Betroffenen und bedarf einer Rechtsgrundlage. Die Datenschutzgesetze des Bundes und der Länder, so z.B. das Bundesdatenschutzgesetz (BDSG), das Bremische Datenschutzgesetz (BrDSG) und das Zehnte Buch des Sozialgesetzbuchs (SGB X), berechtigen öffentliche Stellen zur Verarbeitung personenbezogener Daten, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist.

13.1.2. Keine eigene gesetzliche Aufgabe des Senators für Arbeit

In einer Reihe von Gesetzen hat der Bund die Befugnisse und Zuständigkeiten bei der Bekämpfung von Schwarzarbeit und

illegaler Beschäftigung im einzelnen geregelt und voneinander abgegrenzt. Dazu gehören u.a. das **Gesetz zur Bekämpfung der Schwarzarbeit**, das **Arbeitnehmerüberlassungsgesetz**, das **Arbeitnehmer-Entsendegesetz**, das **Ausländergesetz** und das **Sozialgesetzbuch** mit seinen Büchern III und IV.

Zuletzt ist zum 01.01.1998 das **3. Buch des Sozialgesetzbuchs (SGB III)** in der Fassung des 1.SGB III-ÄndG in Kraft getreten. In seinem 3. Abschnitt (Bekämpfung von Leistungsmißbrauch und illegaler Ausländerbeschäftigung)

- sind in §§ 304 Abs.1 und 305 bis 307 Prüfaufgaben und -befugnisse der Arbeits- und Hauptzollämter bestimmt,
- sind in § 304 Abs.2 die Behörden aufgeführt, die die Arbeits- und Hauptzollämter dabei zu unterstützen haben,
- werden durch § 308 Abs.1 die in § 304 aufgeführten Behörden befugt, die für die Prüfungen erforderlichen Daten und deren Ergebnisse untereinander auszutauschen,
- wird den Arbeitsämtern die Aufgabe zugewiesen, die Ermittlungen zu koordinieren, und
- werden nach § 308 Abs.3 die Arbeits- und Hauptzollämter verpflichtet, die zuständigen Behörden zu unterrichten, wenn sie Anhaltspunkte für Verstöße gegen eines der Gesetze zur Bekämpfung von Schwarzarbeit und illegaler Beschäftigung haben.

Ebenfalls seit dem 01.01.98 dürfen die Verfolgungsbehörden nach dem Gesetz zur Bekämpfung der Schwarzarbeit (z.B. Stadtamt bzw. Ortspolizeibehörde Bremerhaven) und nach dem Arbeitnehmer-Entsendegesetz (Arbeitsämter) den Vergabebehörden (z.B. Bausenator) die für deren Aufgabenerfüllung (z.B. Ausschluss von Wettbewerbern nach § 5 Schwarzarbeitsgesetz

bzw. nach § 8 der Verdingungsordnung Bau, VOB/A) erforderlichen Auskünfte erteilen.

Ein "Informationsverbund" besteht m.a.W. nach der geltenden Rechtslage bereits zwischen allen an der Kontrolle der illegalen Beschäftigung mitwirkenden Behörden in dem Sinne, dass jede dieser Stellen mit jeder anderen alle die Daten austauschen kann, die für getrennte oder gemeinsame Prüfaktionen erforderlich sind. In keinem der einschlägigen Gesetze wird allerdings dem Arbeitsminister oder -senator eines Landes eine eigene "operative" Aufgabe oder Zuständigkeit zur Bekämpfung von Schwarzarbeit und damit eine Befugnis zur Verarbeitung personenbezogener Daten bzw. von Sozialdaten zu diesem Zweck eingeräumt.

13.1.3. Gesetzliche Regelung als Voraussetzung für die Einrichtung von Zentraldateien

Hinzu kommt folgender Gesichtspunkt: Das deutsche Recht kennt eine Reihe von Zentraldateien bzw. Registern. Ihre Kennzeichen sind das Speichern von Daten über einen bestimmten Anlaß hinaus, sowie das Bereitstellen dieser Daten nicht nur für die speichernde Stelle, sondern auch für andere Stellen. Alle haben wegen des Umfangs der registrierten Angaben, der Zahl der eingebenden und abrufenden Stellen, der Unterschiedlichkeit der Abrufzwecke usw. eine **besondere gesetzliche Grundlage**, so etwa das Fahrzeugzentralregister im Straßenverkehrsgesetz, das Strafregister im Bundeszentralregistergesetz, das Gewerbezentralregister in der Gewerbeordnung oder das Melderegister in den Meldegesetzen.

Diese Gesetze regeln im einzelnen, welche Daten gespeichert werden, wie diese Daten erhoben bzw. von wem sie eingestellt werden, wer zu welchen Zwecken welche Daten abrufen darf, auf welche Weise die Richtigkeit und Aktualität des

Datenbestandes gesichert wird, und zu welchem Zeitpunkt welche Daten gelöscht werden müssen. Der Gesetzesvorbehalt gilt erst recht, wenn sog. **"Verdachtsdateien"** eingerichtet werden, bei denen die gespeicherten Vorwürfe oder vermuteten Rechtsverstöße noch nicht rechtskräftig festgestellt worden sind (z.B. die zentrale "Gendatei", s. o. Ziff. 10.1.1.). Auch eine Zentraldatei mit Angaben über die Ergebnisse von Schwarzarbeitskontrollen würde zu großen Teilen nicht gerichtsfeste Angaben enthalten.

Eine derartige gesetzliche Regelung gibt es für eine "Zentraldatei zur Bekämpfung illegaler Beschäftigung" nirgendwo. Es ergibt sich allerdings aus den zitierten Vorschriften des SGB III ein Hinweis darauf, dass der Gesetzgeber den Arbeitsämtern eine zentrale Funktion einschließlich der Koordinierung zuweist. Nach meiner Kenntnis will oder kann das Arbeitsamt Bremen diese ausdrücklich vorgesehene Koordinierungsrolle nicht übernehmen.

Möglich wäre natürlich, die bisher fehlende Rechtsgrundlage durch eine entsprechende Ergänzung des Dritten Abschnitts (§§ 304-308) des SGB III zu schaffen. Hierfür müßte der Senat eine entsprechende Initiative im Bundesrat ergreifen. Selbstverständlich wäre ich bereit, ihn hierbei zu beraten.

13.1.4. Datenverarbeitung im Auftrag durch den Senator für Arbeit

Mangels einer eigenen Rechtsgrundlage für den Informationsverbund bleibt es bei der derzeitigen Rechtslage: Jede der gesetzlich zuständigen Stellen verarbeitet die für ihre Aufgabenerfüllung erforderlichen Daten auf der Grundlage der jeweils für sie geltenden Gesetze. Die Sozialleistungsträger, d.h. die Arbeits- und Hauptzollämter, die Krankenkassen und die Träger der Rentenversicherung haben nach Maßgabe des § 35 SGB I und der §§ 67-85a SGB X das Sozialgeheimnis zu wahren. Dies bedeutet etwa, dass sie

anderen Behörden, die nicht Sozialleistungsträger sind (z.B. der Verwaltungspolizei), Sozialdaten für deren Aufgabenerfüllung nur dann zur Verfügung stellen dürfen, wenn ihnen dies im einzelnen durch das SGB erlaubt ist, und dass deren Online-Abruf unzulässig wäre (§ 79 SGB X).

Als mögliche Alternative habe ich in den bisherigen Gesprächen die sog. **Datenverarbeitung im Auftrag** genannt. Die Stellen, die Daten in die Zentraldatei einstellen bzw. aus ihr abrufen wollen, könnten die Koordinierungsstelle des Senators für Arbeit damit beauftragen, diese Datei für die Auftraggeber zu betreiben. Die rechtlichen Vorgaben ergeben sich je nach Einordnung der auftraggebenden Stelle aus § 80 SGB X, § 11 BDSG oder § 9 BrDSG.

In diesem Falle bliebe die Verantwortung jeder einzelnen auftraggebenden Stelle für die Wahrung der jeweils für sie geltenden gesetzlichen Vorgaben uneingeschränkt bestehen. Die Koordinierungsstelle dürfte die Daten, die die Auftraggeber "einstellen", nur nach Maßgabe der jeweiligen bilateralen Vereinbarungen einspeichern und weitergeben.

Der jeweilige Auftraggeber wäre auch verantwortlich dafür, dass durch geeignete technische und organisatorische Maßnahmen gewährleistet ist, dass den unterschiedlichen Abfragern nur *die* Daten zur Verfügung gestellt werden, die er nach den für ihn geltenden Bestimmungen übermitteln darf.

Diese Rechtslage gilt auch dann, wenn der gespeicherte Datensatz auf die Information beschränkt wird, bei welcher Behörde über einen bestimmten Arbeitgeber oder Arbeitnehmer nähere Informationen zu erhalten sind. Eine solche Hinweisdatei ist leichter aktuell zu halten und hätte den Vorteil, dass die anfragende Dienststelle sich direkt bei

der bereits tätig gewordenen Behörde und damit auf aktuellem Stand informieren kann.

Dieses Modell würde allerdings voraussetzen, dass der Senator für Arbeit mit den an der Zentraldatei interessierten Stellen separate, wenn auch möglicherweise in manchen Passagen textlich übereinstimmende, Abmachungen über die Details der Einmeldungen, Übermittlungen und Abrufe trifft. Dies geht wiederum nur, wenn klar ist, welche Behörde sich mit welchen Daten und mit welchen Verwendungsinteressen aktiv und/oder nur passiv an der Zentraldatei beteiligen will.

13.1.5. Verfahrensstand

Die Vorstellungen von Senat bzw. Senator für Arbeit, zur Bekämpfung der illegalen Beschäftigung eine Zentraldatei bzw. einen Informationsverbund einzurichten, bedürfen mithin noch weiterer **inhaltlicher Präzisierung** und der **Abstimmung mit den zuständigen Stellen**. Eine Koordinierungskonferenz, zu der der Senator für Arbeit im Dezember 1998 Vertreter aller für die Bekämpfung illegaler Beschäftigung im Lande Bremen zuständigen Stellen eingeladen hatte, brachte nicht die erforderliche Aufklärung darüber, welche dieser Stellen sich mit welchen Daten und mit welchem Verwendungsinteresse, sei es durch Einstellung, sei es durch Abruf von Daten, an dem Projekt beteiligen wollen. Das vom Senator für Arbeit erstellte Protokoll der Konferenz verzeichnet unterschiedliche Aussagen zu Datenbedarfen, die über den Einzelfall hinausgehen, d.h. nicht durch Einzelabfragen zu befriedigen sind, hingegen wenig klare Aussagen zur Bereitschaft, Daten in die Zentraldatei einzustellen.

Dagegen machte der Vertreter des Arbeitsamtes Bremen sehr deutlich, dass das Arbeitsamt schwerlich Führung und Pflege der Zentraldatei übernehmen werde. Überdies ist deutlich,

dass der Senator für Arbeit nicht anstrebt, durch eine Initiative auf Bundesebene, z.B. auf Ergänzung der §§ 304-308 SGB III, eine gesetzliche Grundlage mit den gebotenen Präzisierungen für ein derartiges Projekt zu schaffen. Deshalb bleibt nur die "kleine Lösung", d.h. der Senator für Arbeit stellt als Dienstleistung für die mit der Bekämpfung illegaler Beschäftigung zuständigen Stellen für deren Informationsverbund die technische Infrastruktur bereit.

In der Sitzung des **Datenschutzauschusses** der Bremischen Bürgerschaft im Januar 1999 erklärte der Senator für Arbeit, er wolle dem Ausschuss ein entsprechendes, mit den potentiellen Auftraggebern und mit mir abgestimmtes Konzept vorlegen und dem Ausschuss im Mai 1999 über den Verfahrensstand berichten.

Nach Redaktionsschluß hat mir der Senator für Arbeit Textentwürfe für Verträge zwischen ihm und an dem Informationsverbund teilnehmenden Behörden zur Stellungnahme zugeleitet.

14. Bildung, Wissenschaft, Kunst

14.1. Novellierung des Hochschulrechts - meine Vorschläge

Die Bremische Bürgerschaft befand sich bei Redaktionsschluß noch in den Beratungen über eine Änderung des bremischen Hochschulrechts. Im Rahmen dieser Gesetzesänderung sollen u. a. das Bremische Hochschulgesetz und das Gesetz über das Studentenwerk novelliert werden. Ich wurde gebeten, zu einigen datenschutzrechtlich bedeutsamen Änderungsvorschlägen Stellung zu nehmen.

Die bisherige **Datenverarbeitungsregelung** in § 44 a Bremisches Hochschulgesetz, die die Studienbewerber, Studenten und Prüfungskandidaten verpflichtete, für die Zulassung zum Studium, zum Studienverlauf und zur Prüfung

bestimmte Daten anzugeben, soll durch eine auch die Mitglieder und Angehörigen der Hochschulen sowie weitere Zwecke umfassende neue Datenverarbeitungsregelung (§ 9 neu) ersetzt werden. Gegen den ursprünglichen Änderungsvorschlag hatte ich Bedenken erhoben und Formulierungsänderungen empfohlen, über die ich mit dem Senator für Bildung, Wissenschaft, Kunst und Sport beraten habe mit dem Ziel, zu einem abgestimmten Formulierungsvorschlag zu kommen. Meine Änderungsvorschläge betrafen die Verpflichtung der Betroffenen zur Datenangabe und die stärkere Berücksichtigung der funktionellen Aufgaben- und Informationsverteilung sowie des Zweckbindungsgebotes auch im Hochschulbereich. Ein abgestimmter Formulierungsvorschlag (§ 9 neu) wurde in das laufende Gesetzgebungsverfahren eingebracht.

Eine weitere Änderung betrifft die sog. **Evaluierung von Lehrveranstaltungen** und die Nutzung der dabei gewonnenen personenbezogenen Daten über Studenten, Hochschullehrer, Dozenten und Lehrbeauftragte. Eine Gesetzesregelung hierzu gibt es derzeit noch nicht. In der Vergangenheit hatte ich zu dieser Thematik schon häufiger Anfragen und Eingaben, die ich mangels spezifischer Regelungen im Bremischen Hochschulgesetz nur vor dem Hintergrund der allgemeinen Regelungen im Bremischen Datenschutzgesetz beantworten konnte. Auch über die hierfür vorgesehene neue Bestimmung im Bremischen Hochschulgesetz habe ich mit dem Senator für Bildung, Wissenschaft, Kunst und Sport beraten und Änderungsvorschläge gemacht. Mir geht es hierbei darum, die hochschulinterne Verantwortlichkeit für eine derartige Datenerhebung und die Weiterverwendung der dabei erhobenen Daten möglichst präzise festzulegen. Auch zu diesem Punkt konnte ein gemeinsam getragener Formulierungsvorschlag dem Bürgerschaftssausschuß vorgelegt werden.

Außerdem habe ich vorgeschlagen, auch das Problem der **Datenbereitstellung bzw. Veröffentlichung im Internet** zu regeln. Wegen der verbreiteten Unsicherheit darüber, welche personen-bezogenen Daten von Lehrkräften und Mitarbeitern etwa aus ge-druckten Vorlesungsverzeichnissen unter Datenschutzgesichts-punkten zulässigerweise ins "Netz der Netze" eingestellt wer-den dürfen, gibt es beträchtliche Unterschiede bei der Hand-habung durch die Hochschulen. Der Bildungssenator will diesen Punkt in die laufende Novellierung allerdings nicht aufneh-men.

Das **Studentenwerksgesetz** soll ebenfalls geändert werden. Hierbei geht es u. a. auch um den Schutz der Daten, die im Rahmen der **psychologisch-therapeutischen Beratungsstelle** des Studentenwerks verarbeitet werden. In meiner Stellungnahme habe ich empfohlen, die in dieser Beratungsstelle erhobenen Daten nur in der Beratungsstelle selbst zu verarbeiten, sie nur in anonymisierter Form automatisiert zu verarbeiten und die Datenweitergabe nur mit ausdrücklicher Einwilligung der Betroffenen zuzulassen. Auch diese Anregung will der Senator für Bildung, Wissenschaft, Kunst und Sport aufnehmen und den abgestimmten Formulierungsvorschlag in die parlamentarische Beratung einbringen.

Der mir nach Redaktionsschluß noch zugegangene Bericht des nichtständigen Ausschusses "Hochschulrecht" (Drucks. 14/1360), der das Änderungsgesetz zur ersten Lesung für die März-Sitzung der Bürgerschaft enthält, weist aus, dass meine mit dem Bildungssenator abgestimmten Vorschläge vom Ausschuß aufgenommen worden sind.

14.2. Forschungsvorhaben an Bildungsinstitutionen - hoher Beratungsbedarf

Ein nicht unerheblicher Teil meiner Tätigkeit im Bereich Bildung, Wissenschaft und Kunst betrifft die

datenschutzrechtliche Begleitung der Durchführung von **Forschungsvorhaben durch Hochschulen oder andere öffentliche Forschungseinrichtungen** in Bremen und Bremerhaven, insbesondere im Bereich der Schulen (vgl. zuletzt 18. JB, Ziff. 13.1.; ausführl. 17. JB, Ziff. 11.2. und 11.3.). Zu solchen Vorhaben bestehen bei den Forschern oftmals datenschutzrechtliche Fragen, die von ihnen allein nicht gelöst werden können. In den zurückliegenden Monaten bin ich u. a. zu folgenden sozial- und gesellschaftswissenschaftlichen Vorhaben um Beratung gebeten worden:

- Befragung zum Thema "Streß- und Streßbewältigung im Kindes- und Jugendalter",
- Befragung zum Thema "Homosexualität im Lernbereich Schule",
- Befragung zum Freizeitverhalten von Schülern,
- Erhebungen im Rahmen des Forschungsprojektes "Berufe im weiblichen Lebenslauf und sozialer Wandel", und
- Erhebungen im Rahmen des Forschungsprojektes "Kollektive Identität türkischer Migranten in Deutschland".

In meinen Stellungnahmen habe ich hierzu insbesondere auf die speziell von den Hochschulen zu beachtende **Forschungsklausel des § 21 BrDSG** hingewiesen. Nach dieser Bestimmung ist die Verarbeitung personenbezogener Daten zu Forschungszwecken grundsätzlich nur mit schriftlicher **Einwilligung** der Betroffenen zulässig, die über Art, Umfang und Zweck der Nutzung ihrer Daten im Rahmen des Forschungsprojektes aufzuklären sind. Außerdem muß die **Freiwilligkeit** der Teilnahme am Forschungsprojekt sichergestellt sein. **Ohne Einwilligung** der Betroffenen dürfen deren Daten nur verarbeitet werden, wenn de-ren

schutzwürdigen Belange nicht beeinträchtigt werden. Der Forscher hat, sobald der Forschungszweck dies erlaubt, die erhobenen Hilfs- bzw. Identifikationsmerkmale von den übrigen Daten getrennt zu speichern (Prinzip der File-Trennung). Die personenbezogenen Merkmale sind zu löschen, sobald der Forschungszweck erreicht ist. Erhobene oder von anderen bremischen Behörden zulässig übermittelte personenbezogene Daten dürfen nur für das jeweilige Forschungsprojekt und grundsätzlich nur im Rahmen der Einwilligung ausgewertet werden (Prinzip der **Zweckbindung**). Des weiteren sind nach § 7 BrDSG angemessene Datensicherungsmaßnahmen zu ergreifen.

Soll das wissenschaftliche Forschungsvorhaben **an einer öffentlichen Schule** im Lande Bremen durchgeführt werden, so gilt überdies § 13 Abs. 6 und 7 des Gesetzes zum Datenschutz im Schulwesen (BremSchDSG). Danach muß das Vorhaben vor Beginn der Datenerhebung durch den Bildungssenator genehmigt werden. Der Landesbeauftragte für den Datenschutz, der Elternbeirat und der Schülerbeirat sowie bei Einbeziehung mehrerer Schulen die zuständigen Gesamtvertretungen sind vor der Durchführung des Projekts zu unterrichten. Bei minderjährigen Schülern müssen ggf. die Erziehungsberechtigten ihre Einwilligung geben.

Im Rahmen meiner datenschutzrechtlichen Beratung habe ich den jeweiligen Forschern auch das von mir entwickelte **Merkblatt zum Datenschutz bei Forschungsprojekten**, die durch Hochschulen oder andere öffentliche Forschungseinrichtungen in Bremen und Bremerhaven durchgeführt werden, zukommen lassen, dem die einzuhaltenden Anforderungen entnommen werden können (vgl. 17. JB, Ziff. 11.3.1). Insgesamt muß ich feststellen, dass mir nur ein Teil der relevanten Forschungsprojekte bekannt wird.

14.3. Schulbegleitforschung - zahlreiche Projekte

Teilweise unterschiedliche bzw. zusätzliche rechtliche Vorgaben gelten für Erhebungen und Untersuchungen, die der Senator für Bildung, Wissenschaft, Kunst und Sport und der Magistrat Bremerhaven nach § 13 Abs. 1 des Gesetzes zum Datenschutz im Schulwesen (BremSchDSG) **zur Wahrnehmung der ihnen als Schulbehörden obliegenden Aufgaben** vornehmen bzw. durch Dritte vornehmen lassen. Hier liegt ein weiterer Schwerpunkt meiner umfangreichen Beratungstätigkeit im Bildungsbereich. Vom Senator für Bildung, Wissenschaft, Kunst und Sport bzw. dem Schulamt des Magistrats bin ich gem. § 13 Abs. 6 BremSchDSG im Berichtszeitraum u. a. über die geplante Durchführung folgender Vorhaben unterrichtet worden:

- Erhebung zum Thema "Gewalt und Jugendkriminalität in der Schule",
- Untersuchung zur Bildungsorientierung und Schulzufriedenheit in den Oberstufenzentren,
- Erhebungen im Rahmen des Projekts "Studien- und Berufsorientierung an Schulzentren der Sekundarstufe II", und
- Organisationsuntersuchung zur Effizienz des Lehrereinsatzes im Land Bremen.

In meinen Stellungnahmen habe ich auch hier insbesondere auf die Zulässigkeitskriterien, die bei den einzelnen Vorhaben zu beachten sind, aufmerksam gemacht. Wie bei den wissenschaftlichen Forschungsvorhaben sind auch bei Vorhaben, die nach § 13 BremSchDSG durchgeführt werden, die Einhaltung eines korrekten Einwilligungsverfahrens, die Sicherstellung der Freiwilligkeit der Teilnahme an der Erhebung, die Beachtung der Zweckgebundenheit der erhobenen

Angaben, die frühzeitige Anonymisierung des personenbezogenen Datenmaterials und die Ergreifung angemessener Datensicherungsmaßnahmen nach § 7 BrDSG von besonderer Bedeutung. Auch für diese Kategorie von Befragungen in den Schulen habe ich als Erstinformation für die Verantwortlichen ein **Merkblatt** entwickelt (vgl. 17. JB, Ziff. 19.).

Nicht hierher gehören **Aktionen privater Unternehmen** (z.B. Krankenkassen) in Schulen, anläßlich derer Adressen von Schülern z.B. für die Zusendung von Informationsmaterial, die Durchführung von Sehtests o. ä. gesammelt werden. Inwieweit Datenerhebungen dieser Art schul- und datenschutzrechtlich überhaupt rechtmäßig sind, muß im Einzelfall kritisch geprüft werden.

15. Bau, Verkehr, Stadtentwicklung

15.1. Fahrerlaubnis-Verordnung: "Vollständigkeit" statt Erforderlichkeit

Die Fahrerlaubnis-Verordnung (FeV) vom 18. August 1998 (BGBl. I S. 2214) ist am 01. Januar 1999 in Kraft getreten. Sie regelt im wesentlichen das Verfahren über die Erteilung und Entziehung einer Fahrerlaubnis aufgrund der §§ 6, 6a Straßenverkehrsgesetz (StVG) vom 24. April 1998 (BGBl. I S. 747). Über meine Bedenken zu diesem Gesetzesvorhaben hatte ich mehrfach berichtet, zuletzt unter Ziff. 14.1 meines 19. Jahresberichts vom 31. März 1997.

Neben einzelnen zu kritisierenden Regelungen der Verordnung, die hier nicht näher erläutert werden sollen, ist § 11 Abs. 6 Satz 4 FeV besonders problematisch. Danach übersendet die Fahrerlaubnisbehörde bei Zweifeln über die körperliche oder geistige Eignung eines Betroffenen der untersuchenden Stelle (bisher: Medizinisch-psychologisches Institut) die **vollständigen** Unterlagen.

Während der Entwurf der Bundesregierung - wie die bisherigen Eignungsrichtlinien - vorsah, dass nur die **erforderlichen** Unterlagen an die untersuchende Stelle zu übersenden sind, hat der Bundesrat aufgrund des Beschlusses seines Ausschusses für Verkehr, dem nur Bremen nicht zugestimmt hat, die Formulierung in der Verordnung so erreichen können, dass nun die **vollständigen** Unterlagen weiterzuleiten sind. Abgesichert werden soll damit die übliche **bequeme Verwaltungspraxis**, dem Gutachter die gesamte Führerscheinakte ohne weitere Prüfung der Erforderlichkeit des Akteninhalts für die Begutachtung zu übersenden (siehe dazu die folgende Ziff.).

Da die **gesetzliche** Regelung in § 2 Abs. 14 Satz 1 StVG die Übermittlung von Daten durch die Fahrerlaubnisbehörden auf die für die Aufgabenerfüllung der Untersuchungsstelle **benötigten** Daten beschränkt, kann der Verordnungsgeber den Umfang der zu übermittelnden Daten nicht erweitern. Daher ist der Bundesbeauftragte für den Datenschutz gegenüber dem Bundesministerium für Verkehr für eine entsprechende Änderung der Verordnung eingetreten. Das jetzige Bundesministerium für Verkehr, Bau- und Wohnungswesen hat nach Auskunft des Bundesbeauftragten für den Datenschutz inzwischen aber erklärt, es beabsichtige derzeit keine Änderung dieser Regelung.

15.2. Strafakten an Gutachter - umstrittener Erlaß

Wie bedenklich die im vorigen Abschnitt dargestellte Handhabung "vollständiger" Aktenübersendung auch der Justiz erscheinen kann, zeigt die Rückfrage des Amtsgerichts Bremen bei der Führerscheinstelle im Stadtamt Bremen im November 1997, wie es zu erklären sei, dass die gesamte Strafakte (!) eines Beschuldigten ohne Zustimmung des Amtsgerichts an ein Medizinisch-Psychologisches Institut weitergegeben worden sei.

Der Senator für Bau, Verkehr und Stadtentwicklung hatte daraufhin meine Bedenken zum Anlaß genommen, das Verfahren in einem mit mir abgestimmten **Erlaß** so zu regeln, dass Akten über Ordnungswidrigkeiten- und Strafverfahren nur beigezogen werden, soweit sie für die Überprüfung der Eignung zum Führen von Kraftfahrzeugen **erforderlich** sind. Ist eine Beiziehung erforderlich, sieht die Fahrerlaubnisbehörde die ihr übersandte Akte umgehend auf fahreignungsrelevante Sachverhalte durch und nimmt die für die Eignungsfrage wesentlichen Unterlagen (z. B. Urteil, Strafbefehl, Entscheidung, Blutentnahme- und Vernehmungsprotokoll) in Kopie zur Führerscheinakte. Dabei sind sämtliche Angaben über Dritte, die in diesen Kopien enthalten sind, unkenntlich zu machen. Die Akte ist anschließend der übersendenden Stelle zurückzureichen. Eine Weiterleitung beigezogener Originalakten an andere Stellen erfolgt nicht.

Im November 1998 erklärte der Senator für Bau, Verkehr und Stadtentwicklung, angesichts der Neuregelung zur Eignungsüberprüfung von Fahrerlaubnisinhabern und -bewerbern durch Begutachtungsstellen (ehem. Medizinisch-Psychologisches Institut; siehe vorige Ziff.) habe er den **Vollzug seines Erlasses ausgesetzt** und werde ihn mit Inkrafttreten des neuen Fahrerlaubnisrechts zum 01. Januar 1999 aufheben. Er beruft sich dabei auf die neue Vorschrift des § 11 Abs. 6 Satz 4 FeV (siehe vorige Ziff.). Diese sei nunmehr eine gesetzliche Grundlage für die Übersendung der vollständigen Behördenakten einschließlich der beigezogenen Straf- und Ordnungswidrigkeitenakten.

Ich habe der senatorischen Behörde darauf geantwortet, dass diese Vorschrift nur die **Übersendung der Führerscheinakte an die Begutachtungsstelle** regelt, während sich der Erlaß ausschließlich auf die **Heranziehung von Ordnungswidrigkeiten-**

und Strafverfahrensakten, also den Umfang der aus diesen Akten zur Führerscheinakte zu nehmenden Dokumente erstreckt. Dabei ist § 13 Abs. 1 Nr. 1 Justizmitteilungsgesetz (JuMiG) zu beachten. Danach dürfen Gerichte und Staatsanwaltschaften personenbezogene Daten zur Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben nur übermitteln, wenn eine besondere Rechtsvorschrift dies **vorsieht oder zwingend voraussetzt**. Eine solche Vorschrift ist § 3 Abs. 4 Straßenverkehrsgesetz (StVG), wenn die Fahrerlaubnisbehörde in einem Entziehungsverfahren einen Sachverhalt berücksichtigen will, der Gegenstand der Urteilsfindung in einem Strafverfahren ist.

Es handelt sich hier also nach meinem Dafürhalten um **zwei unterschiedliche Konstellationen:** Die Führerscheinstelle übersendet nach § 11 Abs. 4 FeV zwar die **vollständigen** Akten an die Begutachtungsstelle. In diesen Akten dürfen sich aber **aus den Strafakten** nur die **erforderlichen** Unterlagen befinden. Da der vorgenannte Erlaß dem Grundsatz der Erforderlichkeit und der Vorgabe des § 13 Abs. 1 Nr. 1 JuMiG entspricht, habe ich die senatorische Behörde gebeten, ihn wieder in Kraft zu setzen. Sie hat daraufhin die Aufhebung des Erlasses bis zur endgültigen Klärung der unterschiedlichen Auffassungen zunächst zurückgestellt.

15.3. Parkausweis für Schwerbehinderte - auch ohne Namen auf der Vorderseite

Immer wieder beschweren sich autofahrende Schwerbehinderte darüber, dass ihr Name auf der Vorderseite ihres zur Nutzung von Schwerbehindertenparkplätzen berechtigenden Ausweises eingetragen wird, obwohl er sich zusammen mit der Anschrift bereits auf der Rückseite des Ausweises befindet. Weil der Ausweis hinter der Windschutzscheibe des Pkw anzubringen ist, ist er für jeden Passanten, aber auch ggf. für gezielt den Betroffenen beobachtende Straftäter, einsehbar. Die

Anschrift läßt sich dann häufig vergleichsweise einfach über Telefonbücher oder -CDs ermitteln.

Ich nehme alle Eingaben, bei denen es um die möglicherweise unnötige und/oder diskriminierende Offenbarung sensibler persönlicher Angaben wie etwa der körperlichen Behinderung geht, sehr ernst. Das Amt für Straßen und Verkehr hat auf Anfrage erklärt, die Gestaltung der Parkausweise sei durch Verkehrsblattverlautbarung des Bundesministers für Verkehr bundeseinheitlich vorgegeben. Grundsätzlich solle danach der Name zur Sicherung gegen möglichen Mißbrauch auf der Vorderseite eingetragen werden. Gleichwohl eröffne die Verlautbarung auch die Möglichkeit, das **Namensfeld auf Wunsch der Berechtigten freizulassen.** Den Beschwerdeführern empfehle ich daher, sich mit diesem Wunsch umgehend an die Behörde zu wenden und ggf. einen entsprechenden neuen Parkausweis zu beantragen.

16. Umweltschutz

16.1. Endlich: Regelungen über das Altlastenkastaster

Seit Jahren habe ich über die Notwendigkeit datenschutzrechtlicher Regelungen für das sog. **Altlastenkataster** berichtet, zuletzt unter Ziff. 14.3 meines 17. Jahresberichts vom 31. März 1995. Mir ging es vor allem darum, dass gesetzlich klar festgelegt wird, wer was unter welchen Voraussetzungen zu dieser Datensammlung **melden** muß bzw. umgekehrt welche Personen und Stellen unter welchen Bedingungen Auskünfte aus diesem Register erhalten können. Denn diese **Auskünfte** können sehr **sensible**, für den wirtschaftlichen Wert der Grundstücke entscheidende Informationen enthalten.

Endlich ist es soweit: Der Art. 1 des Gesetzes zur Änderung abfallrechtlicher Vorschriften vom 04. August 1998

(Brem.Gbl. S. 223) regelt dies in den §§ 15c und 15d Bremisches Ausführungsgesetz zum Kreislaufwirtschafts- und Abfallgesetz (BremAGKrW-/AbfG).

Während § 15c BremAGKrW-/AbfG definiert, was **schädliche Bodenveränderungen** und **Altlasten** sind, legt § 15d Abs. 1 BremAGKrW-/AbfG fest, dass die zuständige Behörde, soweit erforderlich, **Erhebungen** zur Erfassung von schädlichen Bodenveränderungen, Verdachtsflächen, Altlasten und altlastenverdächtigen Flächen durchführt und dies in einem Bodenkataster erfaßt. Dazu zählen neben den Standortangaben insbesondere Namen von ehemaligen und gegenwärtigen Nutzungsberechtigten und Eigentümern sowie deren Anschriften.

Abs. 2 dieser Vorschrift **verpflichtet** die Behörden und Einrichtungen des Landes und der Stadtgemeinden, die ihnen vorliegenden Erkenntnisse über schädliche Bodenveränderungen oder Altlasten im Sinne von § 15c BremAGKrW-/AbfG **mitzuteilen**. Außerdem sind nach Abs. 3 dieser Vorschrift Eigentümer und Nutzungsberechtigte von Grundstücken verpflichtet, ihnen bekannt gewordene Erkenntnisse über Altablagerungen und Altstandorte auf ihren Grundstücken unverzüglich der zuständigen Behörde anzuzeigen.

Der Senator für Frauen, Gesundheit, Jugend, Soziales und Umweltschutz, Bereich Umweltschutz und Frauen, als zuständige das Bodenkataster führende Behörde, ist nach Abs. 4 dieser Vorschrift befugt, anderen Behörden und Einrichtungen des Landes sowie den Stadtgemeinden Informationen aus dem Kataster zu **übermitteln**, soweit dies zur Wahrnehmung der diesen Stellen auf den Gebieten der Gefahrenermittlung, Gefahrenabwehr, Überwachung oder Planung obliegenden Aufgaben und aus Gründen des fiskalischen Grundstücksverkehrs erforderlich ist.

Außerdem erteilt die das Bodenkataster führende Behörde den **Eigentümern** und Nutzungsberechtigten **Auskunft** aus dem Kataster sowie aus sonstigen Unterlagen und gewährt Einsicht in dem gleichen Umfang. **Dritten** wird Einsicht in das Kataster und Auskunft gewährt, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Abs. 5 dieser Vorschrift regelt, dass, soweit Behörden oder andere Stellen Erkenntnisse über schädliche Bodenveränderungen, Verdachtsflächen, Altlasten oder altlastenverdächtige Flächen der Öffentlichkeit zugänglich machen, diese Bekanntgabe keine Angaben enthalten darf, die einen Bezug auf eine bestimmte oder bestimmbare natürliche Person zulassen. Dies gilt nicht, wenn solche Angaben offenkundig sind oder im Einzelfall ihre Bekanntgabe zur Abwehr von Gefahren oder anderen, schutzwürdige Belange des Betroffenen überwiegenden Gründen des Gemeinwohls erforderlich ist.

An den Beratungen zu diesen datenschutzrechtlichen Bestimmungen bin ich rechtzeitig beteiligt worden. Ich hoffe, dass die Rechtsunsicherheit beim Umgang mit Informationen über Böden mit festgestellten oder vermuteten Verunreinigungen, die immer wieder zu Eingaben und Beschwerden geführt hat, jetzt beseitigt ist.

17. Finanzen

17.1. Hundesteuer - "Fahndung" mit privater Firma

Der Magistrat Bremerhavens hat in der Zeit von April bis Juli 1998 durch eine beauftragte Privatfirma eine sog. **Hundebestandsaufnahme** durchführen lassen. Angestellte dieser Firma gingen von Haus zu Haus, um nicht angemeldete Tiere festzustellen. Diese Aktion fand in der lokalen wie

regionalen Presse ein großes - zuweilen auch humoristisches - Echo.

Die datenschutzrechtliche Fragestellung ergab sich daraus, dass bei dieser Ermittlungsaktion Steuerdaten, d.h. Angaben von Bürgerinnen und Bürgern zur Feststellung eines (kommunal)steuerrechtlichen Tatbestands, erhoben wurden. Anders ausgedrückt: Eine Privatfirma wurde im Zusammenhang mit einer hoheitlichen Verwaltungsmaßnahme eingesetzt.

Ich habe mich nicht zuletzt aufgrund zahlreicher Nachfragen und Beschwerden gegenüber dem Magistrat dahingehend geäußert, dass klar sein muß, dass diese privaten "Steuerfahnder" keinerlei amtlichen Befugnisse haben. Daraus folgt, dass sie sich mit ihren Fragen nur an den möglichen Hundehalter (z.B. Grundstückseigentümer, Mieter o.ä.), also nicht an Dritte wie Nachbarn o.ä. wenden dürfen, sowie die Befragten darauf hinweisen müssen, dass die Beantwortung der Fragen **freiwillig** ist. Auch haben sie z.B. keine Ausforschungsrechte auf dem Grundstück oder in den Gebäuden.

Aufgrund meiner Stellungnahme wurden die Befrager ergänzend über ihre Befugnisse und die Handhabung der ausgefüllten Vordrucke belehrt und dem beauftragten Unternehmen zusätzliche Verpflichtungen aufgegeben (z.B. Übergabe aller Unterlagen an die Stadt; kein Verbleib von Dokumenten in den Firmenräumlichkeiten).

Ende 1998 habe ich beim Magistrat stichprobenweise die zusammenfaßten Unterlagen einschließlich der Aufzeichnungen der Kontrolleure geprüft und festgestellt, dass abgesehen von wenigen Ausnahmen die datenschutzrechtlichen Anforderungen eingehalten waren.

17.2. Steuerberaterkammer - Mitteilungsblatt als "Pranger"?

Die Hanseatische Steuerberaterkammer Bremen veröffentlicht in ihrem Mitteilungsblatt im Zusammenhang mit unerlaubter Hilfe in Steuersachen u.a. strafrechtliche und zivilrechtliche **Gerichtsentscheidungen** sowie strafbewehrte **Unterlassungserklärungen**.

Ich bin mit meinen Kollegen in den anderen Ländern der Auffassung, dass die hier in Rede stehenden **Veröffentlichungen** unzulässig sind. Die Steuerberaterkammer wäre zu einer solchen Veröffentlichung nur befugt, wenn eine spezielle Rechtsvorschrift oder die Übermittlungsbestimmungen des BrDSG dies zuließen. § 23 Abs. 2 des Gesetzes über den unlauteren Wettbewerb (UWG) gestattet die Veröffentlichung von Entscheidungen nach diesem Gesetz nur dann, wenn der Richter dies ausdrück-lich angeordnet hat. Die Zulässigkeitsvoraussetzungen des § 17 BrDSG für die Weitergabe von Daten durch Behörden an private Stellen und Personen sind nicht erkennbar; insbesondere bleibt unklar, welchen gesetzlichen Zweck die Kammer mit dieser Publikation im Kammerorgan erreichen will. Auch die These, die Publikation im Mitteilungsblatt stelle gar keine Datenübermittlung, sondern nur eine interne Information dar, ist nicht haltbar. Zum einen sind die einzelnen freiberuflichen Steuerberater keine Teile der öffentlich-rechtlichen Institution Steuerberaterkammer, zum anderen werden die Mitteilungsblätter auch an die Kammern anderer Länder, an Finanzbehörden und weitere Adressaten versandt.

Aufgrund dieser datenschutzrechtlichen Bedenken haben in einigen anderen Bundesländern die Steuerberaterkammern diese Veröffentlichungspraxis eingestellt. Die hiesige Kammer hält an ihrer aus meiner Sicht unzulässigen Handhabung fest.

17.3. Kosten- und Leistungsrechnung (KLR) - "gläserne" Beschäftigte?

Die Einführung der KLR dient der Erzielung von Kostentransparenz und der Erreichung kostenbewußten Handelns bei den Mitarbeiterinnen und Mitarbeitern in den Dienststellen. Sie ist ferner Grundlage für die Budgetierung von Mitteln und kann zugleich zur Leistungsverrechnung gegenüber anderen Behörden oder von Dienstleistungen gegenüber Bürgern genutzt werden. Zielsetzung der KLR ist es, die Kosten und den Umfang der von der Verwaltung erbrachten oder zu erbringenden Leistungen sowie die hierbei erwirtschafteten Erträge festzustellen.

In Bremen ist die Einführungsphase bereits weit vorangeschritten und durch die Novelle zur Landeshaushaltsordnung (BremGbl. Nr. 64 vom 28.12.1998) rechtlich abgesichert. Diese enthält keine Regelung, wonach eine **personenbezogene** Verarbeitung von Bürger- oder Mitarbeiterdaten erforderlich wäre. Bei der KLR geht es nicht um die Identität der eine Verwaltungsleistung oder –maßnahme erbringenden Bediensteten, sondern um Informationen in aggregierter Form (vgl. auch o. Ziff. 12.2.).

Allerdings kann es im Einzelfall zu einem Personenbezug der Daten von Mitarbeiterinnen und Mitarbeitern etwa bei detaillierten Kostenstellenrechnungen kommen. Hier muß darauf geachtet werden, dass der Personenbezug so weit bzw. so früh wie möglich aufgelöst wird, etwa durch die Bildung von Standardwerten als Basis für die jeweiligen Rechnungsgrößen.

Diese und weitere datenschutzsichernde Punkte hat der Senator für Finanzen in das **Datenschutzkonzept**, das auch Rahmendatenschutzkonzept für die übrige Verwaltung sein soll, aufgenommen. Sie sollen sowohl durch verfahrenstechnische Vorkehrungen umgesetzt als auch durch organisatorische Maßnahmen und Anweisungen zusätzlich

abgesichert werden. Die Einhaltung dieser Vorgaben werde ich im kommenden Berichtszeitraum aufmerksam beobachten. Wie im Vorwort (vgl. o. Ziff. 1.2.) angesprochen, geht es um nicht weniger als darum, dass es zu verhindern gilt, dass die wünschenswerte Transparenz staatlichen Ausgabeverhaltens im Nebeneffekt die Voraussetzungen für den "gläsernen" Beschäftigten schafft.

17.4. SEKT - Verschlüsselung von Zahlungsdaten

In der Bremischen Verwaltung wird ein Projekt vorangetrieben, mit dem die "sichere E-Mail-Kommunikation für den Austausch von Transaktionsdaten" (Abkürzung: SEKT) gewährleistet werden soll. Gegenstand dieser Anwendung ist die **verschlüsselte und doppelt-signierte Übertragung** von Daten zur Zahlbarmachung von Auszahlungen und zur Entgegennahme von Einnahmen im Verkehr zwischen den einzelnen Haushalts- und Rechnungsstellen in den bremischen Behörden und der Landeshauptkasse.

Bei der Konzeption dieses Projektes hat mich der Senator für Finanzen frühzeitig beteiligt und mit dem TuI-Referat der Senatskommission für das Personalwesen und mir die Voraussetzungen für eine aus der Sicht des Datenschutzes einwandfreie Datenübermittlung abgestimmt.

18. Datenschutz in der Privatwirtschaft

18.1. GeldKarte: Umfassende Datenspeicherung in den Evidenzzentralen

Die **GeldKarte** soll als "**elektronische Geldbörse**" die bargeldlose Zahlung von Kleinbeträgen ermöglichen; über ihre Einführung und die sich abzeichnenden datenschutzrechtlichen Fragestellungen enthielt bereits der 18. Jahresbericht einen ausführlichen Abschnitt (vgl. 18. JB, Ziff 18.1.). Die GeldKarte ist Teil eines äußerst **komplexen Systems von Datenverarbei-tungsvorgängen und Datenströmen** zwischen

Kunden, Händlern (Akzeptanzstellen) sowie jeweils mehreren Banken und sog. Evidenzzentralen.

Die im letzten Jahr begonnenen Gespräche der Datenschutzaufsichtsbehörden mit dem Zentralen Kreditausschuß (ZKA) – dem Zusammenschluß der drei großen Spitzenverbände des Kreditgewerbes BdB, BVR und DSGV – über die datenschutzrechtliche Beurteilung der GeldKarte (vgl. dazu 19. JB, Ziff. 20.2.) sind im Berichtszeitraum fortgesetzt worden, konnten aber nicht zuletzt wegen Informationsdefiziten und der Weiterentwicklung der Systeme, in die die GeldKarte eingebunden ist, nicht zum Abschluß gebracht werden. Die grundsätzliche Bewertung soll aber 1999 abgeschlossen werden.

Voraussetzung für die datenschutzrechtliche Beurteilung eines solchen Systems ist, dass dessen genaue Funktionsweise und die damit einhergehenden einzelnen Datenverarbeitungsschritte der verschiedenen beteiligten Stellen genau bekannt sind. Erst im Spätherbst 1998 wurde einer kleinen Delegation aus Vertretern der Datenschutzaufsichtsbehörden und der Datenschutzbeauftragten die Möglichkeit gewährt, umfassenden Einblick in **die einzelnen Datenverarbeitungsschritte** zu nehmen, die **innerhalb einer sogenannten "Evidenzzentrale"** im Rahmen der Verwendung der GeldKarte ablaufen. Die Vorführung fand in einer von derzeit vier Evidenzzentralen statt, und zwar im Rechenzentrum der Sparkassen, das zentral für die gesamte Bundesrepublik die Abwicklung des Zahlungsverkehrs mit GeldKarten für den Bereich der Sparkassen durchführt.

In diesem Rahmen hat das Rechenzentrum folgende beiden Funktionen:

Soweit mit der GeldKarte bezahlt wurde, die von einer Sparkasse ausgegeben worden ist, nimmt die Evidenzzentrale die

im Sparkassenverbund erforderlichen Buchungen gegenüber den jeweils betroffenen Sparkassen selbst vor.

Soweit mit GeldKarten anderer Bankorganisationen, wie z. B. der Raiffeisenbanken, gezahlt wurde, übernimmt die Evidenzzentrale die Aufgabe der Distribution und leitet die für das Verfahren der Abrechnung erforderlichen Datensätze weiter an die für die jeweilige Karte zuständige Evidenzzentrale.

Die Datenverarbeitungsvorgänge werden dabei umfassend dokumentiert und lange archiviert. Die einzelnen auf der Händlereinreichungsdatei **gespeicherten Daten** über die einzelnen Zahlvorgänge mit Informationen über das Händlerterminal, an dem bezahlt wurde, Uhrzeit und Kartennummer sollen nach Angaben der Kreditwirtschaft bis zu **sieben Jahren archiviert** werden.

Damit entsteht im Lauf der Jahre ein riesiges Archiv aller mit der jeweiligen Karte getätigten Zahlungsvorgänge. Das Datenschutzrisiko besteht darin, dass es möglich ist, **kartenbezogen** festzustellen, an welchen Terminals (Händlern) die Karte zum Einsatz gekommen ist. Da dort je nach Händler verschiedene Dienstleistungen oder Warengruppen bezahlt werden, könnte auf diese Informationen bezogen ein Profil zu jeder Karte erstellt werden. Ebenso ließe sich verbunden mit den Uhrzeiten ein Bewegungsprofil der Kartenbenutzung herstellen. Da zur Zeit die GeldKartenfunktion ganz überwiegend nur auf der **Euroscheckkarte** angeboten und die Ladung dieser Karten ganz überwiegend durch Abbuchungen vom eigenen Konto realisiert wird, könnte in diesen Fällen ein Personenbezug auf den Inhaber der Karte erzeugt werden.

Ich habe mich daher in den Gesprächen mit der Kreditwirtschaft immer wieder dafür eingesetzt, dass in größerem Umfang als bisher auch der Einsatz

kontounabhängiger GeldKarten ermöglicht wird, weil diese Karten anders als die Euroscheckkarten anonym ausgegeben werden können, so dass nicht oder aber nur schwer nachvollzogen werden kann, wer mit einer solchen Karte bezahlt hat. Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Konferenzentschließung die Forderungen nach Anonymisierung der Umsatzdaten und dem Angebot konto-ungebundener Karten bekräftigt (vgl. unten Ziff. 20.2.). Die Kreditwirtschaft hat zugesagt, zu recherchieren, in welchem Umfang nicht kontobezogene GeldKarten (sogenannte "White Cards") bisher ausgegeben worden sind. Dieser Punkt wird in den Gesprächen mit der Kreditwirtschaft im Jahre 1999 noch weiter geklärt.

Ein weiterer Datenschutzansatz, die mit dem Einsatz der GeldKarte verbundenen Identifizierungs- und Profilbildungsrisiken zu minimieren, besteht darin, die **Speicherdauer bzw. Archi-vierung der einzelnen Transaktionsdatensätze möglichst kurz zu halten**. Eine Reduzierung der Datensätze dahingehend, dass ein Kartenbezug nicht mehr möglich ist, ist unter den gegebenen Bedingungen deshalb nicht möglich, weil diese Daten benötigt werden, um in Prüfverfahren sicherzustellen, dass Überzahlungen, Doppeleinreichungen oder Manipulationen verhindert bzw., wenn sie passieren sollten, frühzeitig erkannt werden können.

Ich verfolge daher den Ansatz, die Speicherdauer von jetzt vorgesehenen sieben Jahren auf das **rechtlich wie kontrolltechnisch gebotene Minimum** zu reduzieren. Die Kreditwirtschaft hat in den bisherigen Gesprächen erklärt, dass zur Sicherstellung ihrer Prüfroutinen eine Aufbewahrungsdauer von einem halben, maximal von einem Jahr ausreichend wäre. Steuerrechtliche, handelsrechtliche und kreditaufsichtsrechtliche Regelungen verpflichteten sie aber

zu einer längeren Vorhaltung dieser Transaktionsdatensätze, eine Auffassung, die es im einzelnen noch zu überprüfen gilt.

Ungeachtet dessen muß nach meiner Auffassung noch einmal prinzipiell hinterfragt werden, ob angesichts der Tatsache, dass sich die einzelnen Zahlungsvorgänge auf der Händlerseite (Akzeptanzstellen) in den Registrierkassen abbilden, die Notwendigkeit besteht, sie darüber hinaus auch bei den Evidenzzentralen kartengebunden zu archivieren. Ich habe mich daher im letzten Jahr mit einem Schreiben an den Bundesbeauftragten für den Datenschutz gewandt und diesen gebeten, das Problem mit dem Bundesfinanzministerium zu erörtern. Diese Gespräche sind nach Auskunft des Bundesbeauftragten für den Datenschutz noch nicht abgeschlossen; ich werde daher auch diesen Ansatz im Jahre 1999 weiterverfolgen. Dabei wird auch das Bundesaufsichtsamt für das Kreditwesen in die Überlegungen mit einbezogen werden müssen.

Auch die **weitere Entwicklung des Einsatzes der GeldKarte** verspricht interessante Fragestellungen. Zum einen ist erkennbar, dass in den Chip Zusatzfunktionen integriert werden sollen, wie z. B. gewisse Rabattsysteme oder Tickets im öffentlichen Personennahverkehr. Nach der Einführungs- und Verbreitungsphase kann es mit der europäischen Öffnung dieses Systems auch über die Ländergrenzen hinweg zu einem verbindlichen Einsatz mit der dazu gehörigen Struktur von Dateien und Vernetzungen kommen. Schließlich könnten die Bezahl- wie die Ladefunktionen der GeldKarte auch über das Internet aktiviert bzw. genutzt werden.

In Bremen bestehen im Zusammenhang mit dem Projekt MEDIA@Komm (vgl. o. Ziff. 6.1.) Planungen für einen

elektronischen Fahrschein bei der BSAG und einen **Studentenausweis** mit integrierter GeldKarte.

18.2. Videoüberwachung in einer Betriebshalle: Kompromiß in Betriebsvereinbarung

Der Betriebsrat einer Firma aus der Hafenwirtschaft hatte mich darauf hingewiesen, dass in einer Betriebshalle rund um die Uhr **Videoaufzeichnungen mit verdeckten Kameras** erfolgen, und um rechtliche Stellungnahme gebeten. Für den Bereich der Privatwirtschaft ist die **Rechtslage** insofern **unbefriedigend**, als das Bundesdatenschutzgesetz (BDSG) nur dann zur Anwendung kommt, wenn mit der Videokamera nicht nur beobachtet, sondern auch aufgezeichnet wird, und diese Aufzeichnung wie etwa bei digitalisierter Aufnahmetechnik als "Datei" eingestuft werden kann. Bei der anstehenden Novellierung des BDSG müssen Voraussetzungen und Grenzen der Videoüberwachung dringend geklärt werden (s. o. Ziff. 1.1.2.). Der BDSG-Entwurf der Bundestagsfraktion BÜNDNIS 90/DIE GRÜNEN aus der letzten Wahlperiode (BT-Drucks. 13/9082), der in der neuen Legislaturperiode wieder eingebracht worden ist, enthält in § 33 dazu bereits eine spezielle Vorschrift.

Ich habe dem Betriebsrat die Rechtssituation sowohl aus datenschutz- als auch aus arbeitsrechtlichem Blickwinkel erläutert. Einschlägig sind in diesem Zusammenhang u.a. die Entscheidungen des Bundesarbeitsgerichts (BAG) vom 07. Oktober 1987 (Az.: 5 AZR 116/86) und des Landesarbeitsgerichts (LAG) Köln vom 30. August 1996 (Az.: 12 Sa 639/96).

Nach dem Urteil des BAG kann eine **Verletzung des Persönlichkeitsrechts eines Arbeitnehmers** vorliegen, wenn er einem ständigen lückenlosen Uberwachungsdruck dadurch unterworfen wird, dass der Arbeitgeber sich vorbehält, jederzeit ohne konkreten Hinweis den Arbeitsplatz durch versteckt

aufgestellte Videokameras zu beobachten. Nach diesem Urteil kann eine Maßnahme dieser Art allerdings gerechtfertigt sein, wenn überwiegende schutzwürdige Interessen des Arbeitgebers sie erfordern. Hierzu bedarf es einer substantiellen Begründung.

Nach dem Urteil des LAG Köln stellen Aufzeichnungen mit einer verdeckten Videokamera in der Regel einen rechtswidrigen Eingriff in das Persönlichkeitsrecht der beobachteten Arbeitnehmer dar. Die insoweit erlangten Aufzeichnungen dürfen nicht verwertet werden.

Ich habe diese Rechtsprechung auch der Geschäftsleitung mitgeteilt. Daraufhin ist die Videoaufzeichnung zunächst eingestellt worden. Inzwischen haben die Geschäftsleitung und der Betriebsrat eine **Betriebsvereinbarung** abgeschlossen, die den Einsatz von zwei Überwachungskameras in konkret benannten Be-triebsbereichen zum Schutz der Anlagen vor unbefugtem Betre-ten durch betriebsfremde Personen und zur Überwachung der Verkehrssicherheit auf und an der Pier regelt. Vereinbart worden ist, dass diese Kameras nicht zur Überwachung der zu Umschlagsarbeiten auf der Pier eingesetzten Mitarbeiter verwendet, die Kameras zum Beginn des Umschlagbetriebes ausgeschaltet und zum Umschlagsende wieder eingeschaltet werden.

18.3. Videoüberwachung an Tankstelle: abgestuftes Verfahren

Bei der Überprüfung einer Bremer Tankstelle aus anderen Gründen stellte ich auch fest, dass auf dem Vorplatz sieben und im Kassen- und Verkaufsraum vier Videokameras offen sichtbar installiert waren. Ein weiteres Gerät überwacht den Bereich der Waschanlage. Die Videokameras im Außenbereich bestreichen einen Raum nur innerhalb der Grundstücksgrenzen; im Bereich der Tanksäulen sind sie so eingestellt, dass sie eine Sicht auf das Kfz.-Kennzeichen und den Fahrer bzw. die

betankende Personen ermöglichen. Neben der Kasse befindet sich ein Monitor, von dem aus die Bilder aller Kameras abgefordert werden können. Im Büro befinden sich u.a. die technische Steuerung der Gesamtanlage sowie das Bandaufzeichnungsgerät.

Die Gesamtanlage ist von dem das Mineralöl liefernden Unternehmen zur Verfügung gestellt und installiert worden. Es kann daher davon ausgegangen werden, dass auch in anderen Tankstellen des Konzerns entsprechende Anlagen zum Einsatz kommen.

Ich habe gegen die Nutzung bzw. die Funktionsweise der Videoanlage im Ergebnis keine durchgreifenden datenschutzrechtlichen Einwände geäußert (zur Rechtslage generell vgl. die vorige Ziff.). Zu berücksichtigen ist dabei die **Interessenlage bzw. Risikosituation des Pächters**, der auf den notwendigen Schutz vor Betrug, Benzindiebstahl, Beschädigungen etc. verweist. Die Aufzeichnung von Kfz.-Kennzeichen und Verbrauchsdaten dient dazu, den Umfang des Rechtsgeschäfts sicher zu dokumentieren und den Erhalt des zu zahlenden Geldbetrages sicherzustellen. Zwar wäre es eigentlich notwendig, dass nach Bezahlung die den jeweiligen Kunden betreffende Sequenz auf dem Videoband sofort gelöscht wird; die eingesetzte Technik läßt dies aber nicht zu. Da die Aufzeichnung aber spätestens nach einer Woche gelöscht bzw. überschrieben wird, schien mir diese Speicherfrist vertretbar. Im übrigen wurde mir versichert, dass in Fällen, in denen es zu Benzindiebstahl gekommen sei, lediglich die den Tatverdächtigen betreffende Sequenz ausgedruckt und an die Polizei zu weiteren strafrechtlichen Ermittlungen abgegeben werde. Nur dann, wenn es zu einem räuberischen Kassenüberfall kommen sollte, werde das gesamte Band übergeben. Auch dieses **abgestufte Verfahren der Übermittlung** gibt keinen Grund zur Beanstandung.

18.4. Beschränkung des bankinternen Zugriffs auf Kontoinformationen

Immer wieder gibt es Beschwerden von Bankkunden, denen Nachteile dadurch entstanden sind, dass nicht mit der unmittelbaren Kontoführung beauftragte Angestellte auf deren Daten für **private oder jedenfalls nicht vertrags- bzw. bankbezogene Zwecke** zugegriffen haben. Ermöglicht wird das Einsehen und Auslesen von Kundendaten durch eine Vielzahl von Mitarbeitern in verschiedenen Filialen dadurch, dass die Kontendaten in dem zentralen Informationssystem des jeweiligen Kreditinstituts abgespeichert sind.

Ich habe daher bereits vor mehreren Jahren gegenüber der Kreditwirtschaft einen Vorstoß unternommen und Vorschläge unterbreitet, um mit Hilfe technischer Mittel solchen **unberechtigten Zugriffen** Einhalt zu gebieten. Meine Vorstellung war dabei, die Zugriffsmöglichkeiten auf Kontodaten einzelner Kunden auf deren Antrag hin so zu gestalten, dass nur Personen der betreuenden Bankfiliale sowie Personen, die mit Funktionen der Bankaufsicht und der Revision betraut sind, zum Abruf berechtigt sind

Dieses Anliegen, das auch von den anderen Aufsichtsbehörden für den Datenschutz unterstützt wird, wurde letztmals im Frühjahr 1998 mit Vertretern des Zentralen Kreditausschusses (ZKA) besprochen. Leider konnten die Aufsichtsbehörden keinerlei Entgegenkommen feststellen. Die Vertreter der Kreditwirtschaft gaben dabei zu bedenken, dass die Einrichtung von Zugriffsbeschränkungen für bestimmte Filialen bankrechtlich problematisch und technisch nur mit hohem Aufwand zu realisieren sei. Auch wegen der hohen Kosten und des personellen Aufwands könnten solche Maßnahmen nicht vertreten werden, da es sich bei den Beschwerden offenbar nur um Einzelfälle handele.

Ich halte diese Argumentation nicht für stichhaltig und bedauere die mangelnde Bereitschaft, die technische Infrastruktur berechtigten Kundenwünschen anzupassen.

18.5. Versicherungen im Internet - erste Gespräche

Die Versicherungswirtschaft nutzt das Internet bereits in beträchtlichem Umfang. Bei meinen Recherchen im Netz habe ich festgestellt, dass nicht nur Informationsangebote abrufbar sind, sondern auch **Modellrechnungen** zu Beitragshöhe oder Versicherungsverlauf und **Antragstellung online** angeboten werden. In letzteren Fällen übermittelt der Kunde seine Personalien und ggf. Gesundheits- und Kontoangaben über das Netz. Bei Antragsbestätigungen läuft der Übertragungsweg umgekehrt von der Versicherung an den Kunden. In der Papierform verbleiben bisher noch der vom Versicherungsnehmer unterschriebene Antrag und der vom Unternehmen ausgestellte Versicherungsschein.

Die mit der Nutzung des Internet, insbesondere mit der Übertragung von zum Teil sensiblen Daten von Versicherungsnehmern, verbundenen datenschutzrechtlichen und datensicherungstechnischen Fragen werden zwischen den Aufsichtsbehörden für den Datenschutz und dem Gesamtverband der Deutschen Versicherungswirtschaft erörtert. Nach Angaben von dessen Vertretern sind die auf der Grundlage eines Internet-Kontakts zustandegekommenen Abschlüsse zahlenmäßig derzeit zwar noch gering, doch gebe es elektronische Angebote bereits von mehr als der Hälfte der Gesellschaften und in nahezu allen Versicherungssparten.

Für die Datenschutzaufsichtsbehörden ist es ein wichtiger Punkt, dass Kunden möglichst viele Angebote nutzen können, ohne gegenüber den Rechnern der Versicherungswirtschaft ihre Identität preisgeben zu müssen. Auch müssen die Netznutzer von den Unternehmen über die Datensicherungsrisiken bei der

Übertragung ihrer Angaben an die Versicherungsgesellschaften umfassend informiert werden.

Immerhin bieten einige Versicherungsunternehmen für ihre Online-Angebote bereits eine **Verschlüsselungsmöglichkeit** an, über deren Schutzwirkung ich allerdings noch keine Aussage treffen kann. Im übrigen setzt die Branche auf die Sicherungswirkung der "**digitalen Signatur**". Die Gespräche werden fortgesetzt, um in einem möglichst frühen Stadium der Internet-Planungen die Vorstellungen der Aufsichtsbehörden einzubringen.

18.6. "Düsseldorfer Kreis "- Wichtige Themen im Überblick

Die **Obersten Datenschutzaufsichtsbehörden der Bundesländer** haben sich im sog. **Düsseldorfer Kreis**, einem informellen Beratungs- und Abstimmungsgremium, zusammengeschlossen. Unter Federführung des Innenministeriums des Landes Nordrhein-Westfalen als der für dieses Bundesland zuständigen Obersten Datenschutzaufsichtsbehörde werden datenschutzrechtliche Fragen von übergreifender oder überregionaler Bedeutung erörtert. Zu bestimmten Themenfeldern wie z. B. Kreditwirtschaft, Versicherungen, Auskunfteien, Telekommunikation/Tele- und Mediendienste hat der Düsseldorfer Kreis **Arbeitsgruppen** eingerichtet, die unter sich, aber auch mit Verbandsvertretern der Wirtschaft, Softwarehäusern oder anderen Institutionen datenschutzrelevante Fragen erörtern.

Wichtige Themenfelder im Berichtsjahr waren u. a. die **Novellierung des BDSG** (nicht-öffentlicher Teil), die Umsetzung der **EG-Datenschutzrichtlinie** in den Ländern, die unmittelbare Wirkung der EG-Datenschutzrichtlinie nach Ablauf der Umsetzungsfrist(o. Ziff. 5.), **GeldKarte**/Elektronische Geldbörse (vgl. o. Ziff. 18.1.), das

Verhältnis betrieblicher Datenschutzbeauftragter zu den Betriebsräten nach dem BAG-Urteil vom 11.11.1997, **Telearbeit**, Datenverarbeitung durch **Privatärztliche Verrechnungsstellen**, **Patientenunterlagen** eines verstorbenen Arztes, **Schufa-Selbstauskunft** für Mietinteressenten, Schufa-Anschluß von Telekommunikationsdienstleistern, **Warndatei der Mobilfunkanbieter**, Gründung der neuen Auskunftei Creditreform Experian GmbH, und das sog. **Scoringverfahren** der Kreditauskunfteien zur Bewertung der Bonität von Kreditantragstellern.

Der Düsseldorfer Kreis und seine Arbeitsgruppen fassen keine förmlichen Beschlüsse, die dann für die örtlichen Aufsichtsbehörden bindend wären. Die hier erfolgende Meinungsbildung prägt allerdings die Meinung der Datenschutzaufsichtsbehörden wesentlich mit. Leider ist die Abstimmung in diesen Gremien relativ schwerfällig; es dauert manchmal lange, bis ein Thema abschließend erörtert werden kann - manchmal zu lange für die Eingeber bzw. Beschwerdeführer, die betroffenen Unternehmen und die örtlich zuständige, unter Entscheidungsdruck stehende Datenschutzaufsicht. Allerdings liegt dies gelegentlich auch an der mangelnden Informations- und Kooperationsbereitschaft der Gesprächspartner, d.h. der jeweiligen Branchenverbände. Immerhin hat der Düsseldorfer Kreis beschlossen, die Zahl seiner Arbeitsgruppen zu reduzieren und, was ich sehr begrüße, seine Arbeitsweise effizienter zu gestalten.

19. Meldepflichtige Stellen: Statistische Übersicht, Prüfergebnisse, Bußgeldverfahren

19.1. Statistische Übersicht - Entwicklungen

Die Zahl der Stellen, die bei mir zum Register nach § 32 BDSG gemeldet sind, hat sich im Berichtszeitraum wiederum leicht **erhöht**. Insgesamt weist das Register Anfang Januar 1999 130 Stellen gegenüber 124 Stellen im Vorjahr aus. Davon

befinden sich 110 Stellen in Bremen und 20 Stellen in Bremerhaven. Der regionale Schwerpunkt liegt also weiterhin eindeutig in Bremen. Die Mehrzahl der angemeldeten Stellen ist dem Bereich der Auftragsdatenverarbeiter, insbesondere den Dienstleistungsanbietern in den Gebieten Datenverarbeitung und Telekommunikation zuzuordnen.

Das Register nach § 32 BDSG ist kein Selbstzweck. Ursprünglich war es in erster Linie gedacht zur Information der Öffentlichkeit; heute ist es vor allem Grundlage und wesentliche Orientierung für meine Prüftätigkeit nach § 38 Abs. 2 BDSG.

Die Entwicklung im Bereich der Informations- und Kommunikationstechnik, die Dezentralisierung der Datenverarbeitung, die Auslagerung von DV-Aktivitäten sowie neuartige DV- und TK-Dienstleistungen führen zu häufigen Ergänzungen und Änderungen im Register. Aktuellstes Beispiel: Im Zuge der Liberalisierung des Fernsprechmarktes, der technischen Entwicklungen im Bereich der Datenverarbeitung und der Telekommunikation, der zunehmenden Bündelung und Auslagerung betrieblicher Funktionen (Outsourcing) sowie der Effektivierung bestimmter Dienstleistungsfunktionen der Unternehmen wie z. B. Auskunfts- und Servicedienste, Bestellannahme, Akquisition, Telefonmarketing hat in den letzten Jahren die sog. **Call-Center-Branche** einen erheblichen Aufschwung mit zum Teil neuartigen Dienstleistungen erlebt.

Auch in Bremen bzw. Bremerhaven gibt es inzwischen eine ganze Reihe derartiger Betriebe bzw. Unternehmen. Soweit diese Betriebe bzw. Unternehmen geschäftsmäßig personenbezogene Daten dateibezogen verarbeiten - was in allen mir bekannten Fällen wegen der Tätigkeit und der eingesetzten Datenverarbeitungs- und

Telekommunikationstechnik gegeben ist - gelten für sie die datenschutzrechtlichen Bestimmungen, insbesondere das BDSG. Ich habe inzwischen mehrere Call-Center als **DV-Dienstleister** in meinem Register nach § 32 BDSG. Die Zahl dürfte im Hinblick auf die stürmische Entwicklung in diesem Bereich und eine gewisse Dunkelziffer in den nächsten Jahren ansteigen. Festzustellen ist dabei, dass man nicht pauschal jedes Call-Center ins Register nach § 32 BDSG übernehmen kann, sondern die Meldepflicht stets sehr genau im **Einzelfall** an Hand der jeweiligen konkreten Datenverarbeitungs- und Telekommunikationstätigkeit feststellen muß.

Registeränderungen ergeben sich auch dadurch, dass ich - ohne gesetzlich dazu verpflichtet zu sein - Betriebe, bei denen ich aufgrund von Handelsregistereintragungen oder von Branchenzuordnungen eine Meldepflicht vermute, anschreibe und um Prüfung ihrer Meldepflicht (die ja bußgeldbewehrt ist) bitte. Bei einigen angeschriebenen Betrieben ergibt sich, z.T. auch aufgrund örtlicher Feststellungen, tatsächlich, dass meldepflichtige Tätigkeiten ausgeübt werden, die dann zu einer Registereintragung führen.

Einzelheiten zum Stand des Registers zeigt die nachfolgende Übersicht:

Art der Tätigkeit	**insgesamt**	**Bremen**	**Bremerhaven**
Speicherung personenbezogener Daten zum Zwecke der Übermittlung (insgesamt)	**6**	**4**	**2**
Auskunfteien	4	3	1
Adreßverlage/Adreßhändler	2	1	1
Speicherung personenbezogener Daten zum Zwecke der anonymisierten Übermittlung (insgesamt)	**4**	**4**	
Markt- u. Meinungsforschung	4	4	

Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (insgesamt)	**120**	**102**	**18**
Datenerfassung	6	6	
Dienstleistung/Rechenzentren	94	79	15
Mikroverfilmer	4	4	
Mailboxdienste	8	5	3
Datenlöschung/Datenträgervernichtung	8	8	
Gesamt	**130**	**110**	**20**

19.2. Neue Rahmenbedingungen für Datenschutzkontrollen

Nach § 38 BDSG gibt es Anlaßprüfungen (Abs. 1) sowie anlaßlose Prüfungen/Prüfungen von Amts wegen bei den Registerfirmen, d.h. vor allem Auskunfteien, Direktwerbeunternehmen sowie Markt- und Meinungsforschungsinstituten (Abs. 2). Einbezogen sind dabei sowohl die herkömmliche Datenverarbeitung (Batch, Dialog, Fern) als auch die neuen **Teledienste** (z.B. Telebanking, electronic commerce, online-Datendienste). Datenschutzprüfungen bei den Telediensten erfolgen nach dem Teledienstedatenschutzgesetz (TDDSG), das auf § 38 BDSG verweist. Es ist hier kein Anlaß und kein Dateibezug nötig. Datenschutzprüfungen bei den sog. Zertifizierungsstellen nach dem Signaturgesetz erfolgen ebenfalls nach § 38 BDSG; auch hier ist kein Anlaß zur Prüfung nötig.

In Bremen ist der LfD auch zuständig für die Datenschutzkontrolle bei den **Mediendiensten**. Die Gegenstände der Prüfung und die Aufsichtsbefugnisse hier ergeben sich aus dem **Mediendienste-Staatsvertrag** (**MDStV)** und dem Ausführungsgesetz des Landes dazu vom 17.6.1997. Es sind ebenfalls kein Anlaß und kein Dateibezug erforderlich.

Ob im Zusammenhang mit der zunehmenden Rechnervernetzung und neuartigen IuK-Techniken **online-Datenschutzkontrollen**, d. h. evtl. auch ohne Mitwirkung der speichernden Stellen, möglich

werden, bleibt abzuwarten. Derartige Möglichkeiten setzen in jedem Fall aber entsprechende Technik und entsprechendes Know-how bei den Datenschutzaufsichtsbehörden voraus. **§** 38 Abs. 3 und 4 BDSG enthalten derzeit nur Betretens-, Auskunfts-, Einsichts- und Besichtigungsrechte sowie ein Auskunftsverweigerungsrecht. § 38 Abs. 5 BDSG enthält darüber hinaus Anordnungs- und Untersagungsbefugnisse bei Verstößen gegen § 9 BDSG. § 38 BDSG enthält jedoch **keine Verpflichtung**, den Aufsichtsbehörden technische Anschluß- oder Zugriffsmöglichkeiten zu gewähren; auch die EG-Datenschutzrichtlinie sieht derartiges nicht vor. **Online-Datenschutzkontrollen** - in der Fachliteratur als neuartige Methode für die externe Datenschutzkontrolle vorgeschlagen - sind nach derzeitiger sowie absehbarer Rechtslage nur im Zusammenwirken mit den speichernden Stellen möglich.

Im Bereich des **MDStV** ist nach dem Bremischen Ausführungsgesetz der Abruf von kostenpflichtigen Angeboten im Zusammenhang mit einer Datenschutzkontrolle, auch bei Angeboten für geschlossene Teilnehmergruppen, **kostenlos** zu ermöglichen. Daraus läßt sich neben der kostenlosen Prüfungsmöglichkeit eine Zugangsberechtigung zu geschlossenen Teilnehmergruppen entnehmen.

Diskutiert wird derzeit auch, **betriebsexterne** Prüfteams mit hoher fachspezifischer Kompetenz bei der Datenschutzkontrolle einzusetzen. Nach meiner Auffassung ist der Einsatz solcher Teams bei der Datenschutzkontrolle durch den betrieblichen Datenschutzbeauftragten wohl möglich; hier ist leichter die Zustimmung und Mitarbeit der speichernden Stelle zu erreichen und der Schutz der Betriebs- und Geschäftsgeheimnisse vertraglich abzusichern. Für die hoheitlich tätig werdenden **Datenschutzaufsichtsbehörden** ist der Einsatz derartiger Prüfgruppen im Rahmen ihrer Kontrolltätigkeit wegen ihrer Schweigepflicht, ihren

eingeschränkten Befugnisse und ihrem Selbstverständnis nur unter im einzelnen noch zu diskutierenden Voraussetzungen möglich.

19.3. Ergebnisse der Registerprüfungen

Ich habe im Berichtszeitraum bei insgesamt 16 nach § 32 BDSG meldepflichtigen Stellen einfache Registerprüfungen (aufgrund § 38 Abs. 2 BDSG) durchgeführt. Zusätzlich habe ich eine Anlaßprüfung nach § 38 Abs. 1 BDSG bei einem großen Unternehmen in Bremen durchgeführt, um festzustellen, ob eine Meldepflicht nach § 32 BDSG besteht.

Bei den **einfachen Registerprüfungen** überprüfe ich lediglich das Bestehen der Meldepflicht nach § 32 BDSG sowie die Richtigkeit der Meldung, die Bestellung und die Tätigkeit des betrieblichen Datenschutzbeauftragten nach den §§ 36/37 BDSG, die Verpflichtung der Mitarbeiter auf das Datengeheimnis gemäß § 5 BDSG und ggf. die Beachtung der für den Auftragnehmer geltenden Regelungen zur Auftragsdatenverarbeitung nach § 11 BDSG. Technisch-organisatorische Sicherungsmaßnahmen, die Umsetzung der datenschutzrechtlichen Betroffenenrechte sowie die Zulässigkeit der personenbezogenen Datenverarbeitung werden hierbei nicht geprüft; dies bleibt gesonderten Kontrollen vorbehalten. Dabei ist darauf hinzuweisen, dass die Zulässigkeit der personenbezogenen Datenverarbeitung, die bei den gemeldeten Auftragsdatenverarbeitern stattfindet, von den jeweiligen Auftraggebern datenschutzrechtlich zu verantworten ist und dass die anlaßbezogenen Einzelfallprüfungen nach § 38 Abs. 1 BDSG meist Zulässigkeitsfragen der Datenverarbeitung, gelegentlich auch die Betroffenenrechte, zum Gegenstand haben.

Bei meinen Registerprüfungen habe ich auch 1998 wieder Mängel feststellen müssen. Die **wesentlichen Mängel** lagen

wiederum im Bereich der Registermeldungen (z.B. Aktualität der Meldung, fehlende Abmeldung, fehlende Ergänzungsmeldung), beim betrieblichen Datenschutzbeauftragten (z.B. fehlende bzw. nicht formgerechte Bestellung, Bündelung mehrerer Funktionen, mangelnde Möglichkeiten zur Aus- und Fortbildung), bei den Verpflichtungen der Mitarbeiter auf das Datengeheimnis und bei der Beauftragung des Auftragnehmers bei der Auftragsdatenverarbeitung.

19.4. Bußgeldverfahren

Gegen eine private Abrechnungsgesellschaft habe ich ein Bußgeldverfahren wegen Verstoßes gegen die Meldepflicht nach § 32 BDSG eingeleitet. Gegen eine Wirtschafts- und Handelsauskunftei habe ich auf der Grundlage vom § 44 Abs. 1 Nr. 3 BDSG ein Bußgeld wegen unzureichender Benachrichtigung von Betroffenen verhängt.

20. Die Entschließungen der Datenschutzkonferenzen im Jahr 1998

20.1. Datenschutz beim digitalen Fernsehen

(Entschließung der 55.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20.März 1998)

Die Datenschutzbeauftragten des Bundes und der Länder machen darauf aufmerksam, dass bei elektronischen Diensten immer umfangreichere Datenspuren über das Verhalten der Einzelnen entstehen. Mit der Digitalisierung der Fernseh- und Hörfunkübertragung entsteht die technische Infrastruktur dafür, dass erstmals auch das individuelle Mediennutzungsverhalten registriert werden kann. Sie bekräftigen deshalb ihre Forderung, dass auch bei der Vermittlung und Abrechnung digitaler Fernsehsendungen eine flächendeckende Registrierung des individuellen Fernsehkonsums vermieden wird. Im digitalen Fernsehen ("Free

TV" und "Pay TV") muß die unbeobachtete Nutzung des Mediums ohne Nachteile möglich bleiben.

Die Datenschutzbeauftragten begrüßen es deshalb, dass die Staats- und Senatskanzleien Vorschläge für die Änderung des Rundfunkstaatsvertrags vorgelegt haben, mit denen Belangen des Datenschutzes Rechnung getragen werden soll. Besonders hervorzuheben sind folgende Punkte:

- Die Gestaltung technischer Einrichtungen muß sich an dem Ziel ausrichten, dass so wenige personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden;

- die Rundfunkveranstalter müssen die Nutzung und Bezahlung von Rundfunkangeboten anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist;

- personenbezogene Daten über die Inanspruchnahme einzelner Sendungen dürfen für Abrechnungszwecke nur gespeichert werden,

- wie bereits im Mediendienstestaatsvertrag enthält auch der Entwurf des Rundfunkstaatsvertrags eine Vorschrift zum Datenschutzaudit, d.h. Veranstalter können ihr Datenschutzkonzept und ihre technischen Einrichtungen von unabhängigen Gutachtern prüfen und das Prüfungsergebnis veröffentlichen lassen.

Die Datenschutzbeauftragten halten diese Grundsätze für geeignet, eine datenschutzgerechte Nutzung digitaler Fernsehangebote zu ermöglichen. Die technischen Möglichkeiten, diesen datenschutzrechtlichen Vorgaben zu entsprechen, sind gegeben. Die Datenschutzbeauftragten konnten sich bereits 1996 hiervon praktisch überzeugen. Die Systementscheidung von Veranstaltern für einen Decodertyp, der möglicherweise weniger geeignet ist, die

Datenschutzanforderungen zu erfüllen, kann kein Maßstab für die Angemessenheit dieser Anforderungen sein, wenn zugleich andere Geräte ihnen ohne Probleme genügen.

Der Forderung von Inhabern von Verwertungsrechten, einen Nachweis über die Inanspruchnahme von pay-per-view-Angeboten vorzulegen, kann ohne Personenbezug - etwa durch zertifizierte Zähleinrichtungen oder den Einsatz von Pseudonymen - entsprochen werden. Die Datenschutzbeauftragten bitten deshalb die Ministerpräsidentin und die Ministerpräsidenten der Länder, an den datenschutzrechtlichen Regelungen des Entwurfs festzuhalten. Damit würden das bisherige Datenschutzniveau für die Fernsehnutzung im digitalen Zeitalter abgesichert und zugleich die Vorschriften für den Bereich des Rundfunks und der Mediendienste harmonisiert.

Die Datenschutzbeauftragten fordern die Rundfunkveranstalter und Hersteller auf, den Datenschutz bei der Gestaltung von digitalen Angeboten schon jetzt zu berücksichtigen

20.2. Datenschutzprobleme der Geldkarte

(Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20.März 1998)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt ihre Forderung aus ihrer Entschließung vom 13.10.1995 nach einem anonymen elektronischen Zahlungsverfahren bei elektronischen Geldbörsen. Dies gilt insbesondere für die Geldkarte des deutschen Kreditwesens, bei der in kartenbezogenen "Schattenkonten" der Evidenzzentralen nicht nur der Kaufbetrag und ein identifizierbarer Händlerschlüssel, sondern auch der Kaufzeitpunkt gespeichert werden. Mit diesen Daten können sämtliche mit der Geldkarte getätigten Kaufvorgänge jahrelang nachvollzogen werden, wenn die Daten mit den persönlichen Kundendaten zusammengeführt

werden. Diese Geldkarte erfüllt nicht die Forderungen der Datenschutzbeauftragten.

Außerdem werden die Kundinnen und Kunden über diese "Schattenkonten" noch nicht einmal informiert. Die Herausgeber solcher Karten bzw. die Kreditinstitute haben aber die Pflicht, ihre Kundinnen und Kunden über Art und Umfang der im Hintergrund laufenden Verarbeitungsvorgänge zu informieren.

Unabhängig davon müssen bei der Geldkarte des deutschen Kreditwesens sämtliche Umsatzdaten in den Evidenzzentralen und auch bei den Händlern nach Abschluß der Verrechnung (Clearing) gelöscht oder zumindest anonymisiert werden.

Die Datenschutzbeauftragten fordern die Kartenherausgeber und die Kreditwirtschaft erneut dazu auf, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezogene Daten - sog. White Cards - anzubieten. Die Anwendung ist so zu gestalten, dass ein karten- und damit personenbezogenes Clearing nicht erfolgt.

Der Gesetzgeber bleibt aufgerufen sicherzustellen, dass auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher bei Bargeldzahlung anonym zu bleiben.

20.3. Fehlende bereichsspezifische Regelungen bei der Justiz

(Entschließung der 56.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Derzeit werden in allen Bereichen der Justiz – bei Staatsanwaltschaften, Gerichten und Gerichtsvollziehern – im Zuge von Modernisierungsvorhaben umfassende Systeme der automatisierten Datenverarbeitung eingeführt mit der Folge, dass sensible personenbezogene Daten auch hier in viel stärkerem

Maße verfügbar werden als bisher. Sogar die Beauftragung Privater mit der Verarbeitung sensibler Justizdaten wird erwogen. Gerade vor dem Hintergrund dieser vollkommen neuen Qualität der Datenverarbeitung in der Justiz wird deutlich, dass die Rechtsprechung des Bundesverfassungsgerichts zum sogenannten Übergangsbonus hier keine tragfähige Grundlage für Eingriffe in die informationelle Selbstbestimmung mehr darstellen kann. Vielmehr müssen die Entscheidungen des Gesetzgebers den Maßstab für die weitere technische Ausgestaltung der Datenverarbeitung innerhalb der Justiz bilden und nicht umgekehrt. Dabei ist nicht nur für formell ausreichende Rechtsgrundlagen Sorge zu tragen. Auch Fragen der Datensicherheit und der Ordnungsmäßigkeit der Datenverarbeitung bedürfen der Regelung.

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts sind 15 Jahre vergangen. Dennoch werden ausgerechnet im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen deshalb im Anschluß an ihren Beschluß der 48. Konferenz vom 26./27.09.1994 in Potsdam ihre wiederholten Forderungen zu bereichsspezifischen Regelungen bei der Justiz.

Zwar hat der Gesetzgeber in der abgelaufenen Legislaturperiode zumindest Regelungen über Datenerhebung, -verarbeitung und -nutzung im Strafvollzug sowie über die Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentlichen Stellen geschaffen.

Trotzdem sind in wichtigen Bereichen gesetzliche Regelungen weiterhin überfällig. Ausreichende gesetzliche Regelungen fehlen vor allem für

- weite Bereiche der Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien

  namentlich die

  - Übermittlung von Strafverfahrensdaten an nicht am Strafverfahren beteiligte dritte Stellen;

  - Rechte der Betroffenen (nicht nur der Beschuldigten, sondern auch von Zeugen und sonstigen Personen, deren Daten gespeichert werden) in Bezug auf Daten, die im Zusammenhang mit einem Strafverfahren gespeichert werden,

- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien;

- Datenübermittlung zu wissenschaftlichen Zwecken;

- Datenverarbeitung in der Zwangsvollstreckung;

- Datenverarbeitung im Jugendstrafvollzug;

- Datenverarbeitung im Vollzug der Untersuchungshaft.

Der Gesetzgeber sollte daher in der kommenden Legislaturperiode zügig die notwendigen Novellierungen, für die zum Teil ja schon erhebliche Vorarbeiten geleistet worden sind, aufgreifen. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und –verarbeitung in welchem Umfang

erforderlich ist. Ferner hat der Gesetzgeber jeweils bereichsspezifisch zu prüfen, inwieweit Aufgaben der Justiz und damit verbundene Datenverarbeitungen Privaten übertragen werden dürfen.

Der Entwurf für ein "StVÄG 1996" erfüllt diese Voraussetzungen nicht, im Gegenteil fällt er teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z.B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück. Zu kritisieren sind vor allem:

- Mangelnde Bestimmtheit der Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung
- Unangemessen weite Auskunfts- und Akteneinsichtsmöglichkeiten für nicht Verfahrensbeteiligte
- Unzureichende Regelungen über Inhalt, Ausmaß und Umfang von staatsanwaltlichen Dateien und Informationssystemen.

Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe unverzüglich in der neuen Legislaturperiode bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes der Bürgerinnen und Bürger entgegenwirken.

20.4. Weitergabe von Meldedaten an Adressbuchverlage und Parteien

(Entschließung der 56.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Bei den Datenschutzbeauftragten des Bundes und der Länder gehen viele Beschwerden ein, in denen deutlicher Unmut über

veröffentlichte Daten in Adressbüchern und unverlangt erhaltene Werbesendungen geäußert wird. Vor Wahlen nehmen die Beschwerden noch zu. Überrascht stellten Betroffene fest, dass sie persönlich adressierte Wahlwerbung der Parteien bekommmen. Ihnen ist unerklärlich, wie Adressbuchverlage und Parteien an ihre Adressen gekommen sind. Sie erhalten auf Anforderung Daten aus den kommunalen Melderegistern. Damit sind die Adressbuchverlage und Parteien gegenüber anderen gesellschaftlichen Gruppen privilegiert.

Dieser Umgang mit Meldedaten ist weder transparent noch angemessen. Die Konferenz tritt dafür ein, die Rechte der Bürgerinnen und Bürger zu verbessern. Die Information über die Widerspruchsmöglichkeit erreicht die Menschen häufig nicht. Vorzuziehen ist deshalb eine Einwilligungslösung. Sie würde das Grundrecht auf informationelle Selbstbestimmung konsequent umsetzen - erst fragen, dann handeln. Nach der Einwilligungslösung ist eine Erklärung informierter Bürgerinnen und Bürger gegenüber dem Meldeamt nötig, ob sie mit den Datenweitergaben an die genannten Empfänger einverstanden sind oder nicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt den gesetzgebenden Körperschaften, künftig die Einwilligungslösung vorzusehen.

20.5. Dringlichkeit der Datenschutzmodernisierung

(Entschließung der 56.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt und unterstützt grundsätzlich die vom 62. Deutschen Juristentag (DJT) im September 1998 in Bremen gefaßten Beschlüsse zum Umgang mit Informationen einschließlich personenbezogener Daten. Von den

gesetzgebenden Körperschaften erhofft sich die Konferenz die Berücksichtigung dieser Beschlüsse bei der nunmehr dringend erforderlichen Umsetzung der EG-Datenschutzrichtlinie in Bundes- und Landesrecht.

Insbesondere betont die Konferenz folgende Punkte:

- Die materiellen Anforderungen des Datenschutzrechts sind angesichts der wachsenden Datenmacht in privater Hand auf hohem Niveau grundsätzlich einheitlich für den öffentlichen wie für den privaten Bereich zu gestalten.

- Die anlaßfreie Aufsicht für die Einhaltung des Datenschutzes im privaten Bereich muß in gleicher Weise unabhängig und weisungsfrei ausgestaltet werden wie die Datenschutzkontrolle bei öffentlichen Stellen.

- Die Rechte der Bürgerinnen und Bürger sind zu stärken; als Voraussetzung für die Ausübung des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die Verpflichtungen zu ihrer Information, Aufklärung und ihren Wahlmöglichkeiten ohne faktische Zwänge auszuweiten.

- Ein modernisiertes Datenschutzrecht hat die Grundsätze der Datenvermeidung, des Datenschutzes durch Technik, der Zweckbindung der Daten und ihres Verwendungszusammenhangs in den Mittelpunkt zu stellen.

- Zur Sicherstellung vertraulicher und unverfälschter elektronischer Kommunikation ist die staatliche Förderung von Verschlüsselungsverfahren geboten, nicht eine Reglementierung der Kryptographie.

20.6. Entwicklungen im Sicherheitsbereich

(Entschließung der 56.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Sicherheitsbehörden in den vergangenen Jahren umfangreiche zusätzliche Eingriffsbefugnisse erhalten haben. Demgegenüber fehlen in weiten Teilen Erkenntnisse über die Wirksamkeit und Grundrechtsverträglichkeit der Anwendung dieser Instrumente, wie z.B. bei der Schleppnetzfahndung und der Ausweitung der Telefonüberwachung.

Die Datenschutzbeauftragten des Bundes und der Länder erwarten vom Bundesgesetzgeber und der Bundesregierung, dass die Erforderlichkeit und die Wirksamkeit aller Eingriffsbefugnisse anhand objektiver Kriterien überprüft werden (Evaluierung).

20.7. Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten

(Entschließung der 56.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, dass in der Praxis die Abgrenzung ihrer Zuständigkeiten bei den Gerichten immer wieder Anlaß von Unsicherheiten ist. Sie weisen daher darauf hin, dass die Beschränkung der Prüfkompetenz bei den Gerichten einzig und allein den Zweck hat, den grundgesetzlich besonders geschützten Bereich der richterlichen Unabhängigkeit von Kontrollen freizuhalten.

Deshalb erstreckt sich die Kontrolle der Datenschutzbeauftragten bei den Gerichten u.a. auch darauf, ob die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung getroffen und eingehalten werden, insbesondere bei automatisierter Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder halten eine gesetzliche Klarstellung für hilfreich, dass Gerichte

der Kontrolle des Bundesbeauftragten bzw. der Landesbeauftragten für den Datenschutz unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

20.8. Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge

(Entschließung der 56.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Die Datenschutzbeauftragten des Bundes und der Länder betonen das Recht der Bürgerinnen und Bürger auf Auskunft über ihre Daten auch gegenüber der Finanzverwaltung (§ 19 BDSG). Die Betroffenen haben Anspruch, von dem Bundesamt für Finanzen Auskunft über die Freistellungsaufträge zu erhalten, die sie ihrer Bank im Zusammenhang mit dem steuerlichen Abzug von Zinsen erteilt haben.

Der Bundesbeauftragte für den Datenschutz hat die Verweigerung der Auskünfte gegenüber dem Bundesministerium der Finanzen beanstandet und dieses aufgefordert, den entsprechenden Erlaß an das Bundesamt aufzuheben. Bisher hat das Ministerium in der Sache allerdings nicht eingelenkt.

Für die Betroffenen ergibt sich hierdurch ein unhaltbarer Zustand. Ihnen wird die Auskunft zu Unrecht vorenthalten.

Die Datenschutzbeauftragten der Länder unterstützen mit Nachdruck die Forderung des Bundesbeauftragten für den Datenschutz gegenüber dem Bundesministerium der Finanzen, seinen Erlaß an das Bundesamt für Finanzen aufzuheben und dieses anzuweisen, dem Auskunftsanspruch der Auftraggeber von Freistellungsaufträgen nachzukommen.

21. Index