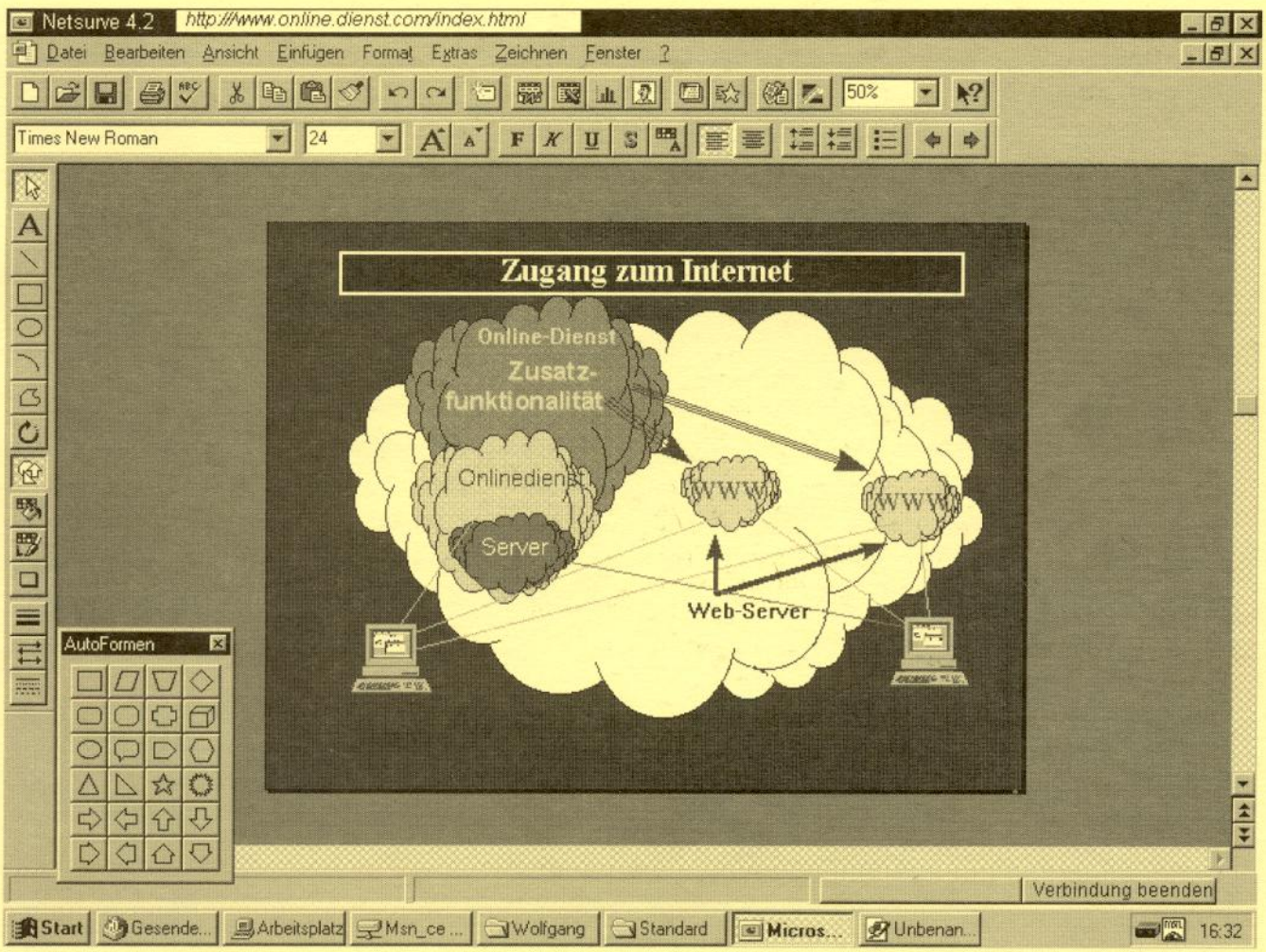
FREIE HANSESTADT BREMEN

Landesbeauftragter für den Datenschutz

18. Jahresbericht



Vorgelegt zum 31. März 1996

BREMISCHE BÜRGERSCHAFT
Landtag
14. Wahlperiode

Drucksache 14/272
18. 04. 96

18. Jahresbericht

des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats meinen 18. Bericht über das Ergebnis meiner Tätigkeit im Jahre 1995 zum 31. März 1996 (§ 33 Abs. 1 Bremisches Datenschutzgesetz - BrDSG)

Dr. Stefan Walz, Landesbeauftragter für den Datenschutz

Inhaltsübersicht

1 Vorwort

1.1 Zur Situation

1.1.1 Trends

„In Bayern soll bald jeder Bürger kostenlos Zugang zum weltweiten Informationsnetz INTERNET erhalten". Diese Ankündigung der bayerischen Staatskanzlei von Ende Februar 1996, die privaten Haushalte im Freistaat an die transnationale Datenautobahn anzuschließen, macht schlaglichtartig deutlich, wie nahe schon heute das Szenario der vernetzten Informationsgesellschaft ist und vor welchen dramatischen Veränderungen der Medienlandschaft und des Kommunikationsverhaltens der Bürger wir stehen.

Daher beginnt dieser Tätigkeitsbericht ganz bewußt mit einem Beitrag zu den Konsequenzen von **Multimedia** für den Datenschutz (vgl. Ziff. 2). Die rechtlichen Rahmenbedingungen für diese Neuordnung der Telekommunikation in Deutschland sollen abschließend in diesem Jahr (1996) festgelegt werden (zur Postreform III und zum Telekommunikationsgesetz vgl. Ziff. 6.2).

Rasche Fortschritte sind nicht nur im Bereich der Telekommunikation, sondern auch in anderen datenschutzrelevanten Technologien zur verzeichnen. Dies gilt - um nur ein Beispiel zu nennen - für die **Chipkarte.** Ihr Siegeszug scheint unaufhaltsam. Chipkarten werden in immer neuen Anwendungsfeldern eingesetzt: Die GeldKarte als elektronische Geldbörse des deutschen Bankensystems soll noch in diesem Jahr (1996) eingeführt werden (vgl. dazu den Beschluß der Datenschutzkonferenz, Ziff. 20.11). Fluggesellschaften wollen Chipkarten zur Erleichterung des Eincheck-Verfahrens und der Gepäckkontrolle nutzen. In einer Reihe von Kommunen finden diese maschinenlesbaren Karten Verwendung vor allem im öffentlichen Personennahverkehr. Die Deutsche Bahn AG will in Zusammenarbeit mit der Telekom und Nahverkehrsunternehmen die „PayCard" auf den Markt bringen, mit der gleichzeitig telefoniert und die Fahrkarte gekauft werden kann. Die Liste ließe sich fortsetzen.

Schwerpunkt in meinen Berichten der letzten drei Jahre war die Darstellung und datenschutzrechtliche Bewertung der Nutzung von **Chipkarten im Gesundheitswesen;** auch im vorliegenden Bericht finden sich aktuelle Ausführungen gerade zu diesem speziellen Anwendungsbereich (vgl. Ziff. 15.2.1).

1.1.2 Reaktionen

1.1.2.1 Gesetzgebung und Verfassungsgericht

Das Datenschutzrecht und die Datenschutzinstanzen stehen angesichts der Dynamik und Tragweite der informationstechnischen Entwicklungen vor dramatischen Herausforderungen. Die Reaktionen der **Gesetzgebung** fallen dabei durchaus unterschiedlich aus. So enthält der Entwurf für das Telekommunikationsgesetz, die rechtliche Basis für die Postreform III und damit die völlige Liberalisierung des Telekommunikationsmarktes (vgl. Ziff. 6.2), eine Datenschutzregelung, die bei aller Kritikwürdigkeit im Detail das Bemühen von Regierung und Parlamentsfraktionen erkennen läßt, einen ausgewogenen Ausgleich zwischen den Vertraulichkeitsinteressen von Verbrauchern bzw. Nutzern, den kommerziellen Erwartungen der Telekommunikationsunternehmen und den Kontrollwünschen der Sicherheitsbehörden herzustellen. Dem steht auf der Negativseite exemplarisch die Ankündigung der Bundesregierung gegenüber, in Kürze auch noch den größtmöglichen Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung, den sogenannten „Großen Lauschangriff", zu legalisieren.

In diesen Kontext, d. h. die Frage nach dem Verhältnis von privater Kommunikation und staatlicher Kontrolle, gehört auch die sog. **„Kryptokontroverse":** Sie wird in den nächsten Monaten eine der wichtigsten Debatten über das Verhältnis von Technikentwicklung und Datenschutz werden. Dabei geht es um die Frage, ob und inwieweit der Staat dem einzelnen Bürger im Interesse der Strafverfolgungsbehörden und der Nachrichtendienste verbieten kann, seine elektronischen Nachrichten zu verschlüsseln. Die Diskussion um die Einführung des „Clipper-Chip" in den USA zur Sicherung der staatlichen Abhörinteressen wird also in vergleichbarer Form auch in Europa intensiv geführt werden.

Wie wichtig die Rolle des **Bundesverfassungsgerichts** bei der Sicherung des Grundrechts auf informationelle Selbstbestimmung auch gegenüber den Entscheidungen großer Parlamentsmehrheiten ist, hat sich im Berichtsjahr erneut und beispielhaft gezeigt: Das höchste Gericht setzte mit einer einstweiligen Anordnung

eine insbesondere auch von Datenschutzbeauftragten kritisierte Regelung des Verbrechensbekämpfungsgesetzes 1994 vorläufig außer Kraft und schränkte damit die dem Bundesnachrichtendienst vom Gesetzgeber eingeräumten Befugnisse zur Weitergabe abgehörter Informationen an die Strafverfolgungsbehörden ein (vgl. Ziff. 6.6).

1.1.2.2 Erfolgreicher Bürgerprotest

Entscheidend wird es in Zukunft vor allem darauf ankommen, wie die Bürger auf datenschutzwidrige Zustände reagieren und inwieweit es kritischen Individuen und Gruppen gelingt, gesellschaftlichen Protest gegen Verletzungen des Rechts auf informationelle Selbstbestimmung zu mobilisieren. Daß **Bürgerprotest** durchschlagende Wirkung zeigen kann, hat der „Fall Bahncard" beispielhaft gezeigt. Der Widerstand der Kunden gegen die zwangsweise Koppelung der traditionellen Rabattkarte der Bundesbahn mit der Kreditkarte eines amerikanischen Unternehmens war so massiv, daß diese beiden Angebote wieder entkoppelt und Antragsformulare sowie Verarbeitungsverfahren grundlegend geändert werden mußten.

1.1.2.3 Zu schwache Aufsichtsbehörden

Wie wenig dagegen die Aufsichtsbehörden für den Datenschutz in der Privatwirtschaft dann tun können, wenn ein datenverarbeitendes Unternehmen die Zulässigkeitsnormen des Bundesdatenschutzgesetzes beharrlich und konsequent mißachtet, ist im Herbst und Winter 1995/1996 in einem bundesweit beachteten Fall deutlich vor Augen geführt worden. Entgegen dem ablehnenden Votum des zuständigen Innenministeriums Baden-Württemberg, das ich ebenso wie andere Aufsichtsbehörden unterstützt habe, hat eine Mannheimer Firma ein bundesweites Telefonverzeichnis auf einer CD-ROM mit unzulässigen Suchfunktionen hergestellt und verkauft. Erst nach dem Absatz von mehreren hunderttausend Stück stoppte eine einstweilige Gerichtsentscheidung den Vertrieb dieser Diskette (vgl. Ziff. 19.1).

Hier wirkt sich nachteilig aus, daß - anders als die Gewerbe- und Umweltämter - die Datenschutzaufsichtsbehörden nach dem BDSG nicht die Befugnis haben, rechtswidrige Verarbeitungsvorgänge zu untersagen. Die **Verbesserung der Kontrollinstrumente** der Datenschutzinstanzen gegenüber der Privatwirtschaft ist daher eine der zentralen Forderungen für die anstehende Novellierung des BDSG. Diese Reform des BDSG ist zwar in erster Linie veranlaßt durch das Inkrafttreten der Datenschutzrichtlinie der Europäischen Union. Die Anpassung an die europarechtlichen Vorgaben bietet jedoch die Chance für eine grundlegende Modernisierung des deutschen Datenschutzrechts und die Anpassung seiner Regelungen an aktuelle technische Entwicklungen. Die Vorbereitungen zu dieser Novellierung von seiten der Datenschutzbeauftragten sind bereits in vollem Gange (vgl. Ziff. 5.1).

1.2 Bremische Akzente

1.2.1 Rechtsentwicklung

Die 1995 nach intensiven Beratungen in Kraft getretene **Novellierung des Bremischen Datenschutzgesetzes (BrDSG)** markiert eine wichtige Etappe in der Weiterentwicklung des Datenschutzrechts in diesem Land. Daß man sich auf diesem Fortschritt nicht ausruhen kann, daß vielmehr in Bereichen mit sensibler Datenverarbeitung besondere gesetzliche Schutzvorkehrungen über das BrDSG hinaus erforderlich sind, gilt insbesondere für das Gesundheitswesen. Die derzeit in Vorbereitung befindlichen Gesetzentwürfe (vgl. Ziff. 7.2) werden die bereichsspezifische Landesgesetzgebung abrunden, die auch im Berichtsjahr wieder um einige wichtige Neuregelungen ergänzt worden ist (vgl. Ziff. 7.1.2 bis 7.1.8).

Der von der Bürgerschaft eingesetzte nichtständige Ausschuß zur Reform der **Landesverfassung** hat den Auftrag, u. a. über die Aufnahme eines Grundrechts auf informationelle Selbstbestimmung zu beraten. Die explizite grundrechtliche Fundierung des Datenschutzes würde sowohl dem Gesetzgeber eine bei allen Einzelvorhaben zu beachtende Leitlinie geben als auch die Rechtsstellung des Bürgers gegenüber den datenverarbeitenden öffentlichen Stellen „verfassungsfest" machen. Nach meinem Dafürhalten sollte Bremen dem Beispiel einer Reihe anderer Bundesländer folgen und den Datenschutz in der Verfassung verankern.

Allerdings können gesetzliche Verbote im Einzelfall auch massive Verletzungen des Persönlichkeitsrechts nicht verhindern, wenn es am **Datenschutzbewußtsein**

fehlt oder dienstliches vertrauliches Wissen sogar absichtlich und interessegeleitet offenbart bzw. den Medien zugespielt wird. Der Fall des Abgeordneten der Bürgerschaft, der sich tiefe Eingriffe in seine Privat- und Intimsphäre gefallen lassen mußte, sollte all denjenigen Anlaß zum Nachdenken über ihre rechtlichen Verpflichtungen sein, die über mit gutem Grund vertraulich zu behandelnde Informationen verfügen und sie gleichwohl weitergeben, offenbaren oder veröffentlichen. Konkrete Verantwortliche für die begangenen Datenschutzverstöße konnten allerdings - auch in den einschlägigen Beratungen des Datenschutzausschusses - nicht festgestellt werden.

1.2.2 Typische Konfliktlagen

1.2.2.1 Kostenkontrolle versus Klientenschutz

In der täglichen Beratungs- und Kontrolltätigkeit des Landesbeauftragten für den Datenschutz tauchen zwei typische Problemlagen immer wieder auf. Ein Konflikt, der vor allem im Sozial- und Gesundheitsbereich virulent wird, ist der zwischen detaillierter **Kostenkontrolle** einerseits und dem Schutz des **Beratungsgeheimnisses** und der Vertraulichkeit der Klientenbeziehung andererseits. Intensive Wirtschaftlichkeitsprüfungen zu Lasten der Privatsphäre der Bürger sind angesichts ständig knapper werdender Budgets eine ständige Versuchung (vgl. Ziff. 14.1 und Ziff. 8.2, dort zu 17. JB, Ziff. 12.3.7.). Bei entsprechender Bereitschaft der Ressorts lassen sich aber durchaus praktikable, die Interessen beider Seiten berücksichtigende Lösungen finden. Vorbildliches Beispiel dafür ist das Zusammenwirken des Sozial- und des Bildungssenators bei der Änderung des Antragsverfahrens zur Bezuschussung von Aufenthalten in Schullandheimen. Das neue Verfahren gewährleistet, daß Eltern nicht mehr dazu gezwungen sind, sich gegenüber der Leitung der Schule ihrer Kinder als Sozialhilfeempfänger zu „outen" (vgl. Ziff. 14.5)

1.2.2.2 TuI-Einführung ohne frühzeitige Unterrichtung des LfD

Das zweite Problem: Um die bremischen Dienststellen rechtzeitig und prophylaktisch bei der **Einführung technikunterstützter Informationsverarbeitung**, insbesondere bei der Vorbereitung des Einsatzes von Netzen, beraten zu können, ist die **frühzeitige Unterrichtung** des Landesbeauftragten für den Datenschutz unerläßlich. Die Vorschrift des § 27 Abs. 4 BrDSG, die diese rechtzeitige Information vorschreibt, gewinnt mit der Beschleunigung des Technikeinsatzes in der Verwaltung zusätzlich an Gewicht, wird zu meinem Bedauern jedoch vielfach zu wenig beachtet. Ich werde mich deshalb in Zukunft verstärkt bereits in der Phase der Aufstellung der TuI-Ressortpläne einschalten (vgl. Ziff. 8.2, dort zu 17. JB, Ziff. 5.1.1).

Der Informationsfluß über geplante datenschutzrelevante TuI-Ausstattungen und DV-Programme muß aber auch von seiten der Stadt Bremerhaven und der Dienststellen außerhalb der senatorischen Behörden verbessert werden. Daß die Kontaktaufnahme zum Datenschutzbeauftragten nur dann Fehlentwicklungen zu vermeiden hilft, wenn sie im **Vorfeld** der Installation und Nutzung von IuK-Technik in den Behörden stattfindet, wird plastisch unterstrichen durch die im Berichtsjahr eingetretene Situation, daß die Einführung eines neuen Programms durch einen marktführenden Hersteller (Windows '95) mangels Kompatibilität mit der bisher eingesetzten Datensicherungssoftware den in Bremen erreichten Schutzstandard zu gefährden drohte (vgl. Ziff. 9.1). Nur rechtzeitige Information erlaubt mir in diesen Fällen, System- bzw. Programmüberprüfungen selbst vorzunehmen und daraus - ggf. negative - Empfehlungen für die Anschaffungs- und Einsatzentscheidungen der Dienststellen zu formulieren.

1.2.2.3 Datenschutz als Führungsaufgabe

Beide geschilderten Problemkonstellationen machen deutlich, daß Datenschutz nicht nur als Bestandteil der täglichen Praxis auf der Mitarbeiterebene zu verstehen ist, sondern auch und vor allem als **Führungs- und Gestaltungsaufgabe**, die von Amts- und Abteilungsleitern wahrgenommen werden muß. Diese Leitungsverantwortung nimmt angesichts der zunehmenden dezentralen Organisations- und Budgetverantwortung an Bedeutung noch zu. Ich habe daher die SKP gebeten, ein entsprechendes Fortbildungsangebot in ihr Kursprogramm aufzunehmen und meine Bereitschaft erklärt, eine Veranstaltung für Leitungskräfte zu moderieren.

1.3 Redaktionelle Hinweise zum Bericht

Der 18. Jahresbericht enthält erstmals ein **Stichwortverzeichnis** (s. Ziff. 21), das den Lesern erleichtern soll, für sie interessante Textstellen aufzufinden. Zum

ersten Mal werden auch die **Gesetzesänderungen** und -vorhaben auf Bundes- und Landesebene nicht in den einzelnen ressortbezogenen Abschnitten, sondern im Zusammenhang dargestellt, um die Dynamik des Rechtsgebiets Datenschutz besser zu illustrieren (vgl. Ziff. 6 und 7). Bereits Tradition ist es, daß ein **Berichtsschwerpunkt** die Datenverarbeitung im **Gesundheitswesen** zum Gegenstand hat (vgl. den umfassenden Beitrag Ziff. 15).

Der wichtigen Rolle der präventiven Beratung der Behörden vor der Entscheidung über die Nutzung bestimmter Datenverarbeitungs- und Kommunikationstechnologien (s.o. Ziff. 1.2.2.2) entspricht die Aufnahme der **„Orientierungshilfe** zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das INTERNET" (vgl. Ziff. 9.2). Dieses von einem Arbeitskreis der deutschen Datenschutzkonferenz erarbeitete Papier soll zu einem Zeitpunkt, zu dem auch in Bremen noch relativ wenige Behörden einen Anschluß an dieses weltweite Kommunikationsnetz haben, auf die Schwachstellen der Datensicherung hinweisen und damit Kriterien für die Überlegungen über das Ob und Wie einer solchen Netzanbindung liefern.

Zum Schluß: Anregungen, Hinweise und Kritik zu Gestaltung und Inhalt dieses 18. Jahresberichtes werden gerne entgegengenommen!

2 Multimedia: Neue Herausforderung für den Datenschutz

2.1 Zukunftsthema gewinnt schärfere Konturen

In der zunehmend lebhaften öffentlichen Debatte über die Zukunft der Informationsgesellschaft ist **„Multimedia"** ohne Zweifel der Schlüsselbegriff, auch wenn im einzelnen mit diesem Terminus vielfach unterschiedliche Inhalte verbunden werden. Die Thematik war im Berichtszeitraum Gegenstand einer Vielzahl politischer bzw. gesetzgeberischer Initiativen, von parlamentarischen Anhörungen und fachlichen Diskursen.

So hat der **Deutsche Bundestag** im Oktober 1995 eine **Enquête-Kommission** eingesetzt, die sich mit der „Nutzung der neuen Möglichkeiten der Informations- und Kommunikationstechnik für Deutschland" beschäftigen soll. Dabei sollen auch u. a. die technischen und administrativen Voraussetzungen von Datensicherheit und Datenschutz ermittelt werden (vgl. Antrag der Fraktionen der CDU/CSU und FDP, BT-Drucks. 13/2753). Der **„Rat für Forschung, Technologie und Innovation"** beim Bundeskanzleramt, in dem u.a. Wirtschaftsvertreter und Wissenschaftler mehrerer Disziplinen mitgearbeitet haben, hat im Dezember 1995 seine Empfehlungen zur Ausgestaltung der Informationsgesellschaft vorgelegt. Abschnitt 2.5. befaßt sich eingehend mit den rechtlichen Rahmenbedingungen für den Datenschutz bzw. die Sicherheit in der Informationstechnik (vgl. jetzt den Bericht der Bundesregierung, „Info 2000 - Deutschlands Weg in die Informationsgesellschaft", BR-Drucks. 140/96, Kap. 1.4). Im Gesetzgebungsverfahren ist derzeit der Entwurf für ein neues **Telekommunikationsgesetz** (TKG), das die rechtlichen Grundlagen für die Neuordnung der Telekommunikationslandschaft nach der Aufhebung des Netz- und Sprachdienstmonopols der TELEKOM am 1. Januar 1998 legen soll. Geht es nach den Plänen der Bundesregierung, soll dieses Gesetz (Postreform III) bis zum Sommer 1996 verabschiedet sein. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat ihre Kernforderungen zu diesem Regelungsvorhaben in der am 10. November 1995 verabschiedeten Entschließung „Datenschutz bei der Neuordnung der Telekommunikation (Postreform III)" zusammengefaßt (der Text ist abgedr. u. Ziff. 20.15, vgl. auch den Beitrag u. Ziff. 6.2)

Im Wiesbadener Schloß fand am 9. Juni 1995 das gemeinsam vom Präsidenten des Hessischen Landtags und vom Hessischen Datenschutzbeauftragten organisierte 4. Forum Datenschutz statt, in dem es um Bestandsaufnahme und Perspektiven nach 25 Jahren Datenschutz in Deutschland ging. In der Bremischen Bürgerschaft hatte die Fraktion Bündnis 90/DIE GRÜNEN am 14./16. November 1995 zu einer öffentliche Anhörung zum Thema „Schöne neue Welt? - Auf dem Weg in die Informationsgesellschaft" eingeladen. Bei beiden Veranstaltungen hatte ich Gelegenheit, meine Überlegungen zur notwendigen Neudefinition der Rolle des Datenschutzrechts, der Datensicherungstechnik sowie des Datenschutzbeauftragten als Institution in der sich abzeichnenden Multimedia-Zukunft vorzutragen. Im folgenden werden sie in komprimierter Form wiedergegeben.

2.2 Multimedia - Systemwandel in der Medienlandschaft

In der weitestgehenden Multimedia-Vision ist der Bürger ein Mensch, der kaum noch unmittelbare zwischenmenschliche Kontakte im Arbeitsleben oder in der Freizeit hat. Von seinem heimischen Allround-Terminal, von seinem „integrierten Telefon-PC-TV" aus sieht er fern, telefoniert er, bestellt und kauft er elektronisch; per Bildschirm liest und kommuniziert er. Eine Vielzahl lebenswichtiger Dienstleistungen wird nur noch elektronisch interaktiv angeboten; nur mit einer häuslichen „Set-Top-Box" ist der Einzelne an die Datenautobahn angeschlossen. Also: **Interaktion wird reduziert auf Telekommunikation.**

Reicht unser heutiges Datenschutzrecht für dieses künftige Multimedia-Zeitalter noch aus ? Das zentrale Datenschutzproblem lautet: Die Anonymität des Barkaufs, des Fernsehkonsums, des Telefonierens und der häuslichen Datenverarbeitung entfällt, wenn jede Aktivität „über das Netz" eine **„Datenspur"** hinterläßt. Persönlichkeits- und Nutzungsprofile können hergestellt werden, der Einzelne wird „gläsern", wenn seine Interessen, Kaufwünsche, Vorlieben, Gesprächspartner usw. registriert und ggf. offengelegt werden.

Die wichtigsten technischen Grundlagen für „Multimedia" sind bereits heute gelegt. Dies zeigt vor allem der ebenso dynamische wie radikale **Wandel der Medienlandschaft.** Aus ursprünglich wenigen öffentlichen Sendern ist ein „duales Rundfunksystem" geworden mit Dutzenden von öffentlich-rechtlichen wie privaten Sendern aus dem In- und Ausland, die über Rückkanäle mögliche „interaktive" Sendungen wie Tele-Shopping oder pay-per-view anbieten wollen und in Bälde auch können. Aus dem Monopolbetrieb Bundespost ist ein buntscheckiges Telekommunikationssystem mit einer Vielzahl von Netzbetreibern und einer breiten Palette von Telediensten, z. B. von Mail-, Phone- und Voice-Boxen geworden. In der Datenverarbeitungslandschaft schließlich werden isolierte Terminals und Großrechnerverfahren zunehmend Vergangenheit. Computer und Telekommunikation sind mobil geworden (Laptops, Notebooks, Mobiltelefon etc.), Informations- und Kommunikationstechnik verschmelzen, Rechner werden unternehmensintern und national ebenso verknüpft wie international über globale Netze wie das INTERNET.

Die **Digitalisierung** der Informationsübertragung und der Vermittlungstechnik hebt die traditionellen Grenzen zwischen Massen- und Individualkommunikation, zwischen Computer und Telefon, aber auch zwischen Musik- und Sprachwiedergabe, auf. Die technischen Grundlagen für die Multimedia-Zukunft sind vorhanden. Deren Protagonisten leitet die Vision von der „Informationsgesellschaft" als globaler, kommerzialisierter und weitgehend privatisierter Informationsinfrastruktur.

Zu diesen Protagonisten gehört ganz maßgeblich die Brüsseler Kommission. Sie nutzt die infrastrukturelle Integrationsdynamik der Europäischen Gemeinschaft, die sich wiederum aus der Leitidee vom Binnenmarkt als Großraum nicht nur für Waren, Kapital und Dienstleistungen, sondern auch für Informationen speist. Diese Leitidee steht Pate für die europaweite Liberalisierung der Datenverarbeitungs- und Telekommunikationsmärkte, der Netze und Dienste, für die Aufhebung der nationalen Post- und Telefonmonopole. Zielsetzungen, die in Deutschland durch die sog. Postreformen und die mit ihnen zusammenhängende Gesetzgebung umgesetzt wurden (Postreformen I und II) bzw. werden (Postreform III, s. Ziff. 6.2.1).

2.3 Datenschutzrecht — Zeit für den Paradigmenwechsel

Dieser technische Systemwandel stellt die Frage nach dem notwendigen Paradigmenwechsel auch im Datenschutz, d. h. nach der Tragfähigkeit der traditionellen Konzeptionen von Rolle und Funktion des Datenschutzrechts:

1. Die Vorstellung aus der „Gründerzeit" des Datenschutzrechts zu Beginn der siebziger Jahre von einer Rechtsmaterie, die ausschließlich die Datenverarbeitung als einen klar definierbaren, von den Massenmedien und der Telekommunikation eindeutig unterscheidbaren Bereich regelt, ist in der Zukunft nicht mehr aufrecht zu erhalten. In einem unterschiedliche Technik- und Kommunikationsformen integrierenden Multimedia-Szenario wird die **traditionelle Abgrenzung von Rechtsgebieten,** die sich auf die jeweils eingesetzte Technik stützt, naturgemäß **unscharf.** So können z. B. — dies ist derzeit politisch sehr umstritten — interaktive Angebote der Fernsehanstalten unter Rundfunk-(recht) („rundfunkähnliche Dienste") oder unter individueller Telekommunikation (früher „Fernmelderecht") eingeordnet werden, mit gravierenden Unterschieden in den Rechtsfolgen.

2. Überholt ist eine Konzeption vom Datenschutzrecht, die sich darauf verläßt, eindeutig definierbare und in der Zahl überschaubare „datenverarbeitende" oder „speichernde Stellen" — gleich ob Behörden oder Unternehmen — als Normadressaten anzusprechen. Schon heute, erst recht aber in den künftigen Netzstrukturen, droht **„multizentrische Verantwortungslosigkeit":** Die Zahl der Datennutzer, aber auch der „Relaisstationen" nimmt exponentiell zu. Immer mehr personenbezogene Kommunikationsdaten werden an mehr Stellen registriert und ausgewertet. Die Verantwortung für die Zulässigkeit des Umgangs mit personenbezogenen Angaben verflüchtigt sich. Dementsprechend erschwert wird die externe Kontrolle durch Datenschutzbeauftragte und Aufsichtsbehörden.

3. Hinzu kommt: Untersuchungen wie das vom BMFT geförderte, von GRVI und VDI/VDE gemeinsam durchgeführte Diskurs-Projekt „Rechtliche Beherrschung der Informationstechnik" haben gezeigt, daß die Steuerungswirkung datenschutzrechtlicher Normen für die tatsächliche Nutzung vorhandener Informationen durch die „Anwender" in Wirtschaft und Verwaltung nur begrenzt ist. Erwartungen an lediglich rechtlich verordnete Zweckbindungsgebote oder Nutzungsbeschränkungen sind vielfach enttäuscht worden. Beispiel dafür ist der Versuch, unberechtigte Abrufe bei On-line-Anschlüssen durch rechtlich-organisatorische Vorkehrungen zu verhindern. Bisher zeigt sich eine **„Steuerungslücke"** vor allem im Verhältnis zwischen (Datenschutz-) Recht und (Informations- und Kommunikations-)Technik. Technisches Sicherheits- und Normungsrecht wie -praxis konstitutieren bzw. vollziehen sich teilweise losgelöst von Datenschutzforderungen. Dies heißt selbstverständlich nicht, auf gesetzliche Vorgaben völlig zu verzichten, sondern verlangt nach einem differenzierten Einsatz des rechtlichen Instrumentariums mit mehr prozeduralen Elementen (s. u.).

4. Inaktuell geworden ist schließlich die Vorstellung, Datenschutz sei in erster Linie auf der nationalen **Regelungsebene** zu verwirklichen. Für grenzüberschreitende Teledienste oder Netzbetreiber reicht kein einzelstaatlicher Regulierungsrahmen. Im Gegenteil: Wer im Alleingang für die „Datenautobahn" zu scharfe Verkehrsregeln aufstellt, muß mit der Flucht in sog. „Datenoasen" rechnen, in Länder also, in denen es weniger oder sogar keinen Datenschutz gibt.

Das Fazit lautet also: Die Technikentwicklung hin zur Multimediazukunft macht tragende Pfeiler des **traditionellen Datenschutzkonzepts brüchig.** Dies bedeutet jedoch nicht, daß auch die Zielsetzung des Datenschutzrechts, die Gewährleistung des Rechts auf informationelle Selbstbestimmung, in der Informationsgesellschaft an Bedeutung verliert. Im Gegenteil: Da im Zeitalter von „Multimedia" die technisch vermittelten Gefährdungen für das Individuum wachsen, wird ein wirksamer Datenschutz zum unverzichtbaren Instrument der **Grundrechtssicherung,** zur notwendigen Vorbedingung für den Schutz des Persönlichkeitsrechts und des Freiheitsraums des Einzelnen.

2.4 Ansätze für ein neues Datenschutzkonzept

Doch verfügt bisher niemand über ein geschlossenes neues Datenschutzkonzept, das die Risiken der dramatischen Technikveränderungen und der globalen Vernetzung umfassend aufzufangen vermag. Die folgenden Thesen verstehen sich als diskussionsbedürftige Teilelemente für ein verändertes Modell:

2.4.1 Datenschutz als „Querschnittsmaterie" — rechtliche Vorgaben

„Multimedia" verlangt auch dem Datenschutz juristische Multidisziplinarität ab. datenschutz muß konzipiert werden als Querschnittsmaterie des sich **neu entwickelnden Informations- und Medienrechts.** Dabei muß die Balance gefunden werden zwischen zu strenger Regulierung, die innovationsfeindlich und standortgefährdend wirken könnte, und zu schwacher Regulierung, die zur symbolischen (Rechts-)Politik entartet.

Ausgangspunkt und Meßlatte sollte dabei der Kernbestand der Datenschutzanforderungen bleiben, wie er schon Anfang der achtziger Jahre in der Diskussion um den Bildschirmtext-Staatsvertrag formuliert worden ist:

a) Vorrang hat zunächst das Prinzip der **Datenvermeidung:** Netzbetreiber und Diensteanbieter müssen verpflichtet werden, überall dort, wo anonyme Zugangs- und Nutzungsformen für On-line-Dienste technisch möglich sind, sie auch entsprechend anzubieten.

b) Wo Verbindungsdaten wie etwa im ISDN technisch zwangsläufig jedenfalls für kurze Zeit gespeichert werden müssen, gelten das **Verbot der Herstellung von Nutzerprofilen** sowie die Gebote der Zweckbindung und der umgehenden Löschung.

c) Der Kunde/die Kundin muß über die Nutzungsrisiken unsicherer Kommunikationsdienste (z. B. Mobilfunk) **umfassend aufgeklärt** werden.

Diese Regelungen sind derzeit noch allgemeiner deutscher Standard in den Rundfunkstaatsverträgen, Landesmediengesetzen sowie dem Telekommunikationsrecht des Bundes und finden sich — wenn auch bereits abgeschwächt — in dem Vorschlag der Europäischen Union für eine sog. ISDN-Richtlinie. Es werden aber erhebliche Anstrengungen nötig sein, dieses Niveau auf Dauer auch zu halten (vgl. unter Ziff. 6.2).

2.4.2 Neue Regelungsebenen und Regelungsformen

„Multimedia" verlangt weiter einen Mix von Regelungsebenen. Grenzüberschreitende Technikstrukturen und -anwendungen können nicht mehr (nur) im nationalen Regelungsrahmen, sondern müssen auf internationaler Ebene angegangen werden. Die **Europäische Union** z. B. setzt mit ihren **Richtlinien** in vielen Bereichen des Informationsrechts europaweite Vorgaben. Die „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten" ist im Juli 1995 verabschiedet worden (Amtsbl. der EG 1995, L 281, 31 ff.) und soll für einen harmonisierten Mindeststandard in allen Mitgliedstaaten sorgen (vgl. dazu Ziff. 5.1). Für den sog. „Offenen Netzzugang" verlangen die einschlägigen Richtlinien die Beachtung des Datenschutzes der Netzteilnehmer. Die Globalisierung der Netze erzwingt über die europäische Ebene hinaus auch die **Globalisierung von Standards und Regeln.** Die französische Regierung hat in diesem Kontext jüngst die Erarbeitung einer internationalen Konvention für das INTERNET entsprechend den Übereinkommen etwa im Seerecht vorgeschlagen.

Der Datenschutz muß seine **Lernfähigkeit** mitorganisieren. Innovation ist daher auch bei den Regelungsformen gefragt. Als Alternative zu dem in Deutschland vorherrschenden zwingenden Recht bietet sich die autonome Selbstregulierung der Beteiligten an. Dieser Ansatz läge auch im Trend der in vielen Industriestaaten festzustellenden verstärkten „Prozeduralisierung" von Recht. Die EU-Datenschutzrichtlinie (s. o.) hat hierzu holländische Erfahrungen mit Branchenvereinbarungen aufgegriffe, in denen sich Unternehmensverbände und Verbraucherschutzorganisationen gemeinsam über Datenschutzstandards etwa in den Bereichen Direktmarketing oder Marktforschung verständigen. Vielleicht entwickeln sich in Zukunft auch für die transnationalen Info-Bahnen überstaatliche Rechtskonstruktionen, wie sie sich für den weltweiten Handelsverkehr gebildet haben („lex mercatoria").

2.4.3 Datenschutztechnik und Risikobewußtsein

Die **„Allianz von Datenschutz und Technik"** (so der frühere hessische Datenschutzbeauftragte Simitis) ist möglich; Datenschutz durch Technik hat Zukunft. Wirksame **Verschlüsselungsprogramme** gibt es ebenso wie **anonyme Chipkarten.** Doch droht hier immer das Kostenargument als Einsatzsperre. Anders formuliert: Die Durchsetzung von Datensicherungsstandards „gegen den Markt" ist jedenfalls auf Dauer nicht möglich. Doch reicht es nicht, abstrakt auf die Verantwortung der Hersteller von IuK-Technik hinzuweisen und an sie zu appellieren, datenschutzfreundliche technische Optionen anzubieten. Druck in diese Richtung muß auch und gerade über den Markt ausgeübt werden. Besonders wirksam ist dabei der organisierte **Nachfragedruck** großer IuK-Kunden, etwa von Kreditinstituten, die sichere Übertragungswege für das „Telebanking" verlangen. Gleiches gilt für ein datenschutzbewußtes koordiniertes Anschaffungsverhalten großer Verwaltungen, etwa wenn Bundesministerien nur auf der Grundlage von Datenschutzstandards des Bundesamts für die Sicherheit in der Informationstechnik IuK-Bestellungen vornehmen.

Von entscheidender Bedeutung wird die **Risikoperzeption** technischer Systeme in der breiten Bevölkerung sein. Druck auf Hersteller, Netzbetreiber oder Diensteanbieter wird vor allem dann entfaltet, wenn Sicherheitslücken technischer Systeme bei den Bürgern zu Akzeptanzverlust führen. Wo über bestehende Gefährdungen **aufgeklärte Verbraucher** sich weigern, bestimmte Geräte oder On-line-Dienste ohne ausreichende Schutzvorkehrungen zu kaufen bzw. zu nutzen, drohen Absatzeinbußen. Diese Aufklärung wird aber nur möglich, wenn es

gelingt, für die Themen der Informationsgesellschaft eine **kritisch-mißtrauische Medienöffentlichkeit** herzustellen. Gebraucht werden dazu vor allem fachkundige Journalisten, die nicht den Versprechen oder Ankündigungen der Medienindustrie „auf den Leim gehen" und deren Pressemeldungen unkritisch publizieren, sondern die für die aus der Nutzung von Informations- und Kommunikationstechnologien resultierenden Gefährdungen (Beispiel Mobilfunk) sensibilisieren können und wollen.

Für eine Strategie zum Schutz des Persönlichkeitsrechts in der Informationsgesellschaft unverzichtbar ist nicht zuletzt eine kritische technische Intelligenz in Industrie und Wissenschaft. Gebraucht werden DV-Spezialisten bei Herstellern, Anwendern und in den Hochschulen, die über die Sozialverträglichkeit ihrer Tätigkeit ebenso wie über innovative datenschutzfreundliche Techniklösungen nachdenken und diese Erkenntnisse dann in die Aus- und Fortbildung einbringen.

2.4.4 Neues Rollenverständnis der Datenschutzbeauftragten

Konsequenzen sind auch für das Rollenverständnis der Datenschutzbeauftragten unvermeidlich: Sie haben, wenn sie sich als reine Kontrollbürokratie verstehen, keine Zukunft. Sie können und wollen nicht die Polizei auf der Datenautobahn spielen. Nur wenn sie sich als aktive Akteure im gesellschaftlich-politischen Raum bewegen, sich als Instanzen eines **medienpolitischen und -rechtlichen „Frühwarnsystems"** betätigen, als Ansprechpartner für kompetente Technikberatung fungieren, bei der **Technikfolgenabschätzung** mitwirken und als Gesprächspartner für Hersteller, Netzbetreiber und Diensteanbieter, aber auch für Interessenverbände (z. B. Verbraucherschutz) zur Verfügung stehen, können sie ihre Aufgabe, die effiziente Grundrechtssicherung in der künftig völlig veränderten Medienlandschaft, noch erfüllen.

2.5 Aktueller Handlungsbedarf

Die neue Herausforderung für den Datenschutz läßt sich jetzt klarer definieren: Die mit dem Schlagwort „Multimedia" zusammengefaßte Entwicklung bedeutet zwar das Ende für viele Elemente der traditionellen Konzeption von Datenschutzrecht. „Multimedia" bringt aber auch den starken Anstoß für einen Paradigmenwechsel und damit die Chance für eine moderne **Neukonzeption des Datenschutzrechts.** Gelegenheit dazu besteht jetzt, wenn in den kommenden drei Jahren das deutsche Datenschutzrecht ohnehin novelliert werden muß, um es an die Vorgaben der EU-Richtlinie anzupassen. Die Konferenz der Datenschutzbeauftragten wird ihre Vorstellungen für diese Reform auf ihren nächsten beiden Tagungen im März und im Oktober 1996 festlegen (vgl. dazu Ziff. 5.1).

3 Bürgerberatung, Medienkontakte, Fort- und Weiterbildung

3.1 Eingaben, Beschwerden und Hinweise

3.1.1 (Teil-) Bilanz in Zahlen

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 werden telefonische Anfragen und Hinweise ebensowenig zahlenmäßig registriert wie die vielen Einzelgespräche anläßlich von Tagungen oder Fortbildungsveranstaltungen. Gleiches gilt für die Bitten um Zusendung von Informationsmaterial. Erfaßt und nach Stichworten rubrizierbar sind lediglich die **schriftlichen Eingaben.** Zahl und Inhalt dieser Schreiben zeigen, worüber sich die Bürgerinnen und Bürger besonders ärgern, in welchem Bereich sie ihre Individualrechte einfordern und zu welchen Datenschutzthemen Informationsbedarf besteht. Es geht also nicht nur um Beschwerden oder Kritik; manchmal wird auch nur um eine Rechtsauskunft gebeten.

3.1.2 Öffentlicher Bereich (Verwaltung)

Im Berichtsjahr 1995 habe ich insgesamt 139 Eingaben erhalten. 87 davon betrafen Stellen der öffentlichen Verwaltung. Schwerpunktbereiche waren die Polizei (17), die Gerichte (10) - wobei der LfD gegenüber der Justiz nur über eingeschränkte Kontrollbefugnisse verfügt - sowie Gesundheitswesen bzw. Krankenhäuser (8). Die Finanzverwaltung und die Justizverwaltung stehen mit jeweils 3 Eingaben zu Buche.

Im folgenden zur Illustration einige wenige Stichworte zu den Themen:

Bei der **Polizei** wurde z. B. moniert

— Umfang der Speicherung bzw. nicht erfolgte Löschung,

— Datenabrufe aus dem polizeilichen Informationssystem zu privaten Zwecken,

— abgelehnte Auskunftsanträge,

— erkennungsdienstliche Behandlung,

— mehrere Verhöre im gleichen Raum,

— Aufbewahrung von Video-Filmen bei Verwarnungen.

Die Kritik des Datenumgangs im öffentlichen Gesundheitswesen und in den Krankenhäusern bezog sich u. a. auf

— Aufbewahrung von Patientenakten,

— Einsicht in Akten des Gesundheitsamts,

— Datensatz auf dem Einklebezettel im Mutterpaß,

— Datenweitergabe an externe Dritte,

— Datenverarbeitung beim Sozialpsychiatrischen Dienst.

3.1.3 Privatwirtschaft

52 Anschreiben hatten Datenschutzfragen in privaten Unternehmen zum Gegenstand. „Spitzenreiter" waren hier die **Auskunfteien** (13), **Arztpraxen** (8) und **Kreditinstitute** (5). Einige Fälle aus dem Bereich der Banken und Sparkassen sind im Abschnitt 19.2 ausführlicher wiedergegeben. Bei den Ärzten kommt es immer wieder zu berechtigten Beschwerden über die Entsorgung von Patientenunterlagen, etwa wenn diese achtlos in allgemein zugängliche Mülleimer geworfen werden. Zu Recht gerügt wird auch, wenn behandelnde Mediziner dem Patienten Schwierigkeiten bei der Wahrnehmung des ihm zustehenden Einsichtsrechts in seine Krankenakte machen.

3.2 Aus- und Fortbildung, Vortrags- und Lehrtätigkeit

3.2.1 Ein Schwerpunkt: Bildung und Forschung an Schulen

Im Berichtsjahr habe ich mich verstärkt bemüht, über Datenschutzfragen bei der Durchführung von Forschungsprojekten und von Datenerhebungen, Untersuchungen und **Forschungsvorhaben an Schulen** zu informieren. Zu beiden Themenkomplexen habe ich Merkblätter entwickelt, die ich bereits im letzten Tätigkeitsbericht (vgl. 17. JB; Ziff. 11.2, 11.3) vorgestellt habe. Mit der besonderen Fortbildungstätigkeit für Forscher (z. B. des Sonderforschungsbereiches 186 der Universität Bremen) und Lehrer (z. B. im Zusammenhang mit der Schulbegleitforschung) verbinde ich die Erwartung, daß die Datenschutzregelungen für diese Bereiche nicht nur eine größere Beachtung und weitere Verbreitung, sondern auch größere Akzeptanz finden. Gerade in den Themenfeldern Forschung und Schule stoßen verschiedene Grundrechtspositionen zusammen, die in ein befriedigendes Verhältnis gebracht werden müssen. Ich habe vor, diese Kontakte fortzuführen.

3.2.2 Weitere Aktivitäten im Überblick

Neben dem traditionellen viertägigen Grundseminar zum Bremischen Datenschutzgesetz im Aus- und Fortbildungszentrum (AFZ) der SKP haben meine Mitarbeiter Lehr- bzw. Fortbildungsveranstaltungen abgehalten u. a.

— an der Hochschule Bremen/Fachbereich Sozialwesen (Datenschutz im Jugendamt),

— an der Hochschule Bremerhaven/Fachbereich Systemanalyse (Datenschutz und Datensicherung I und II),

— bei der Bremischen Evangelischen Kirche (Fortbildung für Erzieherinnen),

— an der Datenschutzakademie Schleswig-Holstein (Sozialgeheimnis) und

— an der Schule für Verfassungsschutz (Referat: Datenschutz und Verfassungsschutz).

Weitere **Referate** von mir und meinen Mitarbeitern auf Foren, Kolloquien und Podiumsveranstaltungen hatten u. a. die folgenden Themen zum Gegenstand:

— Multimedia: Ende des Datenschutzrechts ? (vgl. dazu den Beitrag Ziff. 2),

— Datenschutz in der sich entwickelnden Informationsgesellschaft - Vom Schutz gegen Mißbrauch personenbezogener Daten über das informationelle Selbstbestimmungsrecht zur Datenverkehrsordnung?

— Informationelle Selbstbestimmung, Sicherheit und Datenschutz: Was ist nötig, was ist machbar?

— Datenverschlüsselung: Gefährdung staatlicher Hoheit oder Sicherung der Privatheit

Diese Auflistung zeigt anschaulich die Spannbreite des die Öffentlichkeit interessierenden Themenspektrums. Das Engagement im Bereich Fortbildung und Vortragstätigkeit steht allerdings unter dem Vorbehalt der beschränkten Kapazitäten; zu meinem Bedauern muß ich immer wieder Anfragen zu Veranstaltungen und Referaten ablehnen.

3.3 Presse- und Öffentlichkeitsarbeit

3.3.1 Medienkontakte und Pressemitteilungen

Die Darstellung meiner Presse- und Rundfunkkontakte im Jahresbericht hat eine doppelte Funktion: Zum einen soll deutlich gemacht werden, wie wichtig die Unterstützung einer **kritischen Medienöffentlichkeit** für die Schaffung von Problembewußtsein in Politik, Verwaltung und Wirtschaft für die Belange des Datenschutzes ist (vgl. auch o. Ziff. 2.4.3). Zum anderen geben die von den Medien aufgegriffenen aktuellen Themen einen guten Überblick über die gerade aus der Sicht des Bürgers und damit des „Objekts" behördlicher oder geschäftlicher Datenverarbeitung besonders relevanten Fälle und Konflikte.

1995 hatte ich den Vorsitz der Konferenz der Datenschutzbeauftragten des Bundes und der Länder inne. Wichtige Aufgabe des Vorsitzenden ist die Vermittlung der Konferenzergebnisse an Medien und Öffentlichkeit. Nach der März-Sitzung in Bremen fand daher ebenso wie nach der November-Konferenz in Bremerhaven jeweils eine Zusammenkunft der **Landespressekonferenz** statt, auf denen ich die verabschiedeten Entschließungen vorgestellt habe (zu den Beratungsergebnissen ausführl. Ziff. 4). Beide Treffen der Datenschutzbeauftragten hatten ein breites überregionales Medienecho.

Presseerklärungen habe ich - abgesehen von den Konferenzzusammenfassungen - u. a. zu folgenden aktuellen Themen abgegeben:

11. 05. 95: „Gläserner Mieter": Verstoß gegen den Datenschutz - Mißbrauch der **Schufa-Selbstauskunft durch Vermieter** (vgl. dazu 17. JB, Ziff. 17.3);

26. 05. 95: Mehr Rechte für den Bürger - **Neues Datenschutzgesetz** tritt in Kraft (vgl. zum Inkrafttreten des novellierten Bremischen Datenschutzgesetzes in diesem Bericht Ziff. 7.1.1),

06. 07. 95: Unzulässige Volksbefragung durch die neuen **Bahncard**-Anträge - Sofortige Änderung der Formulare und Löschung der unzulässig erhobenen Daten notwendig (zusammen mit den Datenschutzbeauftragten von Hamburg und Niedersachsen; vgl. dazu in diesem Bericht Ziff. 1.1.2.2).

Meine Stellungnahmen und Interviews auf Anfrage von Journalisten betrafen im Berichtsjahr u. a. die **überregionalen** Themen

— Datenschutz bei unternehmenseigenen Netzen (sog. "corporate networks");

— Erweiterung der Telefonkontrolle im Entwurf des Bundesrates für ein Korruptionsbekämpfungsgesetz;

— „Komfort-Auskunft" der TELEKOM;

— „elektronische Geldbörse";

und die lokalen Themen

— Überprüfung von Vermietern von Wohnungen an Sozialhilfeempfänger und Flüchtlinge (dazu u. Ziff. 14.2),

— Frage nach dem Arbeitgeber des Ehepartners beim Ortszuschlag (dazu u. Ziff. 10.3).

3.3.2 Arbeitshilfen und Broschüren

Zusammen mit zahlreichen Verbraucherzentralen, der Arbeitsgemeinschaft der Verbraucherverbände (AgV), mehreren Patientenstellen und -initiativen sowie meinen Datenschutzkollegen in Hamburg, Niedersachsen, Saarland, Sachsen und Schleswig-Holstein habe ich im Dezember 1995 das **Faltblatt „Die Gesundheits-Chipkarte: Alles auf eine Karte setzen"** herausgegeben. Es soll den Bürgerinnen und Bürgern Hilfe leisten bei der Entscheidung über die Teilnahme an den immer zahlreicheren Kartenprojekten im Gesundheitswesen (ausführlich zu den Datenschutzproblemen bei den Patientenchipkarten 16. JB, Ziff. 8.3.1.; 17. JB. Ziff. 13.1.4; s. a. in diesem Bericht Ziff. 15.1.1). Das Faltblatt enthält darüber hinaus Hinweise auf weiterführende Literatur und die Anschriften der Stellen, bei denen es bestellt werden kann bzw. zusätzliche Auskünfte eingeholt werden können. Selbstverständlich kann dieses Informationsblatt auch bei meiner Dienststelle kostenlos angefordert werden.

Zu den **„Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das INTERNET"** - ein solcher Anschluß wird auch außerhalb von Universitäten und sonstigen Wissenschaftseinrichtungen von mehr und mehr Behörden gewünscht - hat der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten eine Orientierungshilfe erstellt. Ihr Inhalt ist auszugsweise in diesem Bericht unter Ziff. 9.2 abgedruckt; der vollständige Text kann als separates Papier bei mir angefordert werden.

4 49. und 50. Datenschutzkonferenz in Bremen - die wichtigsten Ergebnisse

4.1 Bremischer Vorsitz im Jahr 1995

Die Datenschutzbeauftragten des Bundes und der Länder treffen sich in der Regel zweimal jährlich zu ihren Konferenzen, um gemeinsame Stellungnahmen vor allem zu aktuellen Gesetzgebungsvorhaben zu verabschieden und Kontrollerfahrungen auszutauschen. Der Vorsitz wechselt jährlich in alphabetischer Reihenfolge. Die beiden Konferenzen des Jahres 1995 fanden unter bremischem Vorsitz statt; die März-Sitzung in Bremen, die Zusammenkunft im November in Bremerhaven. Der Senat, die Handelskammer Bremen, der Magistrat der Stadt Bremerhaven und das Morgenstern-Museum in Bremerhaven haben die Durchführung dieser beiden Konferenzen maßgeblich unterstützt und ermöglicht.

4.2 49. Datenschutzkonferenz am 9./10. März in Bremen

Die 49. Konferenz sprach sich zunächst nachdrücklich gegen die Aufhebung des Verbots der **Rundfunkberichterstattung aus Gerichtsverhandlungen** aus. Auch die Einwilligung der Prozeßbeteiligten könne Verletzungen des Persönlichkeitsrechts nicht ausschließen; in medienwirksamen Strafprozessen bestehe die Gefahr, daß Angeklagten oder Zeugen ihre Einwilligung abgekauft werde (vgl. den Wortlaut des Beschlusses u. Ziff. 20.5).

Gewarnt wurde weiter vor einer unkritischen Euphorie für **„Multimedia"** und die „Datenautobahn"; die Persönlichkeitsrechte der Millionen von Nutzern dürften dabei nicht kommerziellen Interessen geopfert werden. Für die neuen interaktiven Dienste wie Teleshopping oder Pay-TV müßten anonyme Zugriffs- und Zahlverfahren wie etwa die vorausbezahlte Karte angeboten werden. Wenn aber der Kunde aufgrund der eingesetzten Technik unvermeidlich eine „Datenspur" hinterlasse, müsse durch bundesweit einheitliche Regelungen die Herstellung von Benutzerprofilen untersagt werden (Beschluß u. Ziff. 20.5).

Zu dem **BKA-Gesetzentwurf** der Bundesregierung verlangte die Konferenz einschneidende Änderungen: Die Verantwortung der Länderpolizeien für „ihre" Daten dürfe ebensowenig wie die Kontrollbefugnisse der Datenschutzbeauftragten der Länder durch eine Zentralisierung der Informationsverarbeitung beim Bundeskriminalamt unterlaufen werden. Die verdeckte Datenerhebung aus Wohnungen müsse so eindeutig auf den Schutz gefährdeter Ermittler beschränkt werden, daß nicht der „große Lauschangriff" durch die Hintertür eingeführt werde (Beschluß u. Ziff. 20.1).

Neben der Beratung von Vorhaben der aktuellen Gesetzgebung und der Technikentwicklung wurden weitere Themen behandelt:

- bei der Entwicklung von **Verkehrslenkungs- und Mautsystemen** die Sicherung der „datenfreien Fahrt" statt detaillierter Registrierung mit dem Risiko der Herstellung von Bewegungsprofilen (vgl. u. Ziff. 20.4),
- gefordert wurde eine aussagefähige Statistik bei den Berichtspflichten der Staatsanwaltschaften im Zusammenhang mit der Telefonüberwachung,

— die Einschränkung der **Sicherheitsüberprüfungen** von Mitarbeitern in sicherheitsempfindlichen Betrieben („personeller Sabotageschutz", vgl. u. Ziff. 20.2),

— die Sicherung des Wahlgeheimnisses bei der **Wahlstatistik** durch Bildung ausreichend großer Stimmbezirke und den Schutz von „Geheimadressen" bei der Auslegung des Wählerverzeichnisses (vgl. u. Ziff. 20.9) und

— mehr Information für den Betroffenen in Verfahren der **Berufsgenossenschaften**, z. B. über die beauftragten Gutachter (vgl. u. Ziff. 20.6).

4.3 50. Datenschutzkonferenz am 9./10. November in Bremerhaven

Die Entschließung zu der voraussichtlich bereits 1996 in Kraft tretenden **Postreform III** betont die Tatsache, daß das von der Bundesregierung vorbereitete Telekommunikationsgesetz (vgl. dazu den Beitrag Ziff. 6.2) die Rechtsgrundlage bilden wird für den endgültigen Eintritt Deutschlands in das Zeitalter weltweiter Vernetzung, von Multimedia und On-line-Diensten. Mit dem Konsum von Angeboten der Telekommunikation und des interaktiven Rundfunks würden auch die „Datenspuren", die der Bürger hinterläßt, stark zunehmen. Die Datenschutzbeauftragten betonten daher das Prinzip der Datenvermeidung bzw. -reduzierung bei der Ausgestaltung der neuen Dienste. Netzbetreiber und Diensteanbieter sollen verpflichtet werden, anonyme Zugangs- und Nutzungsformen und wirksame Verschlüsselungsverfahren bereitzustellen. Die Kunden seien über die Risiken unsicherer Kommunikationstechniken (z. B. Mobilfunk) umfassend aufzuklären. Die Datenschutzkontrolle dürfe wegen der möglichen Interessenkonflikte nicht wie vom Bundespostminister geplant der vorgesehenen Regulierungsbehörde zugewiesen werden (vgl. u. Ziff. 20.15).

Die Konferenz plädierte anläßlich der bevorstehenden Überarbeitung der **Gemeinschaftsverträge** für die Aufnahme eines Grundrechts auf Datenschutz in einen gemeinschaftsweit verbindlichen Grundrechtskatalog. Damit würde für die Bürgerinnen und Bürgern verdeutlicht, daß der Schutz ihrer Privatsphäre auch in einem Europa mit transeuropäischen elektronischen Datennetzen und zunehmendem grenzüberschreitenden Informationsaustausch gesichert bleiben soll. Die Datenschutzbeauftragten fordern weiterhin die vertragliche Verankerung eines unabhängigen EU-Datenschutzbeauftragten für die Datenbanken der zahlreichen Behörden der Gemeinschaft (vgl. u. Ziff. 20.13).

Die Konferenz stellte angesichts der Zunahme von Modellversuchen und Pilotprojekten zur Einführung von Patientenchipkarten mit medizinischen Daten eine Reihe von Anforderungen an einen datenschutzgerechten Einsatz auf: Der Patient müsse die freie Entscheidung darüber behalten, ob er überhaupt eine **Gesundheits-Chipkarte** benutzt, welche Daten auf ihr gespeichert werden und ob er die Karte beim Arztbesuch vorlegt oder nicht. Die auf der Karte gespeicherten Angaben müßten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt werden wie die vom Arzt aufgezeichneten Daten. Die Karten dürften nicht dazu dienen, neue zentrale medizinische Datenbanken bei Krankenkassen oder Kartenherstellern einzurichten (vgl. u. Ziff. 20.14, s. auch den Beitrag Ziff. 15.2.1).

In ihrem Beschluß zur Telefonüberwachung verlangten die Datenschutzbeauftragten erneut eine wirksame Erfolgskontrolle von Ermittlungsmaßnahmen, die erheblich in die Grundrechte des Bürgers eingreifen. Sie fordern daher die Justizministerkonferenz auf, die vorgesehene **Abhörstatistik** aussagekräftig und detailliert zu führen. Nur mit eindeutigen Erkenntnissen über die tatsächliche Praxis und ihre Erfolge könne der Gesetzgeber verantwortlich über Erweiterungen der Telefonüberwachung, wie sie z.B. im Gesetzentwurf des Bundesrates für ein Korruptionsbekämpfungsgesetz enthalten sind, entscheiden (vgl. u. Ziff. 20.15). Den Datenschutzausschuß der Bremischen Bürgerschaft habe ich jeweils über die Beratungsergebnisse der Datenschutzkonferenz unterrichtet.

5 Europa

5.1 Datenschutzrichtlinie der Europäischen Union in Kraft

5.1.1 Anpassung erfordert Novellierung

Die Datenschutzrichtlinie der Europäischen Union ist, fünf Jahre nach Vorlage des Erstentwurfs, im Oktober 1995 endlich in Kraft getreten und im Amtsblatt der EG veröffentlicht worden (L 281, 31 ff.). Zwischen der Verabschiedung des sogenannten „Gemeinsamen Standpunkts" am 20.02.1995 (vgl. 17. JB, Ziffer 6.1) bis zur endgültigen Annahme des Textes im EU-Ministerrat am 24.07.1995 gab es

noch einzelne kleinere Korrekturen im Wortlaut und in den Erwägungsgründen aufgrund von Änderungswünschen aus der 2. Lesung im Europäischen Parlament am 15.06.1995. Von Bedeutung ist allerdings die in der Schlußversion enthaltene Änderung betr. die Durchführungsbefugnisse der EU-Kommission.

Die **Frist** für die Mitgliedstaaten zur Anpassung ihres einzelstaatlichen Datenschutzrechts an die Richtlinie beträgt drei Jahre. Diese Zeit bis zum Herbst 1998 muß intensiv genutzt und mit den Vorarbeiten muß umgehend begonnen werden, wenn man bedenkt, daß die letzte Reform des Bundesdatenschutzgesetzes mehr als vier Jahre gedauert hat.

Hinzu kommt, daß ja nicht nur das Bundesrecht, sondern auch die Landesdatenschutzgesetze mit den Vorgaben der EG in Einklang zu bringen sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat aus diesem Zeitdruck die Konsequenzen gezogen und beschlossen, **Eckpunkte** für die Änderung des BDSG schon auf ihrer 51. Konferenz im März 1996 vorzulegen. Zu den vorrangigen Forderungen gehört dabei vor allem, die Anknüpfung an den überholten Begriff der „Datei" aufzugeben und die Restriktionen für die Datenschutzkontrolle im nicht-öffentlichen Bereich wegfallen zu lassen. Neu definiert werden muß auch die Rechtsstellung des betrieblichen Datenschutzbeauftragten.

5.1.2 Chance für die Modernisierung des Datenschutzrechts

Den deutschen Datenschutzbeauftragten geht es dabei um mehr als durch Gemeinschaftsrecht erzwungene Minimalkorrekturen, um mehr als den buchhalterischen Abgleich zwischen den deutschen Gesetzestexten und den europäischen Formulierungen. Eine BDSG-Novellierung, die in zwei oder drei Jahren in Kraft tritt, kann die rapide Veränderung der Informations- und Kommunikationstechnik, kann die seit Inkrafttreten des zweiten BDSG vor fünf Jahren deutlich gewordenen Regelungsdefizite nicht außer acht lassen.

Anders ausgedrückt: Das Gebot der Anpassung der deutschen Rechtslage an die EU-Richtlinie muß als Chance wahrgenommen werden, das Datenschutzrecht in unserem Land von veralteten Konzepten zu entrümpeln und Regelungserfordernissen der von „Multimedia" geprägten Zukunft gerecht zu werden. Nur mit dieser doppelten Zielsetzung, d. h. **Anpassung „an Europa"** und **Modernisierung in Richtung auf die Informationsgesellschaft**, kann das Datenschutzrecht auch am Ende dieses Jahrzehnts seine Schutzrolle für das informationelle Selbstbestimmungsrecht der Bürger erfüllen (vgl. dazu ausführl. den Beitrag Ziff. 2).

5.1.3 Weiterentwicklung des Datenschutzes auf Gemeinschaftsebene

Die verabschiedete Richtlinie stellt jedoch nur einen Zwischenschritt dar. Für eine konsequente Weiterentwicklung des Schutzes von Individualität und Privatsphäre in der Europäischen Union bedarf es weiterer Maßnahmen:

- Das Recht auf Achtung der Privatsphäre, im deutschen Verständnis das Recht auf informationelle Selbstbestimmung, gehört in einem Europa, das grenzüberschreitende Datenflüsse multipliziert und transeuropäische Datennetze aufbaut, in den Grundrechtskatalog einer geschriebenen EU-Verfassung.
- Die Institutionen und Organe der EG, die zunehmend in ihren eigenen Computern persönliche Daten der Gemeinschaftsbürger sammeln und auswerten (z.B. in den Bereichen Statistik, Fonds-Verwaltung und Bekämpfung des Subventionsbetrugs), müssen sich selbst dem Datenschutz-Regime unterwerfen, das die Richtlinie für die Behörden und Unternehmen in den Mitgliedstaaten vorschreibt.
- Gleiches gilt für die Kontrolle: Die Regelungen für die Brüsseler und Luxemburger Behörden müssen von einem in den Gemeinschaftsverträgen abgesicherten, unabhängigen Datenschutzbeauftragten kontrolliert werden.

Diese drei **Kernforderungen** hat die Europäische Datenschutzkonferenz im September 1995 auf Vorschlag der deutschen Delegation beschlossen. Die deutsche Datenschutzkonferenz hat diese Petita in ihrer Entschließung im November 1995 in Bremerhaven bekräftigt (s.o. Ziff. 4.3; Text der Entschließung u. Ziff. 20.13).

Die **Reaktionen aus Brüssel** zu diesen letzten beiden, seit langem bekannten Forderungen waren bisher mehr als zögerlich. Weder beim behördeninternen Datenschutz noch bei der Bestellung eines Beauftragten sind bisher nennenswerte Fortschritte erzielt worden. Die EU-Organe müssen sich allerdings darüber klar sein,

daß „hausinterne" Organisationsregelungen zum Datenschutz nicht mehr ausreichen. Vielmehr kann die Übermittlung personenbezogener Daten von nationalen Behörden an die Dienststellen der Gemeinschaft für den Fall, daß keine speziellen europarechtlichen Rechtsgrundlagen die Weitergabe vorschreiben, gefährdet sein, wenn diese nicht über einen den Mitgliedstaaten äquivalenten Datenschutz-Standard verfügen. Nur ein solcher einzelstaatlicher Druck auf Brüssel war es auch, der seinerzeit zur Verabschiedung der EG-Statistik-Verordnung geführt hat, die das Statistikgeheimnis auch beim Europäischen Amt in Luxemburg sichert.

5.1.4 Konzertation durch Datenschutzgruppe

Die Richtlinie setzt in Art. 29 eine Arbeitsgruppe ein. Sie wird u. a. die **Umsetzung** in das einzelstaatliche Recht begleiten und sich bei Zweifelsfragen der **Interpretation** einschalten. Darüber hinaus hat die Kommission alle Regelungsprojekte der EU mit Datenschutzbezug dieser Gruppe zur Stellungnahme vorzulegen. Diesem Gremium wird es auch obliegen, in Zweifelsfällen das Datenschutzniveau in Staaten außerhalb der Gemeinschaft, in die personenbezogene Angaben „exportiert" werden sollen, auf seine Vergleichbarkeit mit dem nach der Richtlinie verbindlichen gemeinschaftsweiten Standard zu überprüfen.

Die Gruppe hat sich am 17.01.1996 erst vorläufig konstituiert; die Verabschiedung der Geschäftsordnung wird erst auf der nächsten Sitzung im Mai stattfinden. In diesem Organ sind alle Mitgliedstaaten mit ihren unabhängigen Datenschutzkontrollbehörden vertreten. Die föderale Struktur der deutschen Datenschutzkontrolle im öffentlichen Bereich soll bei der **deutschen Repräsentanz** in der Gruppe nach Art. 29 so abgebildet werden, daß für den Bund der Bundesbeauftragte für den Datenschutz und für die Länder ein Stellvertreter aus dem Kreis der Landesbeauftragten an den Sitzungen teilnimmt.

6. Gesetzesvorhaben auf Bundesebene - Stellungnahmen

6.1 Justizmitteilungsgesetz (Entwurf)

6.1.1 Regelungsziel und Systematik des Entwurfs

Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach darauf hingewiesen, daß die in allgemeinen Verwaltungsvorschriften wie den „Mitteilungen in Strafsachen" (MiStra) und den „Mitteilungen in Zivilsachen" (MiZi) festgelegten Regelungen für Übermittlungen der Staatsanwaltschaft und der Gerichte aus Straf- und Zivilverfahren auf ihre Erforderlichkeit hin zu überprüfen und normenklar gesetzlich zu regeln sind (vgl. zuletzt die Entschließung der Datenschutzkonferenz vom 26./27. September 1994, abgedr. im 17. JB, Ziff. 20.8.). Die Bundesregierung hat den Landesjustizressorts den von ihr beschlossenen Entwurf eines Justizmitteilungsgesetzes (JuMiG) zugeleitet (BR-Drucks. 889/95). Der Bundesrat hat seine Stellungnahme am 09.02.1996 abgegeben.

Ziel des Gesetzentwurfes ist es, der Rechtsprechung des Bundesverfassungsgerichts zum Volkszählungsgesetz Rechnung zu tragen und die bisher überwiegend in bundeseinheitlich vereinbarten Verwaltungsvorschriften des Bundes und der Länder geregelten Mitteilungspflichten der Gerichte und Staatsanwaltschaften an andere öffentliche Stellen auf eine gesetzliche Grundlage zu stellen sowie verfahrensrechtliche Vorkehrungen zum Schutz des Persönlichkeitsrechts zu treffen. Besonders sensibel sind beispielsweise die Information des Arbeitgebers über die Einleitung eines Strafverfahrens gegen einen Mitarbeiter oder Mitteilungen über Entmündigungs- und Sorgerechtsverfahren

Der Gesetzentwurf, der grundsätzlich vom Vorrang spezifischer Übermittlungsregelungen ausgeht, schafft Übermittlungs**befugnisse.** Die Begründung von Mitteilungs**pflichten** soll weiterhin Verwaltungsvorschriften überlassen bleiben. Der Entwurf enthält Zweckbindungsregelungen sowie Berichtigungs- und Nachberichtspflichten. Benachrichtigungspflichten über Mitteilungen aus den Verfahren an die Betroffenen sind nur in sehr geringem Umfang vorgesehen. Auch die Erfüllung von Auskunftspflichten wird an den damit verbundenen Aufwand für die Verwaltung geknüpft.

6.1.2 Datenschutzrechtliche Kritik

Bereits im Vorfeld hatte sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit bekanntgewordenen Regelungen des Gesetzentwurfs auseinandergesetzt und mich als Vorsitzenden der Konferenz der Datenschutzbeauftragten gebeten, einige grundsätzliche Bedenken verbunden mit Verbesserungsvorschlägen an die Justizministerkonferenz heranzutragen.

Ich habe auf der Grundlage der mir vom Senator für Justiz und Verfassung zur Verfügung gestellten Niederschrift über die Beratungen im Unterausschuß Recht des Bundesrates eine Stellungnahme abgegeben, in der ich generell zum Ausdruck gebracht habe, daß die Regelungen nicht klar und präzise genug ausgefallen sind, daß betroffene Beschuldigte und Angeklagte erkennen könnten, wann sie mit einer Meldung welchen Inhalts an welche Behörde oder sonstige Stelle zu rechnen haben. Die Regelungen entsprechen daher weder den Anforderungen des BVerfG noch den in verschiedenen Beschlüssen der Konferenz der Datenschutzbeauftragten geforderten, aus den verfassungsrechtlichen Vorgaben abgeleiteten Standards.

Kritisiert habe ich u.a. auch die Regelungen über die Benachrichtigung der von einer staatsanwaltschaftlichen oder gerichtlichen Mitteilung Betroffenen und über die Weitergabe an Stellen, die Sicherheitsüberprüfungen durchführen.

Die vom Bundesrat verabschiedete Stellungnahme hat zu meinem Bedauern die von meinen Kollegen und mir vorgetragenen Kritikpunkte kaum berücksichtigt. Ich hoffe jetzt, daß der Bundestag noch wesentliche Korrekturen an den Vorstellungen der Länder vornimmt.

6.2 Telekommunikationsgesetz und TDSV

6.2.1 Die Postreform III als Gesetzentwurf

Das Bundeskabinett hat am 30. Januar 1996 dem vom Bundesministerium für Post und Telekommunikation (BMPT) vorgelegten **Entwurf eines Telekommunikationsgesetzes** (TKG-E) zugestimmt und dann dem Bundesrat zugeleitet. Er wurde Anfang März in den Ausschüssen des **Bundesrates**, federführend in dem unter dem Vorsitz Bremens stehenden Verkehrs- und Postausschuß, beraten (BR-Drucks.-Nr. 80/96). Die endgültige Haltung des Bundesrates soll am 22. März 1996, also nach Redaktionsschluß dieses Berichts, vom Plenum des Bundesrats festgelegt werden, so daß an dieser Stelle noch nicht darüber informiert werden kann, welche der Vorschläge, die meine Kollegen und ich ihren jeweiligen Landesregierungen unterbreitet haben, von der Länderkammer akzeptiert worden sind. Soweit dies nicht der Fall ist, bleibt als Adressat für Änderungswünsche noch der **Bundestag;** auch in seinen zuständigen Ausschüssen steht das TKG - dort als Fraktionsentwurf - auf der Tagesordnung (BT-Drucks. 13/609) und wird dort noch Gegenstand von Expertenanhörungen sein.

Die Datenschutzbeauftragten haben sich intensiv mit den im TKG-E enthaltenen Vorstellungen für die Postreform III auseinandergesetzt und dazu auf ihrer 50. Konferenz in Bremerhaven im November 1995 eine Entschließung verabschiedet (vgl. o. Ziff. 4.3 und u. Ziff. 20.15).

Die aus meiner Sicht notwendigen datenschutzrechtlichen Verbesserungen habe ich in zwei ausführlichen Stellungnahmen gegenüber der Senatskanzlei bzw. dem jetzt für die Telekommunikation zuständigen Häfensenator zur Vorbereitung und Abstimmung der Bremer Position im Bundesrat dargelegt. Sie beziehen sich u.a. auf die Regelungen über die Teilnehmerverzeichnisse (früher: Telefonbuch), die Rufnummernauskunft, den Einzelentgeltnachweis, das Widerspruchsrecht des Kunden gegen die Verwendung seiner Daten für Werbezwecke und die Kontrolle „mißbräuchlicher Inanspruchnahme" durch das TK-Unternehmen.

In diesem Berichtsbeitrag greife ich nur die wenigen Punkte heraus, die nach meiner Ansicht besonders dringend der Änderung bedürfen, um das Grundrecht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis in einer durch die Postreform III dann völlig liberalisierten Telekommunikations-Landschaft zu sichern.

6.2.2 Anwendungsbereich

Der **Anwendungsbereich** wird im TKG-E dadurch zu stark beschränkt, daß nach § 3 Nr. 15 nur **„gewerbliche"** Angebote als Telekommunikationsdienstleistungen i.S.d. TKG gelten. Damit fallen nicht-kommerzielle Angebote aus der Regelung des TKG und damit auch aus den spezifischen Datenschutzvorschriften heraus, soweit der Anwendungsbereich dort nicht ausdrücklich erweitert wird. Es ist aber nicht erkennbar, warum der gewerbliche Charakter des TK-Angebots ein unterschiedliches Datenschutzniveau rechtfertigen soll bzw. kann. Dies stellt auch eine Einschränkung gegenüber der geltenden Rechtslage dar, d.h. gegenüber der Definition von Telekommunikationsdienstleistungen, wie sie derzeit in § 2 Ziff. 2 Teledienstunternehmen-Datenschutzverordnung (UDSV) enthalten ist, dar; dort

heißt es **„geschäftsmäßig"** (und nicht „geschäftlich", also kommerziell). Gleiches gilt für den Anwendungsbereich des Bundesdatenschutzgesetzes.

Mit „geschäftsmäßig" ist im allgemeinen Datenschutzrecht (BDSG) die auf eine gewisse Dauer angelegte DV- bzw. TK-Aktivität gemeint, ohne daß es auf die Gewinnerzielungsabsicht bei der Verarbeitung der personenbezogenen Daten der TK-Teilnehmer ankommt. Ausgenommen vom Anwendungsbereich bleibt dann die TK-Dienstleistung, die ausschließlich **persönlichen und privaten** Charakter aufweist. Der Entwurf stellt leider nur für das Fernmeldegeheimnis selbst (§ 82 Abs. 2) ausdrücklich klar, daß auch geschäftsmäßige Angebote erfaßt sein sollen. Dies sollte auch für die übrigen datenschutzrechtlich relevanten Normen geschehen. Ich habe daher für die §§ 84 und 86 des Entwurfs entsprechende Textänderungen vorgeschlagen.

6.2.3 Datenschutzkontrolle

Verbesserungsbedürftig sind auch die Regelungen zur Kontrolle des Datenschutzes (§ 88). Hier ist eine Klarstellung erforderlich, die deutlich macht, wie sich die Aufsichtsbefugnisse der **Regulierungsbehörde** zu den Aufgaben und Instrumenten des **Bundesbeauftragten für den Datenschutz** (BfD) verhalten. Wenn, wie die Begründung des TKG-E nahelegt, eine Beanstandung nur über die Regulierungsbehörde erfolgen kann, ist eine effiziente und von möglicherweise konfligierenden Regulierungsinteressen unabhängige Kontrolle nicht gewährleistet. Der BfD muß daher Beanstandungen **direkt** an das betroffene Unternehmen richten können. Ferner sollten die Befugnisse des BfD aus dem BDSG auch im Bereich des TKG **in vollem Umfang** gelten.

Davon zu trennen ist die Frage, ob der BfD, also eine Institution des Bundes, bundesweit für **alle** TK-Dienstleistungsunternehmen ohne Rücksicht auf Größe und regionalen Geschäftsbereich zuständig sein soll. Nach meiner Auffassung sollten sie nicht pauschal aus der Kontrolle durch die **Aufsichtsbehörden der Länder** nach § 38 BDSG herausgelöst und der Zuständigkeit des BfD unterstellt werden.

Zumindest für Angebote, die ausschließlich oder überwiegend in einem Bundesland angeboten werden, sollte die Aufsicht bei den Landesbehörden verbleiben und von der bloßen Anlaßaufsicht in eine **Regelaufsicht** umgewandelt werden. Um Zersplitterung in der Prüfpraxis zu vermeiden, sind gerade im Telekommunikationsbereich bundeseinheitliche Bewertungsmaßstäbe unverzichtbar. Daher habe ich eine weitere Ergänzung des § 88 dahingehend angeregt, daß der Bundesbeauftragte für den Datenschutz und die Aufsichtsbehörden der Länder sich mit dem Ziel einer einheitlichen Verfahrensweise hinsichtlich der Kontrolle **abstimmen.**

6.2.4 Auskunftsersuchen der Sicherheitsbehörden

Nach § 87 TKG-E wird der Zugriff auf Kundendaten bei Auskunftsersuchen der Sicherheitsbehörden so ausgestaltet, daß nicht diese selbst, sondern die Regulierungsbehörde für sie auf die erforderlichen Angaben zugreift. Das vorgesehene On-line-Verfahren führt dazu, daß es einen jederzeitigen Zugriff der Regulierungsbehörde auf die Kundendateien **aller** TK-Anbieter gibt, d. h. **bundesweit der Gesamtdatenbestand aller TK-Teilnehmer für eine Behörde zum Direktzugriff bereitgehalten wird.** Zudem soll der Zugriff durch die Regulierungsbehörde den betroffenen Unternehmen verborgen bleiben. Warum die Sicherheitsbehörden nicht, wie es derzeit in der Fernmeldeüberwachungsverordnung geregelt ist, im Einzelfall mit ihrem Auskunftsersuchen **direkt** an die jeweiligen Dienstebetreiber herantreten können, ist nicht ersichtlich.

Selbst wenn man bei dem von mir kritisierten Regelungskonzept des TKG-E bleibt, muß jedenfalls ausdrücklich klargestellt werden, daß der Datensatz nach der Weitergabe an die anfragende Sicherheitsbehörde bei der Regulierungsbehörde gelöscht wird.

6.2.5 Auskunft über die Telekommunikation

§ 96 Abs. 1 Satz 2 Nr. 2 TKG-E sieht vor, daß **§ 12 Fernmeldeanlagengesetz** (FAG) in sprachlich nur leicht veränderter Form und unter Benennung der Grundrechtseinschränkung fortgelten soll. Damit wird Richtern und bei Gefahr im Verzug auch der Staatsanwaltschaft zu Ermittlungszwecken weiterhin außerhalb von §§ 100a ff. Strafprozeßordnung (StPO) ein zusätzliches, kaum beschränktes Auskunftsrecht über telekommunikative Aktivitäten eines Beschuldigten eingeräumt.

Die Datenschutzbeauftragten haben wiederholt darauf hingewiesen, daß eine derart weitgehende Befugnis, die auch bei kleinsten Delikten greift, mit dem Recht auf informationelle Selbstbestimmung und dem Schutz des Fernmeldegeheimnisses unvereinbar ist und generell nicht ins Fernmelde- bzw. Telekommunikationsrecht, sondern in die StPO gehört. Der Bundesrat hat bereits 1991 zu § 12 FAG festgestellt: „Ein umfassender Grundrechtsschutz verlangt, diese Eingriffe auf das unerläßliche Maß zu beschränken. Der Gesetzgeber ist deshalb gehalten, auch unter Berücksichtigung des Bestimmtheitsgebots eine Neuregelung des § 12 FAG vorzunehmen, . . ." (Bundesrats-Drs. 416/91, S. 5). Es ist daher unverständlich, daß diese aufgrund ihrer Eingriffstiefe unverhältnismäßige Norm im wesentlichen unverändert in die Neuregelung übernommen werden soll.

Ich habe daher vorgeschlagen, **§ 12 FAG zu streichen**, d. h. die Bestimmung mit Inkrafttreten des TKG außer Kraft zu setzen. Die „Auskunft über die Telekommunikation" sollte statt dessen dort geregelt werden, wo auch die übrigen Ermittlungsbefugnisse im Strafverfahren geregelt sind, nämlich in der StPO.

6.2.6 TDSV (neu)

Ein Teil der in Ziff. 6.2.1 erwähnten Punkte ist auch in der von der Bundesregierung beschlossenen „Telekommunikationsdienstunternehmen-Datenschutzverordnung-TDSV) vom 30.01.96 (Bundesrats-Drucks. 60/96) enthalten, die im Bundesrat nach dem gleichen Zeitplan wie der TKG-E beraten wird bzw. wurde. Diese Verordnung beruht auf § 10 des PTRegG als Rechtsgrundlage, ist also Bestandteil der 1994 durchgeführten Postreform II. Zum Datenschutz im Zusammenhang mit der Privatisierung und Zergliederung der TELEKOM hatte sich die Datenschutzkonferenz in zwei Entschließungen 1993 und 1994 geäußert (vgl. den Wortlaut dieser Beschlüsse in 16. JB, Ziff. 15.2, und 17. JB, Ziff. 20.4.) Auch zu diesem Gesetzgebungsvorhaben habe ich gegenüber dem Häfensenator im Detail Stellung genommen.

6.3 Die „kleine Volkszählung": Vorbereitung des Mikrozensus 1996

6.3.1 Korrekturen des Regierungsentwurfs

Der Deutsche Bundestag hat Anfang Dezember 1995 mit Zustimmung des Bundesrates ein neues Gesetz zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt sowie die Wohnsituation der Haushalte (Mikrozensusgesetz) in den Jahren 1996 bis 2004 verabschiedet. Im Januar 1996 wurde es verkündet, am Tag nach der Verkündung trat es in Kraft.

Dieses Gesetz war in der Entwurfsphase von deutlicher Kritik der Datenschutzbeauftragten begleitet. Kritisiert wurde insbesondere die geplante Ausweitung des Katalogs der Erhebungsmerkmale sowie die Einschränkung des Katalogs der freiwilligen Merkmale und damit verbunden die Ausdehnung der Auskunftspflicht. Im Gesetzgebungsverfahren wurde erreicht, daß das Erhebungsprogramm und die Auskunftspflicht nicht im anfänglich beabsichtigten Maße erweitert wurden. So wurde z. B. auf die Erhebung zusätzlicher Daten zum Freizeitverhalten, wie etwa Angaben über Kurzreisen und Tagesausflüge, die sogar mit Auskunftspflicht belegt waren, gänzlich verzichtet. Angaben, die nach dem alten Mikrozensusgesetz von Ausländern auf freiwilliger Basis erhoben wurden, z. B. über im Ausland lebende Ehepartner, Kinder oder Eltern, fallen entgegen der Planung auch weiterhin nicht unter die Auskunftspflicht.

Nicht erreicht werden konnte die auch von mir in der Vergangenheit mehrfach geforderte Ausdehnung der freiwilligen Auskunftserteilung z. B. auf Merkmale, die die berufliche Situation betreffen, oder gar eine Einschränkung des Erhebungskatalogs durch den Verzicht auf Angaben.

6.3.2 Datenschutzgerechte Erhebungsvordrucke

Bei der Durchführung des Mikrozensusgesetzes werden Erhebungsvordrucke verwendet. Diese Erhebungsvordrucke müssen nach Auffassung der Datenschutzbeauftragten so gestaltet sein, daß der Bürger aus ihnen ohne Schwierigkeiten entnehmen kann, welche Fragen der Auskunftspflicht unterliegen und welche Fragen von ihm freiwillig beantwortet werden können. Dies war bei der Durchführung früherer Mikrozensuserhebungen nicht gewährleistet. Die verwendeten Fragebögen enthielten vielmehr vermengt freiwillig zu beantwortende Fragen und Fragen unter Auskunftspflicht, so daß der Bürger die beiden Fragengruppen infolge einer wenig auffälligen Kennzeichnung kaum unterscheiden konnte.

Inzwischen hat das für die Gestaltung der Erhebungsvordrucke zuständige Statistische Bundesamt für die Mikrozensuserhebungen ab 1996 Erhebungsunterlagen entwickelt, die dem Bürger eine Unterscheidung der beiden Fragengruppen ermöglichen.

6.3.3 Computergestützte Erhebung

Gleichzeitig mit der Verabschiedung des neuen Mikrozensusgesetzes wurde auch das Bundesstatistikgesetz (BStatG) geändert. Der neue § 11a Abs. 1 BStatG sieht vor, daß Bundesstatistiken künftig auch mit computergestützten Erhebungsverfahren durchgeführt werden können. Damit werden z. B. der Einsatz tragbarer Computer (Laptops) oder computergestützte Telefoninterviews ermöglicht.

Der Einsatz technischer Erhebungsmittel bei der Durchführung von Statistiken birgt für das informationelle Selbstbestimmungsrecht der Betroffenen zusätzliche Gefahren. Dies gilt insbesondere für die Durchführung computergestützter Telefoninterviews. Anders, als wenn der Bürger Erhebungsbögen ausfüllt und diese direkt an das Statistische Amt übersendet oder die Beantwortung der Fragen unmittelbar gegenüber einem Interviewer erfolgt, der sich zuvor ausgewiesen hat, ist es dem verpflichteten Bürger bei diesen für ihn oft überraschenden Interviews z. B. kaum mehr möglich zu kontrollieren, ob die von ihm preisgegebenen Daten tatsächlich von der dafür zuständigen Stelle erhoben werden.

§ 11a Abs. 2 BStatG schränkt die Durchführung computergestützter Erhebungen insoweit ein, als den Betroffenen die Möglichkeit eingeräumt wird, ihre Antworten auch schriftlich zu erteilen. Dies gilt allerdings nur, soweit durch Rechtsvorschrift nichts anderes bestimmt ist. Gibt es eine solche Vorschrift, besteht die Möglichkeit zur schriftlichen Auskunftserteilung für den Betroffenen somit nicht.

Grundrechtssichernde Maßnahmen, wie sie § 11 Abs. 4 BStatG mit der Pflicht zur Angabe der Rechtsgrundlage und der bei der Durchführung der Statistik verwendeten Hilfsmerkmale auf Erhebungsvordrucken vorschreibt, fehlen in § 11a BStatG. Sinnvoll wäre z. B. die Aufnahme einer Bestimmung gewesen, nach der die betroffenen Bürger über die beabsichtigte Datenerhebung vorher schriftlich zu informieren und auf die Möglichkeit einer schriftlichen Auskunftserteilung hinzuweisen sind.

6.4 Datenabgleiche und Kontrolle der Privatsphäre: Neues von der Bekämpfung des Sozialleistungsmißbrauchs

6.4.1 Die Mahnung des Bundestages

Bundesregierung und einzelne Bundesländer werden nicht müde, neue Initiativen zur Intensivierung der Bekämpfung des Mißbrauchs von Sozialleistungen zu ergreifen. In meinen beiden letzten Jahresberichten (zuletzt in Ziff. 1.2 des 17. JB) habe ich die vielen Bundesgesetze der Jahre 1993/94 aufgelistet, die mittels Datennetzen und Datenflüssen den beklagten Mißbrauch bekämpfen sollen. Anstatt meine Kritik zu wiederholen, zitiere ich aus dem Beschluß, den der Deutsche Bundestag am 22.06.1995 (Plenarprotokoll der 13. Wahlperiode, S.3623) auf Empfehlung des Innenausschusses (BT-Drs. 13/1636) gefaßt hat. Dort heißt es unter Nr.1: „Die Bundesregierung wird aufgefordert, vor der Einrichtung von Datenabgleichsverfahren jeweils zu prüfen, ob sie im Interesse des Gemeinwohls zur Erreichung eines konkreten Ziels erforderlich und verhältnismäßig sind."

Im Bericht des Ausschusses heißt es hierzu: „Im Berichtszeitraum ist die Tendenz zur Kontrolle und Überwachung von Leistungsbeziehern mit Hilfe pauschaler automatisierter Datenabgleichsverfahren deutlich gewachsen. Selbst wenn die einzelnen Abgleiche und Kontrollvorgänge für sich eine gewisse Berechtigung, z. B. zur Bekämpfung von Leistungsmißbrauch haben, hat der Innenausschuß die Gefahr gesehen, daß ein umfassendes Netz von Überwachungs- und Überprüfungsmöglichkeiten geschaffen und vergrößert wird. Er hat es daher für unerläßlich angesehen, vor der Einrichtung von Datenabgleichsverfahren jeweils unter rechtsstaatlichen Erfordernissen, insbesondere dem Grundsatz der Verhältnismäßigkeit, zu prüfen, ob sie im Interesse des Gemeinwohls zur Erreichung eines konkreten Zieles erforderlich und verhältnismäßig sind".

Zwei Beispiele zeigen die Aktualität der Mahnung des Bundestages:

6.4.2 Mißbrauchsbekämpfung im Datenquerverbund - Die Initiative Bayerns

Fürs erste gescheitert, aber doch erschreckend in seiner Tendenz ist der Antrag Bayerns vom August 1995, die Konferenz der Arbeits- und Sozialminister des

Bundes und der Länder möge den Bund auffordern, gesetzlich zu ermöglichen, daß die in einer beliebigen Stelle der Verwaltung gespeicherten Bürgerdaten für alle Sozialleistungsträger verfügbar gemacht werden. Dies sei bürgerfreundlich und verhindere Leistungsmißbrauch.

Verbunden mit einer Reihe von Einzelvorschlägen (etwa eines direkten Zugriffs der Polizei auf Dateien der Arbeitsämter) würde dadurch die verfassungsrechtlich gebotene, ohnehin bereits arg durchlöcherte Zweckbindung der Datennutzung und ihre Transparenz für die betroffenen Bürger vollends abgeschafft. Hoffentlich hat das Scheitern dieses Vorstoßes das Bewußtsein der Verantwortlichen für die Fragwürdigkeit der Tendenz geschärft, die er verkörpert. Meine Stellungnahme, die ich auf seine Bitte hin dem Senator für Arbeit gegenüber abgegeben hatte, nahm der Bundesbeauftragte für den Datenschutz zum Anlaß, ein inhaltlich identisches Schreiben an das Bundesministerium für Gesundheit zu richten.

6.4.3 „Schnüffelei" in Wohngemeinschaften - Die Initiative des Bundes zur Änderung des Sozialhilferechts

Jedermann, der in einer Wohngemeinschaft wohnt, sollte verpflichtet werden, dem Sozialamt Auskunft über Einkommen und Vermögen zu geben, sofern ein Mitbewohner Sozialhilfe beantragt oder erhält. Entkräfte er nicht die Vermutung, er wirtschafte mit dem Hilfeempfänger gemeinsam, so solle diesem die Hilfe gekürzt bzw. beim Mitbewohner Regreß genommen werden. Dies hatte die Bundesregierung in ihrem Entwurf eines Gesetzes zur Reform des Sozialhilferechts, als Drs.13/2440 im September 1995 dem Bundestag zugeleitet, vorgeschlagen.

Die damit einhergehende Ausdehnung der bisher nur Ehegatten und unterhaltspflichtige enge Verwandte treffenden Auskunftspflicht mißachtet die Realität, drohte, sozial Schwache auszugrenzen und zu Schnüffelei in der Privatsphäre zu führen. Heutzutage wird der Einzug in eine Wohngemeinschaft meist durch die - gerade für junge Menschen, Senioren und Behinderte - zu hohen Mieten für Einzelappartements erzwungen und ist selten mit der Perspektive gemeinschaftlichen Lebens verbunden. Zweitens: Wer wird es bei Inkrafttreten einer solchen gesetzlichen Regelung noch riskieren, mit einem Sozialhilfeempfänger oder jemandem, der es werden könnte, zusammenzuziehen? Und schließlich: Bereits jetzt werden Befragungen bei „Verdacht" auf nichteheliche Lebensgemeinschaft als peinlich empfunden. Künftig müßten ggf. alle Bewohner von Wohngemeinschaften Fragebögen des Sozialamts ausfüllen oder mit amtlichen Besuch rechnen.

Nachdem der Bundesrat im ersten Durchgang ablehnend votiert hatte, sagte die Bundesregierung zu, Verbesserungsmöglichkeiten zu überprüfen. Der Änderungsantrag, den anschließend die Koalitionsfraktionen im Bundestag stellten, bedeutete aber keine Verbesserung aus Datenschutzsicht. Weiterhin sollte von Gesetzes wegen vermutet werden, daß Mitbewohner einer Wohngemeinschaft bereit seien, gegenseitig die Kosten der Unterkunft zu tragen. Die kritisierte Auskunftspflicht und Darlegungslast der Mitbewohner eines Sozialhilfeempfängers sollte unvermindert gelten. Zwar hat der federführende Gesundheitsausschuß des Bundestages auch diesen neuen Vorschlag abgelehnt, aber lediglich mit der Begründung, er werfe eine Reihe von Fragen auf, die jetzt nicht abschließend erörtert werden könnten. Der Vorstoß ist daher nicht endgültig vom Tisch. Es ist damit zu rechnen, daß er bei der nächsten Novellierung des Sozialhilferechts erneut aufgetischt wird.

6.5 Schuldnerverzeichnis: Detailregelungen für Inhalt, Verarbeitungszwecke, Empfänger und Automation

6.5.1 Zur Funktion des Schuldnerverzeichnisses

Am 01.01.1995 ist das „Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis (BGBl. I, 1566) in Kraft getreten. Die Regelungen passen die Vorschriften der ZPO den verfassungsrechtlichen Anforderungen im Hinblick auf die Wahrung des Rechts auf informationelle Selbstbestimmung an (vgl. Bericht des Rechtsausschusses des Deutschen Bundestages, BT-Drs. 12/6914). Das Schuldnerverzeichnis dient vor allem dem Schutz des Geschäftsverkehrs vor unzuverlässigen bzw. illiquiden Vertragspartnern. Durch Erzwingen einer eidesstattlichen Versicherung (früher: Offenbarungseid) hat der Gläubiger das Mittel, sich über das gesamte verwertbare Vermögen des Schuldners zu informieren, da dieser persönlich sein Vermögen genau angeben und die Richtigkeit an Eides statt und damit unter Strafandrohung versichern muß. Die Aufnahme in das Schuldnerverzeichnis hat in der Regel erhebliche nachteilige Folgen für den Schuldner im Geschäftsverkehr. Er verliert dadurch weitgehend seine Kreditwürdigkeit. Durch Tilgung seiner Schulden kann er allerdings eine vorzeitige Löschung erreichen.

Das Gesetz gestattet jedermann die Einsicht in das Schuldnerverzeichnis, ohne daß er hierfür ein berechtigtes Interesse darlegen muß. Das Register hat also eine gewisse Prangerwirkung, die die in ihm enthaltenen personenbezogenen Daten besonders sensibel macht.

6.5.2 Kernpunkte der Neuregelung

Das Gesetz begrenzt nunmehr in § 915 Abs. 2 ZPO ausdrücklich die Zwecke, für die die personenbezogenen Daten des Schuldnerverzeichnisses verwendet werden dürfen. Hierzu zählen neben der Zwangsvollstreckung und der Erfüllung gesetzlicher Pflichten zur Prüfung der wirtschaftlichen Zuverlässigkeit auch die Abwendung wirtschaftlicher Nachteile, die dadurch entstehen können, daß Schuldner ihren Zahlungspflichten nicht nachkommen. Durch diese Regelung werden auch Dritte gebunden, die die Informationen nur zu dem Zweck verwenden dürfen, zu dem sie sie erhalten haben. Nicht-öffentliche Stellen sind bei der Datenweitergabe über die Zweckbindung zu informieren.

Gemäß § 915b Abs. 2 ZPO gilt eine Eintragung als gelöscht, wenn seit dem Tage der Abgabe der eidesstaatlichen Versicherung drei Jahre verstrichen sind.

Gesetzlich geregelt ist auch die Führung zentraler bundesweiter oder regionaler Schuldnerverzeichnisse (§ 915e ZPO), deren Betreiber auf Antrag Ausdrucke zum laufenden Bezug auch in nur maschinell lesbarer Form erhalten können. Gleiches gilt für die Industrie- und Handelskammern und die Kammern, in denen Angehörige eines Berufes kraft Gesetzes zusammengeschlossen sind.

Auskünfte aus diesen Sekundärverzeichnissen dürfen auch im automatisierten Abrufverfahren erteilt werden, soweit dies unter Berücksichtigung der Belange der Betroffenen wegen der Vielzahl der Übermittlungen oder wegen ihrer besonderen Eilbedürftigkeit angemessen ist (vgl. § 915e Abs. 2 ZPO).

§ 915h ZPO ermächtigt die Bundesregierung, mit Zustimmung des Bundesrates den Inhalt des Schuldnerverzeichnisses, den Bezug von Abdrucken, das automatisierte Abrufverfahren sowie sich daraus ergebende Fragen näher zu regeln. Von dieser Ermächtigung ist mit der Verordnung über das Schuldnerverzeichnis (Schuldnerverzeichnisverordnung - SchuVVO) vom 15.12.1994 Gebrauch gemacht worden (BGBl. I, S. 3817).

6.5.3 Erweiterung der Kontrollbefugnisse

Ich beabsichtige, bei einzelnen mir von den Amtsgerichtspräsidenten gemeldeten Stellen bzw. bei sonstigen Empfängern von Abdrucken und Listen die Einhaltung dieser Vorschriften zu kontrollieren. Dazu bringt § 915e Abs. 4 ZPO eine wichtige Erweiterung der Kontrollmöglichkeiten: Bei Unternehmen, die statt Einzelauskünfte Abdrucke aus dem Schuldnerverzeichnis erhalten, und bei Firmen, die von ersteren Einzelauskünfte bekommen, kann die Aufsichtsbehörde abweichend von der Regel nach § 38 Bundesdatenschutzgesetz (BDSG) auch ohne hinreichende Anhaltspunkte für einen Verstoß gegen Vorschriften des Datenschutzes und ohne Beschränkung auf die dateimäßige Verarbeitung die Einhaltung der Datenschutzbestimmungen kontrollieren. Der Gesetzgeber unterstreicht damit die Sensibilität von Schuldnerdaten und trägt dem Risiko unkontrollierter Datenproliferation aus dem Schuldnerverzeichnis Rechnung.

6.6 Verbrechensbekämpfungsgesetz 1994 - Die Intervention des Bundesverfassungsgerichts

6.6.1 Erweiterte Abhörbefugnisse für den BND

Mit dem Verbrechensbekämpfungsgesetz vom 28.10.1994 (BGBl. I, 3186) sind die Regelungen des Gesetzes zu Art. 10 GG in verschiedener Hinsicht geändert worden. Insbesondere erweitert das Gesetz die Befugnis des Bundesnachrichtendienstes (BND) zur **Überwachung des Fernmeldeverkehrs** im Bereich des internationalen nicht leitungsgebundenen Verkehrs erheblich. Der BND wird ermächtigt, diesen Fernmeldeverkehr ohne konkreten Verdacht zu überwachen und Gespräche zur Planung und Begehung bestimmter Straftaten aufzuzeichnen. Zu diesem Zweck darf er **Suchbegriffe** verwenden. Damit wäre das Fernmeldegeheimnis im internationalen Fernmeldeverkehr faktisch aufgehoben worden. Der BND wird verpflichtet, die erlangten Daten vollständig an die Strafverfolgungs- und Sicherheitsbehörden weiterzugeben, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Eine wirksame Datenschutzkontrolle durch den Bundesbeauftragten für den Datenschutz ist vom Gesetz nicht vorgesehen. Meine Kritik an dieser **Vermischung von Strafverfolgung und nachrichtendienstlicher Auslandsaufklärung** habe ich im letzten Jahresbericht eingehend begründet (vgl. 17. JB, Ziff. 9.1.1.).

6.6.2 Übermittlungsstop durch einstweilige Anordnung

Ich habe in meiner Stellungnahme gegenüber dem Bundesverfassungsgericht diese Kritik wiederholt und ebenso wie eine Reihe meiner Kollegen die Verfassungsmäßigkeit der neuen Abhörregelungen in Zweifel gezogen. Bereits die 48. Datenschutzkonferenz hatte sich übrigens am 26./27.09.1994 mit einer Entschließung gegen die Datenverarbeitungsregelungen für den BND im Verbrechensbekämpfungsgesetz ausgesprochen (vgl. 17. Jahresbericht, Ziff. 20.10).

Das Bundesverfassungsgericht hat mit Beschluß vom 05.07.1995 (1 BvR 2226/94) den **Vollzug** des Verbrechensbekämpfungsgesetzes insoweit **vorläufig außer Kraft gesetzt**, als es um die zu extensiven Befugnisse des BND zur Weitergabe von Abhördaten an die Sicherheitsbehörden geht. Diese einstweilige Anordnung hat das Gericht mit Beschluß vom 21.12.1995 wiederholt. Die Entscheidung des Bundesverfassungsgerichts läßt keinen Zweifel an der zentralen Bedeutung der Kommunikationsfreiheit für jeden einzelnen Bürger und die Gesellschaft. Sie läßt erkennen, daß die Verfassungsrichter den tatsächlichen Eingriffscharakter des Gesetzes sehr hoch einschätzen. Die künftige Entscheidung in der Hauptsache wird wegweisende Bedeutung für die verfassungsrechtliche Bewertung des Verhältnisses von Kommunikationskontrolle und dem Recht auf unbeobachtete Kommunikation haben.

7. Rechtsänderungen in Bremen

7.1 Neue gesetzliche Regelungen in Kraft

7.1.1 Novellierung des Bremischen Datenschutzgesetzes

7.1.1.1 Inkrafttreten und Neubekanntmachung

Die Novellierung des Bremischen Datenschutzgesetzes ist am 27. Mai 1995 in Kraft getreten. Die Neufassung wurde im Gesetzblatt der Freien Hansestadt Bremen Nr. 43/1995 vom 6. Juli 1995 bekannt gemacht (Brem.GBl. 1995, S. 343). Die Bürgerschaft hatte das Gesetz noch in ihrer letzten Sitzung der 13. Wahlperiode am 9. Mai einstimmig verabschiedet.

7.1.1.2 Kernpunkte der Neuregelung

Schwerpunkt der Neufassung ist die **Erweiterung der Rechte des Bürgers** gegenüber der Verwaltung. Bei Vermögensschäden oder Verletzung des Persönlichkeitsrechts aufgrund unrichtiger automatisierter Verarbeitung seiner Daten kann der Einzelne von der zuständigen Behörde jetzt **Schadensersatz** auch ohne Nachweis eines Verschuldens verlangen. Anspruchsberechtigt ist beispielsweise jemand, der einen Kredit aufnehmen muß, weil ein bremisches Amt aufgrund eines Computerfehlers beantragte oder zugesagte Geldleistungen nicht in voller Höhe oder zu spät ausgezahlt hat.

Verstärkt wurde auch das **Auskunftsrecht:** Wer von staatlichen und städtischen Stellen in Bremen und Bremerhaven wissen will, welche Angaben diese über ihn/sie haben, bekommt in aller Regel eine schriftliche Auskunft. Wem das nicht genügt, der kann künftig auch **Einsicht in „seine" Akte** verlangen und sich **Abschriften oder Kopien** machen (lassen). Eine weitere Verbesserung: Das Auskunftsrecht des Bürgers erstreckt sich jetzt auch auf die Personen oder Stellen, **von denen seine Daten herkommen oder an die sie weitergegeben worden sind,** damit er auch dort seine Berichtigungs- und Löschungsansprüche geltend machen kann. **Ausnahmen** gibt es allerdings nach wie vor bei berechtigten Geheimhaltungsinteressen anderer Beteiligter oder der Behörde selbst, etwa bei laufenden Ermittlungen. Die Auskunftsverweigerung muß jedoch begründet und kann vom Datenschutzbeauftragten nachgeprüft werden.

Eine ausführliche Darstellung der Neuregelungen habe ich im 17. JB unter Ziff. 4. gegeben.

In einer Presseerklärung anläßlich des Inkrafttretens habe ich dazu aufgefordert, von den Auskunfts-, Berichtigungs- und Löschungsrechten nach dem Datenschutzgesetz rege Gebrauch zu machen. Wer dafür Hilfestellung brauche oder bei Behörden auf Schwierigkeiten stoße, solle sich sofort an mich wenden.

7.1.1.3 „Parlamentsklausel" beim Anwendungsbereich

Bis zuletzt diskutiert und sowohl im Datenschutzausschuß wie im Verfassungs- und Geschäftsordnungsausschuß beraten wurde der **Anwendungsbereich des**

BrDSG in bezug auf die Bürgerschaft und die Fraktionen; erst in der gemeinsamen Sitzung beider Ausschüsse am 26. April 1995 wurde die jetzt Gesetz gewordene Formulierung festgelegt.

Nach dem neu gefaßten § 1 Abs. 3 BrDSG unterliegen die Bürgerschaft (Landtag), ihre Mitglieder, ihre Gremien, die von ihr gewählten Mitglieder der Deputationen, die Fraktionen und Gruppen sowie deren Verwaltungen und deren Beschäftigte nicht den Bestimmungen des Gesetzes, soweit sie in Wahrnehmung verfassungsmäßiger Aufgaben personenbezogene Daten verarbeiten. Dies gilt entsprechend für die Stadtbürgerschaft. Im Gesetzgebungsverfahren habe ich auf die Gefahr aufmerksam gemacht, daß diese Formulierung des BrDSG bei extensiver Interpretation die Geltung des BrDSG zu stark einschränkt.

Zunächst bedeutet allerdings die Nichtanwendbarkeit des BrDSG bei der parlamentarischen Tätigkeit nicht, daß der in § 1 Abs. 3 BrDSG genannte Personenkreis den verfassungsrechtlich gewährleisteten Schutz des informationellen Selbstbestimmungsrechts der Bürger nicht zu beachten braucht. Die **Geheimhaltungspflicht** der Abgeordneten der Bürgerschaft ergibt sich aus Art. 83 der Landesverfassung und § 5 der Geschäftsordnung der Bürgerschaft. Für die Deputierten, die nicht Mitglied der Bürgerschaft sind, wurde gleichzeitig mit dem BrDSG § 6 Abs. 2 Deputationsgesetz dahingehend ergänzt, daß für sie die Geheimhaltungspflichten der Abgeordneten ebenfalls gelten (Brem.GBl. 1995, S. 307).

Diese Regelungen reichen jedoch nicht aus, um den Schutz des Rechts auf informationelle Selbstbestimmung bei der Verwendung persönlicher Daten von Bürgerinnen und Bürgern zu parlamentarischen Zwecken sicherzustellen. Geheimhaltungsvorschriften betreffen nur die Frage der Weitergabe von Informationen nach außen. Sichergestellt werden müssen aber auch die **Individualrechte** der Betroffenen auf Auskunft und Löschung für ihre im Parlamentsbereich verarbeiteten Daten. Ein anderes Beispiel: Bei parlamentarischen Dokumentations- und Informationssystemen (zum Bremer Projekt PARLIS vgl. 17. JB. Ziff. 7.2.) müssen **Speicherumfang und Zugriffsberechtigungen** festgelegt werden.

7.1.1.4 Datenschutzordnung für die Bürgerschaft

Parlamentsinterne Regelungen über die Verarbeitung von Informationen über die Bürger werden sinnvollerweise zusammengefaßt in einer **Datenschutzordnung.** Eine solche Datenschutzordnung ist keine Ausgeburt von bürokratischem Perfektionismus, sondern notwendiges, verfassungsrechtlich gebotenes Korrelat der Herausnahme des Parlaments aus der Geltung des Datenschutzgesetzes. Ausreichende bürgerschaftsinterne Normen sind auch unverzichtbar für die effiziente Ausübung der parlamentarischen Kontrollrechte, wenn diese - wie häufig - mit der Offenlegung persönlicher Daten durch die senatorischen Behörden verbunden ist. § 16 Abs. 1 BrDSG macht die Übermittlung personenbezogener Angaben durch die Verwaltung an die Bürgerschaft davon abhängig, daß „überwiegende schutzwürdige Belange der Betroffenen nicht entgegenstehen". § 16 Abs. 2 BrDSG verlangt bei der Übermittlung von Daten, die einem besonderen Amts- oder Berufsgeheimnis unterliegen, darüber hinaus, daß die Vertretungsorgane „die Wahrung dieser Geheimnisse durch geeignete Vorkehrungen gewährleisten".

Diese Regelungen geben die **verfassungsrechtlichen Vorgaben** wieder, wie sie das Bundesverfassungsgericht in seiner Rechtsprechung insbesondere zur Abwägung zwischen parlamentarischen Untersuchungsbefugnissen und dem Schutz des Persönlichkeitsrechts aufgestellt hat (vgl. auch 17. JB, Ziff. 7.1.1). Das Hamburgische Verfassungsgericht hat in seinem Urteil vom 19.07.95 (Az. 1/95) ebenfalls klargestellt, daß der (dortige) Senat von der Bürgerschaft und ihren Ausschüssen angeforderte Akten nur dann unbeschränkt vorlegen müsse, wenn die Bürgerschaft sichergestellt habe, daß schutzwürdige persönliche Daten entsprechend den Vorschriften des Grundgesetzes geschützt würden. Das Gericht hat weiterhin festgestellt, daß die Hamburger Bürgerschaft keine diesen Anforderungen genügende normative Sicherung des Grundrechts auf informationelle Selbstbestimmung hergestellt habe und hat dementsprechend Einschränkungen für die Aktenvorlage verfügt.

Bei der Beratung der BrDSG-Novelle hatte die Bürgerschaftverwaltung bereits vorgeschlagen, in § 1 ausdrücklich zu verankern, daß die Bürgerschaft sich unter Berücksichtigung ihrer verfassungsrechtlichen Stellung eine Datenschutzordnung gibt. Diese Formulierung habe ich unterstützt. Andere Bundesländer sind hier schon weiter; eine solche Regelung besteht bereits in Hessen (vgl. § 39a Hessisches DSG und Datenschutzordnung des Hessischen Landtags vom 05.04.95) und Rheinland-Pfalz (§ 2 Abs. 2 Rh.-Pf. DSG). Der Datenschutzausschuß kam damals

überein, diese gesetzliche Selbstverpflichtung nicht ins Gesetz aufzunehmen, lehnte aber die Anregung der Bürgerschaftsverwaltung nicht inhaltlich ab. Im März 1995 haben die Direktoren bei den deutschen Landesparlamenten von einer Arbeitsgruppe vorbereitete **„Thesen zum parlamentsspezifischen Datenschutzrecht"** einschließlich eines **Musterentwurfs einer Datenschutzordnung** zustimmend zur Kenntnis genommen und der Präsidentenkonferenz vorgelegt.

Der Präsident der Bremischen Bürgerschaft hat mir zugesagt, den Direktor des Parlaments damit zu beauftragen, sich mit dieser Fragestellung zu befassen und mich dabei einzuschalten. Auch der Datenschutzausschuß wird das Thema voraussichtlich wieder aufgreifen.

7.1.2 Gesetz über den Öffentlichen Gesundheitsdienst im Lande Bremen

Am 01.12.1995 ist endlich das Gesetz über den öffentlichen Gesundheitsdienst in Kraft getreten (ÖGDG, Brem.GBl. S. 175). Es trägt in seinen §§ 30 bis 36 meiner langjährigen Forderung Rechnung, angesichts der Vielfalt der Aufgaben der Gesundheitsämter, die von streng vertraulicher Beratung in heiklen Gesundheitsfragen (z.B. AIDS-Beratung) über gutachterliche Stellungnahmen (z. B. amtsärztlicher Dienst) bis zu Überwachungs- und Zwangsmaßnahmen (z. B. Unterbringung psychisch Kranker) reichen, die Zweckbindung der Klientendaten sicherzustellen, d. h. grundsätzlich zu untersagen, daß etwa Beratungsdaten für Gutachten oder Zwangsmaßnahmen genutzt werden, es sei denn, der Betroffene hätte wirksam eingewilligt oder eine der eng umschriebenen Ausnahmevoraussetzungen läge vor (z. B. Gefährdung von Leib oder Leben).

Es wird darauf ankommen, diese klare gesetzgeberische Entscheidung

- bei der anstehenden Rechtsverordnung über den Umfang der Erhebung und Speicherung von Klientendaten, die Löschungsfristen und die für die Zweckbindung bedeutsame Abgrenzung der Aufgabenbereiche der Gesundheitsämter zu präzisieren,
- durch das Gesetz für psychisch Kranke (vgl. u. Ziff. 7.2.3) nicht zu verwässern, sondern zu akzentuieren,
- bei der Automatisierung der Datenverarbeitung in den Gesundheitsämtern (aktuelle Beispiele: EDV im amtsärztlichen Dienst und im sozialpsychiatrischen Dienst des Gesundheitsamtes Bremen, vgl. u. Ziff. 15.3) durch die gebotenen technischen Vorkehrungen umzusetzen und
- durch die Bestellung geeigneter Personen als Datenschutzbeauftragte der Gesundheitsämter abzusichern.

Die Schaffung einer gesetzlichen Grundlage für eine unabhängige Ethikkommission in § 30 des ÖGDG für die Beratung der Ärzte im Lande Bremen in Fragen wissenschaftlicher Forschung habe ich zum Anlaß genommen, dem Gesundheitsressort vorzuschlagen, mir Gelegenheit zu geben, der Kommission gegenüber zu datenschutzrechtlichen Problemen von medizinischen Forschungsprojekten Stellung zu nehmen. Dies würde sowohl der Berücksichtigung der schutzwürdigen Belange betroffener Patienten als auch der Akzeptanz von Forschung dienen, etwa für den Fall, daß im künftigen Krebsregister gespeicherte Patientendaten zu Forschungszwecken genutzt werden (vgl. zum Krebsregister Ziff. 7.2.1).

7.1.3 Heilberufsgesetz

Der Bundesgerichtshof hat 1991/92 in zwei Entscheidungen aus der ärztlichen Schweigepflicht den Schluß gezogen, daß es der Einwilligung ihrer Patienten bedarf, wollen Ärzte deren Daten nach **Verkauf der Praxis** ihrem Rechtsnachfolger (vgl. 15. JB, Ziff. 10.4) oder zur Einziehung von Honorarforderungen gegenüber Privatpatienten einer **Verrechnungsstelle** (vgl. 14. JB, Ziff. 3.5) übermitteln. Die Umsetzung der Rechtsprechung hat für die Ärzteschaft die unangenehme Konsequenz, daß sie gewohnte Praktiken beim Umgang mit Patientendaten aufgeben muß.

Die Befürchtung, daß diese höchstrichterliche Rechtsprechung nicht immer Beachtung findet, scheint nicht von der Hand zu weisen, jedenfalls deuten immer wieder Eingaben Betroffener darauf hin. Deshalb sind auf meinen Vorschlag hin im Rahmen einer Änderung des Heilberufsgesetzes (BremGBl. 1996 S. 1) mit Wirkung vom Dezember 1995 die Ärztekammern verpflichtet worden, in ihre Berufsordnungen Regelungen über Einhaltung der ärztlichen Schweigepflicht bei Praxisaufgabe, Praxisnachfolge und bei Privatliquidation über Verrechnungsstellen

aufzunehmen. Entsprechende Aufforderungen richten sich auch an die Apothekerkammern.

Die Kammern sind nunmehr per Gesetz gehalten, wirksame Schritte zur Umsetzung der einschlägigen Rechtsprechung zu unternehmen, nachdem sie sich bislang darauf beschränkt hatten, in ihren Publikationsorganen über sie zu berichten. Das Gesundheitsressort wird insoweit notfalls per Rechtsaufsicht den Vollzug des Heilberufsgesetzes durch die Kammern durchsetzen müssen.

7.1.4 Zweitwohnungssteuer-Gesetz in Bremen - Melderegister als Datenquelle

Anfang Dezember 1995 hat die Stadtbürgerschaft Bremen das Ortsgesetz über die Erhebung einer Zweitwohnungssteuer in der Stadtgemeinde Bremen beschlossen. Es wurde noch im Dezember 1995 vom Senat der Freien Hansestadt Bremen verkündet und trat am 01.01.1996 in Kraft. Steuerpflichtig sollen nach diesem Ortsgesetz (§ 3) die Inhaber von Wohnungen sein, deren melderechtliche Verhältnisse die Beurteilung der Wohnung als **Zweitwohnung** bewirken. Damit setzt das Ortsgesetz am melderechtlichen Begriff der **Nebenwohnung** an. Um die relevanten Steuerfälle zu erhalten, soll eine regelmäßige Übermittlung der in Bremen mit Nebenwohnung gemeldeten Einwohner an die zuständige Finanzbehörde realisiert werden.

Hierfür ist eine **Änderung der Bremischen Meldedatenübermittlungsverordnung** erforderlich. Dazu hatte der Finanzsenator mir noch im Dezember 1995 einen Vorschlag zur Stellungnahme zugesandt. In meiner Stellungnahme habe ich darauf hingewiesen, daß mit einer regelmäßigen Übermittlung von Einwohnerdaten mit Nebenwohnungsstatus für Zwecke der Zweitwohnungsbesteuerung keine korrekte und vollständige Erfassung der Steuerpflichtigen erreicht werden kann. So muß zum einen auf den unsicheren Aktualitätstand des Melderegisters und der dortigen Angaben verwiesen werden, ferner auf die Dunkelziffer nicht gemeldeter Personen, insbesondere gerade solcher mit Nebenwohnsitz. Auch ist eine Vielzahl der von der Meldebehörde übermittelten Nebenwohnungsfälle für eine Zweitwohnungsbesteuerung nicht relevant, weil eine Zweitwohnung im Sinne des Ortsgesetzes gar nicht vorliegt (z.B. Gemeinschaftsunterkunft, Wohnheim oder andere Beherbergungsstätte, möbliertes Zimmer, Räume in Kleingartengebieten etc.). Und ob sich aus den Regelungen über die Ausnahmen, Befreiungen und Sonderbestimmungen zur Meldepflicht weitere Besonderheiten ergeben, muß ebenfalls überprüft werden.

Nach einer Berechnung der Verwaltung werden für Bremen etwa 27.000 Zweitwohnungen geschätzt. Die Zahl der Einwohner, die mit Nebenwohnung in Bremen gemeldet sind, ist nicht bekannt. Nach den Erfahrungen einer anderen deutschen Großstadt waren dort fast 40 % der zugesandten Zweitwohnungssteuererklärungen unzustellbar; nur in etwa 50 % der Fälle wurde eine Steuererklärung abgegeben; von denjenigen, die eine Steuererklärung abgaben, erhielt wiederum nur ein Teil einen Zweitwohnungssteuerbescheid.

Im Ergebnis muß man also feststellen, daß die Treffsicherheit des Melderegisters hinsichtlich der für eine Zweitwohnungsbesteuerung relevanten Fälle nicht besonders hoch ist. Ich habe deshalb empfohlen, die beabsichtigte Änderung der Meldedatenübermittlungsverordnung vorerst nur **befristet** einzuführen, um den melderechtlichen Anknüpfungspunkt der Zweitwohnungsbesteuerung auf seine Tauglichkeit hin zu erproben.

Da es sich um eine kommunale Steuer handelt, dürfen die Meldedaten nicht an die Finanzämter allgemein, sondern nur an die die **örtlichen** Steuerangelegenheiten wahrnehmende Finanzbehörde übermittelt werden. In der Stadtgemeinde Bremen ist das aufgrund der geltenden Übertragungsregelungen von Verwaltungszuständigkeiten allein das Finanzamt Bremen Mitte. Kritische Anmerkungen habe ich auch gemacht zu dem vom Finanzsenator gewünschten, nach meiner Auffassung zu umfangreichen **Katalog** von Meldedaten.

Die Beratung und Beschlußfassung zur Änderung der Bremischen Meldedatenübermittlungsverordnung steht noch aus. Gleichwohl werden derzeit schon systemtechnische Einzelheiten der geplanten ADV-Lösung zwischen Finanzsenator und Stadtamt Bremen abgestimmt, ein hoffentlich nicht vorschnelles Vorgehen.

7.1.5 Mehr Demokratie wagen - Das neue Gesetz über Volksbegehren und Volksentscheid

Auf der Grundlage der 1994 geänderten Landesverfassung, die neue Formen unmittelbarer Demokratie wie den Bürgerantrag, das Volksbegehren und den

Volksentscheid eingeführt hat, hat die Bürgerschaft (Landtag) am 24. Januar 1996 das neue Gesetz über das Verfahren beim Volksentscheid verabschiedet (Brem.GBl. 1996 S. 41). Für mich war es in diesem Zusammenhang vor allem wichtig, daß die Daten der Personen, die sich durch ihre Unterstützungsunterschrift zu einem Anliegen bekennen und damit ihre demokratischen Rechte wahrnehmen, nicht zweckentfremdet werden, etwa als Grundlage für melderechtliche Verfahren oder als Anlaß für sicherheitsbehördliche Beobachtung. § 28 des neuen Gesetzes bestimmt auf meinen Vorschlag hin eindeutig, daß die zur Einleitung bzw. Durchführung von Volksbegehren oder Volksentscheiden erhobenen personenbezogenen Daten nur für diesen Zweck, d.h. nur zur Überprüfung der Teilnahmeberechtigung bzw. des Wohnsitzes, genutzt werden dürfen und zu vernichten sind, wenn sie für das jeweilige Verfahren nicht mehr benötigt werden.

Eine parallele Regelung findet sich auch in dem Bremerhavener Ortsgesetz, mit dem basisdemokratische Verfahren eingeführt werden (vgl. die folgende Ziff.).

7.1.6 Bremerhaven: Ortsgesetz zur Einführung des Einwohnerantrags, Bürgerentscheids, Bürgerbegehrens

Im Berichtsjahr wurden durch das Ortsgesetz zur Änderung der Verfassung der Stadt Bremerhaven (Brem.GBl. vom 23.03.1995, S. 335) auch weitergehende Rechte der Einwohner bzw. Bürger Bremerhavens zur unmittelbaren Mitwirkung in kommunalen Angelegenheiten beschlossen. So können Einwohner ab dem 16. Lebensjahr beantragen, daß die Stadtverordnetenversammlung bestimmte ihr obliegende Selbstverwaltungsangelegenheiten berät und entscheidet. Ein solcher Antrag muß von mindestens fünftausend Einwohnern unterschrieben sein. Außerdem können Bürger der Stadt ein Bürgerbegehren beantragen, das wichtige Selbstverwaltungsangelegenheiten zum Gegenstand hat. Hierfür sind mindestens fünfzehntausend Unterschriften erforderlich. Schließlich kann auch die Stadtverordnetenversammlung beschließen, daß die Bürger der Stadt selbst über wichtige Selbstverwaltungsangelegenheiten entscheiden (sog. Bürgerentscheid).

Zur Umsetzung dieser neuen Möglichkeiten wurden Durchführungsregelungen erlassen, die insbesondere die Antrags- bzw. Unterschriftslisten und ihre Behandlung innerhalb der Verwaltung betreffen.

Unter Hinweis auf denkbare Gefahren des Mißbrauchs dieser Listen sowie entsprechende Regelungen im Landesrecht (s.o. Ziff. 7.1.5) habe ich für das Ortsrecht Bremerhavens Datenschutzregelungen für die Verwendung der Antrags- bzw. Unterschriftslisten innerhalb der Verwaltung vorgeschlagen. Die Stadtverordnetenversammlung ist diesem Verlangen nachgekommen und hat beschlossen, daß die Antragslisten oder Einzelanträge ausschließlich zur Prüfung der Zulässigkeit eines Einwohnerantrags bzw. Bürgerbegehrens verwendet werden dürfen und daß diese Unterlagen nach Abschluß des Antragsverfahrens zu vernichten sind.

7.1.7 Gesetz über den Abbau der Fehlsubventionierung im Wohnungswesen (Brem.AFWoG)

Dieses bremische Gesetz regelt die Erhebung der Fehlbelegungsabgabe. Wesentliche Änderung der Novellierung mit dem Gesetz vom 27. März 1995 (Brem.GBl. S. 191) war aus datenschutzrechtlicher Sicht die Neufassung des § 5 Abs. 3 Brem.AFWoG. Die bisherige Regelung besagte generalklauselartig, daß alle Behörden, insbesondere die Finanzbehörden, und die Arbeitgeber der zuständigen Stelle, konkret dem Amt für Wohnung und Städtebauförderung, Auskunft über die Einkommensverhältnisse der betroffenen Wohnungsinhaber zu erteilen hatten, soweit die Durchführung dieses Gesetzes es erforderte.

Auf meinen Vorschlag hin sieht die neue Gesetzesfassung jetzt vor, daß derartige Auskünfte bei dritten Stellen erst dann eingeholt werden dürfen, wenn begründete Zweifel an der Richtigkeit der Angaben des Wohnunginhabers bestehen. Vor einem Mitteilungsersuchen an den Arbeitgeber und die Finanzbehörden soll dem Wohnungsinhaber Gelegenheit zur Stellungnahme gegeben werden. Bekräftigt wird damit der auch im BrDSG verankerte Grundsatz, daß Angaben am Bürger vorbei und ohne seine Kenntnis nur in Ausnahmefällen bei anderen Behörden erfragt werden dürfen (vgl. § 10 Abs. 2 BrDSG).

7.1.8 Die neue Hafengebührenordnung

Am 5. Dez. 1995 ist die Änderung der Hafengebührenordnung (Brem.GBl S. 469) erlassen worden. Die novellierte Fassung enthält erstmalig Bestimmungen über

die Verarbeitung von personenbezogenen Daten bei der Gebührenfestsetzung, bei der Rechnungsstellung und bei der kassenmäßigen Abwicklung. Ebenso wurde geregelt, zu welchem Zeitpunkt die Daten zu sperren und zu löschen sind.

7.2 Entwürfe zur Änderung von Rechtsvorschriften

7.2.1 Krebsregistergesetz - Vorarbeiten für einen Entwurf

7.2.1.1 Vorgaben des Bundesgesetzgebers

Die medizinische Forschung mag für die vollständige Erfassung aller Krebskranken zwecks Speicherung ihrer Daten in einem Krebsregister noch so gute Gründe anführen, die auf Dauer angelegte Speicherung personenbezogener medizinischer Daten weckt doch Befürchtungen, die Daten könnten einen Tages auf derzeit nicht vorhergesehene Weise auch zum Schaden der davon Betroffenen genutzt werden. Deshalb - und dies war seit jeher die Forderung der Datenschutzbeauftragten (vgl. 13. JB, Ziff. 2.6.4) - ist ein der Registrierung entgegenstehender Wille eines Krebskranken zu beachten, ist die Nutzung seiner Daten eng zu begrenzen und sind die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen.

Einen entsprechenden Rahmen gibt das Krebsregistergesetz des Bundes (BGBl. I 1994, S. 3351) vor, das zum 01.01.1995 in Kraft getreten ist - lang erwartet und bis zur abschließenden Abstimmung im Bundesrat heftig umstritten. Dabei ging es neben der Abwägung zwischen Forschungsinteresse und Persönlichkeitsschutz um Fragen der Finanzierung und Kompetenzaufteilung zwischen Bund und Ländern. Aus Datenschutzsicht ist das Ergebnis widersprüchlich: Einerseits regelt das Gesetz die Erhebung und den Umgang mit den registrierten Daten krebskranker Menschen minutiös und skrupulös. Auf der anderen Seite ist ein Großteil der Regelung unter den Vorbehalt abweichender Länderregelungen gestellt und die Geltung des Gesetzes insgesamt bis zum 31.12.1999 befristet - eine bislang wohl einzigartige Kompromißkonstruktion.

7.2.1.2 Vorarbeiten für ein Landesgesetz

Jedenfalls sind nach § 1 des Bundesgesetzes, der nicht unter Vorbehalt abweichender Ländergesetze steht, vor Ablauf der Geltungsfrist Krebsregister einzurichten, die Auftreten und Entwicklung aller Formen von Krebserkrankungen beobachten, vornehmlich anonymisierte Daten für die Forschung bereitstellen und nach Maßgabe näherer Länderregelungen aus selbständigen, räumlich, organisatorisch und personell voneinander getrennten Vertrauensstellen und Registerstellen bestehen, d. h. einer Stelle, die das Krankheitsregister führt und einer Stelle, der allein es vorbehalten ist, zu bestimmten gesetzlich vorgegebenen Zwecken den Personenbezug der registrierten Daten herzustellen, etwa nach Einwilligung der betroffenen Patienten zu Forschungszwecken.

Die bisherigen Vorarbeiten für ein bremisches Krebsregistergesetz, an dem ich von Anfang an beteiligt worden bin, geben zu der Erwartung Anlaß, daß ein Gesetzentwurf vorgelegt werden wird, der den zwingenden bundesgesetzlichen Anforderungen genügt und die dem Landesgesetzgeber eröffneten Möglichkeiten für Regelungen nutzt, die sowohl den Belangen der Forschung als auch dem Persönlichkeitsschutz der betroffenen Patienten gerecht wird.

7.2.2 Krankenhausgesetz - Entwurf in Vorbereitung

Das Bremische Krankenhausdatenschutzgesetz von 1989 (Brem.GBl. S. 202) regelt in noch heute bundesweit beachteter und vorbildlicher Weise die Vertraulichkeit und streng zweckgebundene Nutzung der Patientendaten in allen Krankenhäusern im Lande Bremen (zu meinen Datenschutzprüfungen auf der Grundlage dieses Gesetzes vgl. Ziff. 15.4.2 und 15.4.3).

Derzeit ist ein Landeskrankenhausgesetz in Vorbereitung, in dem das Krankenhausdatenschutzgesetz als Abschnitt IV „Patientendatenschutz" aufgehen soll. Nachdem ich vorübergehend den Eindruck hatte gewinnen müssen, man wolle mich von der Vorbereitung des Gesetzes ausschließen, ist nunmehr auch gegenüber den Krankenhäusern geklärt worden, daß zwar eine Modernisierung der Datenschutzregelungen, nicht aber deren Abschwächung ansteht. Unter diesen Voraussetzungen kann ich die beabsichtigte Integration des Datenschutzes in die Festlegung der Aufgaben der Krankenhäuser nur begrüßen.

7.2.3 Gesetz für psychisch Kranke - Novellierung in Arbeit

Derzeit wird im Hause des Gesundheitssenators eine umfassende Novellierung des Gesetzes für psychisch Kranke (PsychKG) von 1979 vorbereitet. Es besteht Einvernehmen darüber, daß die im Gesetz über den öffentlichen Gesundheitsdienst getroffenen Datenschutzregelungen (vgl. o. Ziff. 6.1.2) auch für Beratung und Hilfen für psychisch Kranke sowie ihre zwangsweise Unterbringung Anwendung finden. Dies gilt auch für die Bestimmungen zur Abschottung vertraulicher Beratungsdaten vor einer Nutzung zu Zwangsmaßnahmen. Ausnahmen sollen nur zur Abwehr von Gefahren für Leib und Leben der betroffenen Person oder Dritter zulässig sein.

7.2.4 Sicherheitsüberprüfungsgesetz (SÜG) - Entwurf überfällig

Bereits im Bericht des Datenschutzausschusses zum 15. Jahresbericht (Bürgerschafts-Drs. 13/686, S. 1) hat der Ausschuß die Erwartung geäußert, daß der Senat so bald wie möglich den Entwurf eines SÜG für das Land Bremen vorlegt, um für die mit den Sicherheitsüberprüfungen verbundenen erheblichen Eingriffe in die Persönlichkeitsrechte der Betroffenen eine gesetzliche Grundlage zu schaffen. Ich habe dieses Petitum in meinem 17. JB wieder aufgegegriffen (vgl. 17. JB, Ziff. 1.3.1.).

Der Senator für Inneres hat mir inzwischen einen ersten Entwurf für ein Landesgesetz zur Stellungnahme zugeleitet. In meiner Rückäußerung, die ich im Herbst 1995 abgegeben habe, habe ich u. a. darauf hingewiesen, daß dieser Entwurf hinter der Haltung Bremens im Bundesrat beim Erlaß eines Sicherheitsüberprüfungsgesetzes des Bundes zurückbleibt. Es fehlt die Grundorientierung hin auf eine Reduzierung der Personenüberprüfungen auf den unbedingt erforderlichen Umfang. Auch sind die betroffenen Sicherheitsbereiche noch zu unklar und zu weit gefaßt. Zu viele Lebenspartner und Familienangehörige sollen mit überprüft werden. Änderungsbedarf besteht auch noch beim Umfang der Sicherheitserklärungen (Fragebögen), bei den Regelungen über die Zuständigkeiten für die Kontrollen in der Privatwirtschaft sowie beim Anhörungsverfahren und dem Auskunftsrecht.

Der Datenschutzausschuß der Bremischen Bürgerschaft hat sich im November 1995 mit diesem Thema befaßt. Der vom Landtag angenommene Bericht des Ausschusses zu meinem 17. JB (Bürgerschafts-Drucks. 14/210) äußert -erneut - die Erwartung, daß so bald wie möglich ein Gesetzentwurf vorgelegt und dabei meine Stellungnahme berücksichtigt wird (vgl. Ziff. 8.2).

7.2.5 Bauvorlagenverordnung - Entwurf in Vorbereitung

Nachdem die Novellierung der Bremischen Landesbauordnung (Brem.LBO) vom 27. März 1995 (Brem.GBl. S. 211) am 1. Januar 1996 in Kraft getreten ist, obliegt es nunmehr dem Senator für Bau, Verkehr und Stadtentwicklung, durch **Rechtsverordnung** nach § 86 Abs. 2 Nr. 4 i. V. m. § 62 Brem.LBO Vorschriften zu erlassen über die Verarbeitung personenbezogener Daten der am Bau verantwortlich Beteiligten, der Grundstückseigentümer, Nachbarn, Baustoffproduzenten und sonstigen am Verfahren zu Beteiligenden. Danach bedarf es näherer Bestimmungen über Art, Umfang und Zweck der **Datenerhebung** in den verschiedenen Verfahren. Im einzelnen festzulegen sind auch die zu **übermittelnden** Daten und deren Empfänger sowie Anlaß und Empfänger bei regelmäßigen Datenübermittlungen.

Inzwischen hat die senatorische Dienststelle den ersten Entwurf einer Bauvorlagenverordnung vorgelegt. Ich habe hierzu u.a. vorgeschlagen, wegen der umfangreichen und für den Betroffenen wenig übersichtlichen Regelungen über die Datenübermittlung an andere Behörden vorzusehen, daß dem Empfänger eines baurechtlichen Bescheides bekanntzugeben ist, welche Stellen personenbezogene Daten im Rahmen seines Verfahrens erhalten haben. Der überarbeitete Entwurf berücksichtigt meine Vorschläge.

8. Die Arbeit des Datenschutzausschusses

8.1 Beratung des Doppelhaushalts 1996/1997

Für die parlamentarische Kontrolle des Datenschutzes besteht nach § 35 BrDSG der **Datenschutzausschuß** als ständiger Parlamentsausschuß. Er ist nach der Neuwahl der Bürgerschaft im Mai 1995 neu konstituiert worden. Seine Aufgaben sind erst mit der Novellierung des BrDSG 1995 ausdrücklich gesetzlich geregelt worden (vgl. 17. JB, Ziff. 4.6.). § 35 BrDSG erwähnt zum einen die Beratung der Jahres-

berichte und der Zwischenberichte des LfD (dazu u. Ziff. 8.2). Zum anderen weist die Vorschrift dem Ausschuß die Beratung des jeweiligen Entwurfs des **Haushalts**kapitels des LfD als Aufgabe zu.

Bei der Beratung des Doppelhaushaltes 1996/1997 erhielt ich zu meinem Bedauern nicht die Unterstützung des Ausschusses für meine Vorlage. Die Mehrheit war nicht bereit, von den vom Senat festgesetzten Eckwerten auch nur geringfügig abzuweichen, so daß mein ohnehin bescheidenes konsumtives Budget (1995 = 190.000 DM) für beide Haushaltsjahre jeweils um ca. 16 % gekürzt werden wird (160.000 DM), wobei der für 1996 veranschlagte Betrag noch unter dem Vorbehalt einer weiteren 5%igen Kürzung steht.

Ich habe vor dem Ausschuß meine Auffassung dargelegt, daß die derart **stark gekürzten Beträge** nicht ausreichen, um den tatsächlichen Mittelbedarf auch nur für den Kernbereich meiner gesetzlichen Aufgaben zu decken. Dies gilt insbesondere für die **Fortbildung** meiner Mitarbeiter: § 27 Abs. 4 BrDSG verlangt vom LfD, zu den Auswirkungen des Einsatzes neuer (!) Informationstechniken Stellung zu nehmen. Eine zukunftsorientierte Datenschutzberatung und -kontrolle ist aber nur möglich, wenn der LfD sein technisches Wissen ständig erweitert und mit seinen IuK-Kenntnissen nicht unter das Niveau der Anwender in der bremischen Verwaltung gerät.

8.2 Beratung des 17. Jahresberichts für 1994

In drei Sitzungen wurden mein 17. Jahresbericht und die zugehörige Stellungnahme des Senats (Bürgerschafts-Drucks. 14/29) in Anwesenheit der jeweiligen Ressortvertreter beraten. In einer Reihe von Punkten hat der Datenschutzausschuß meine Position unterstützt und den Senat zu entsprechendem Handeln aufgefordert. Er verabschiedete seinen abschließenden Bericht am 6. Februar 1996 (Bürgerschafts-Drucks. 14/210); die Bürgerschaft nahm ihn in ihrer Februar-Sitzung zur Kenntnis.

Der Ausschußbericht enthält folgende Feststellungen, Empfehlungen und Aufforderungen im Wortlaut:

Zu 17. JB; Ziff. 1.3.1: Sicherheitsüberprüfungsgesetz des Landes

Der Ausschuß schließt sich der bereits im Bericht des Ausschusses zum 15. Jahresbericht geäußerten Erwartung an, daß der Senat so bald wie möglich ein Sicherheitsüberprüfungsgesetz für das Land Bremen vorlegt, um für die mit diesen Überprüfungen verbundenen erheblichen Eingriffe in das Persönlichkeitsrecht der Betroffenen eine gesetzliche Grundlage zu schaffen. Der Ausschuß geht davon aus, daß bei der Vorbereitung des Entwurfs die Stellungnahme des Landesbeauftragten für den Datenschutz berücksichtigt wird. (Anm.: Vgl. den Beitrag Ziff. 7.2.4)

Zu 17. JB; Ziff. 5.1.1: Das TuI-Regelwerk - eine unendliche Geschichte

Da das Regelwerk für die Einführung technikunterstützter Informationsverarbeitung (Anm.: Gemeint ist der im Brem. Abl. Nr. 7/96 veröffentlichte erste Teil des sog. TuI-Regelwerks) nicht sicherstellt, daß der Landesbeauftragte für den Datenschutz frühzeitig unterrichtet wird, unterstreicht der Ausschuß die Pflicht der Verwaltung, den Landesbeauftragten für den Datenschutz bereits im Stadium der TuI-Planung zu beteiligen.

Zu 17. JB; Ziff. 9.2: Erkennungsdienstliche Behandlung aller Bürgerkriegsflüchtlinge?

Die Konferenz der Innenminister und -senatoren des Bundes und der Länder schlägt eine Gesetzesänderung vor, wonach künftig für alle Bürgerkriegsflüchtlinge dieselben Regelungen wie für Asylbewerber gelten sollen. Dies würde insbesondere bedeuten, daß Bürgerkriegsflüchtlinge in jedem Fall erkennungsdienstlich zu erfassen wären.

Der Senator für Inneres hat gegenüber dem Datenschutzausschuß die in der Senatsstellungnahme dazu enthaltene und nicht ganz eindeutige Aussage klargestellt, indem er hervorgehoben hat, daß bis zu einer eventuellen Gesetzesänderung Bürgerkriegsflüchtlinge entsprechend der geltenden Rechtslage nur dann erkennungsdienstlich behandelt werden, wenn sie keinen Paß vorlegen können.

Zu 17. JB; Ziff. 9.2.5: Verfassungsschutzüberprüfung bei Einbürgerung

Der Landesbeauftragte für den Datenschutz hat den Ausschuß darüber informiert, daß in der Mehrzahl der anderen Bundesländer in Einbürgerungsverfahren keine Regelanfrage bei den Verfassungsschutzämtern durchgeführt wird. Der Ausschuß hält es der Sache nach für angemessen, daß sich der Senat dieser Praxis anschließt und Rückfragen beim Verfassungsschutz nur in Fällen vornimmt, in denen Anhaltspunkte dafür vorliegen, daß Erkenntnisse des Verfassungsschutzes einer Einbürgerung entgegenstehen.

Zu 17. JB; Ziff. 9.4.1: Wahlkampf mit Wählerdaten

Der Ausschuß bittet den Senator für Inneres, für eine landeseinheitliche Handhabung der Weitergabe von Wählerdaten an die Parteien Sorge zu tragen und insbesondere sicherzustellen, daß keine Daten aus den Melderegistern Bremens und Bremerhavens an nicht zur Wahl antretende Parteigliederungen außerhalb Bremens weitergegeben werden.

Zu 17. JB; Ziff. 9.4.2: Meldesperren und Wählerverzeichnis

Der Senator für Inneres wird gebeten, bis zum 30.09.1996 dem Ausschuß zu berichten, welche Maßnahmen er zur Lösung des Konflikts zwischen dem Prinzip der Öffentlichkeit des Wählerverzeichnisses und dem Anspruch gefährdeter Personen auf Geheimhaltung ihrer Anschrift zu treffen beabsichtigt.

Zu 17. JB; Ziff. 10.1: Strafakten als multifunktionale Informationsquelle

Der Datenschutzausschuß sieht in Übereinstimmung mit dem Senator für Justiz und Verfassung und dem Landesbeauftragten für den Datenschutz einen dringenden Bedarf für eine bundesgesetzliche Regelung über die Datenverarbeitung im Strafverfahren und zur Akteneinsicht in staatsanwaltschaftliche Verfahrensregister, wie sie im Entwurf des Bundesrates für ein Strafverfahrensänderungsgesetz (StVÄG) zum Ausdruck gekommen ist. Der Ausschuß begrüßt die Absicht des Senats, die seinerzeit vom Land Bremen im Bundesrat vorgeschlagenen, jedoch nicht berücksichtigten Änderungen zur Verbesserung des Datenschutzes im StVÄG zu gegebener Zeit erneut einbringen zu wollen.

Zu 17. JB; Ziff. 11.2: Erhebungen, Untersuchungen und Forschungsvorhaben an öffentlichen Schulen im Lande Bremen und

zu 17. JB; Ziff. 11.3: Datenschutz bei Forschungsprojekten

Der Ausschuß begrüßt, daß zwischen dem Senator für Bildung und Wissenschaft und dem Landesbeauftragten für den Datenschutz inhaltlich Übereinstimmung besteht über die datenschutzrechtlichen Voraussetzungen für die Durchführung von Erhebungen und Forschungsvorhaben an öffentlichen Schulen. Er nimmt weiterhin zur Kenntnis, daß zur Umsetzung dieser Vorgaben zwischen den beiden Behörden abgestimmte Merkblätter bzw. Checklisten zur Verfügung stehen. Der Datenschutzausschuß erwartet aber, daß die notwendigen Abstimmungsprozesse bei den Antrags- bzw. Genehmigungsverfahren zwischen dem Senator für Bildung, Wissenschaft, Kunst und Sport und dem Landesbeauftragten zügig erfolgen und Verzögerungen von Forschungsvorhaben vermieden werden. Zu diesem Zweck hält es der Ausschuß für notwendig, daß die noch bestehende Meinungsverschiedenheit zwischen diesen beiden Dienststellen über den Umfang der von der senatorischen Behörde zu leistenden datenschutzrechtlichen Prüfung von Forschungsvorhaben umgehend ausgeräumt wird. (Anm.: Vgl. dazu den Beitrag Ziff. 13.1)

Zu 17. JB; Ziff. 12.2.2: Anonymität in der Schwangerschaftskonfliktberatung und beim Sozialamt

Der Ausschuß hat zur Kenntnis genommen, daß aufgrund des Schwangeren- und Familienhilfeänderungsgesetzes die Zuständigkeit für die finanzielle Hilfe für Schwangere ab Januar 1996 bundesweit von den Sozialämtern auf die gesetzlichen Krankenkassen übergegangen ist. Der Ausschuß ist weiterhin darüber informiert worden, daß derzeit in Bremen Gespräche zwischen den gesetzlichen Krankenkassen und dem Landesbeauftragten für den Datenschutz stattfinden, um eine größtmögliche Anonymität der Schwangeren im Verfahren der Kostenerstattung sicherzustellen. Der Ausschuß erwartet, daß der Senator für Arbeit diese Zielsetzung bei Bedarf im Rahmen seiner Aufsichtstätigkeit unterstützt. (Anm.: Vgl. dazu auch Ziff. 14.4)

Zu 17. JB; Ziff. 12.3.6: Schutz des Beratungsgeheimnisses im Amt für Soziale Dienste

Wie dem Auschuß vom Sozialressort mitgeteilt worden ist, werden die im Mai 1994 vom Amt für Soziale Dienste in Kraft gesetzten Dienstanweisungen zum Hilfeplan und zum Datenschutz gegenwärtig auf ihre Praktikabilität hin überprüft. Der Ausschuß bittet den Senator für Frauen, Gesundheit, Jugend, Soziales und Umweltschutz, ihm bis zum 30. Juni 1996 über das Ergebnis der Prüfung zu berichten.

Zu 17. JB; Ziff. 12.3.7: Wirtschaftlichkeits- und Qualitätsprüfung - auch mit Mitarbeiter- und Klientendaten?

Durch die Änderung des § 93 des Bundessozialhilfegesetzes sind als Voraussetzung für die Kostenübernahme Regelungen mit den Einrichtungen der freien Wohlfahrtsverbände zu treffen, die den Trägern der Sozialhilfe eine Prüfung von Wirtschaftlichkeit und Qualität der Leistungen ermöglichen. Nach Auffassung des Datenschutzausschusses ist die Befürchtung des Landesbeauftragten für den Datenschutz, dabei könnten auch sensible Daten der Klienten herangezogen werden, nicht von der Hand zu weisen. Wie der Vertreter des Sozialressorts im Ausschuß berichtet hat, sollen zur Frage der Wirtschaftlichkeitskontrolle bundeseinheitliche Rahmenbedingungen erarbeitet werden.

Der Ausschuß bittet das Sozialressort, zu gegebener Zeit über die Praxis der Kostenübernahme zu berichten und dabei insbesondere über eine eventuelle Erhebung und Auswertung von Mitarbeiter- und Klientendaten bei der Kostenkontrolle zu informieren. Der Ausschuß geht dabei davon aus, daß der Landesbeauftragte für den Datenschutz bei der Festlegung von Standards für die Wirtschaftlichkeitskontrollen nach dem Bundessozialhilfegesetz rechtzeitig beteiligt wird. (Anm.: Vgl. dazu auch Ziff. 14.1)

Zu 17. JB, Ziff. 16.1.: Vorlage des Steuerbescheids statt Nachweis von Einzelangaben

Um bestimmte öffentliche Leistungen wie zum Beispiel Wohngeld, Sozialhilfe oder Kindergartenplätze in Anspruch nehmen zu können, müssen Einkommensnachweise erbracht werden. Hierfür steht derzeit nur der Steuerbescheid zur Verfügung, der jedoch eine Fülle anderer Daten enthält, deren Mitteilung für die Gewährung der Leistung nicht erforderlich ist.

Nach Auffassung des Ausschusses ist vom Senat bisher nicht hinreichend geprüft worden, ob nicht generell für beantragte Leistungen der genannten Art ein mit der Erteilung des Steuerbescheides zusätzlich herzustellender Teilausdruck, der nur die Höhe des zu versteuernden Einkommens angibt, als ausreichend anzusehen ist. Der Datenschutzausschuß bittet den Senat hierzu um einen Bericht, der insbesondere auch darstellt, welche Angaben im einzelnen bei den jeweiligen einkommensabhängigen Leistungen verlangt werden.

8.3 Aktuelle Themen

Der Datenschutzausschuß hat auch die Funktion, den Informations- und Meinungsaustausch zwischen den Abgeordneten und dem LfD über aktuelle, vor allem über von den Medien aufgegriffene oder im Parlamentsbetrieb angesprochene Themen zu ermöglichen. Die Tagesordnung jeder Sitzung enthält dafür den Punkt „Aktuelle Probleme des Datenschutzes". Von seiner Konstituierung nach der Sommerpause 1995 bis Februar 1996 hat der Ausschuß u. a. **folgende Themen** behandelt:

- Telefonbücher auf CD-ROM (vgl. dazu Ziff. 19.1),
- Sicherheitsrisiken von Anrufbeantwortern,
- Meldedatenübermittlung für die Erhebung der Zweitwohnungssteuer (vgl. dazu in diesem Bericht Ziff. 7.1.4),
- Angabe des Arbeitgebers des Ehegatten beim Antrag auf Ortszuschlag (vgl. dazu Ziff. 10.3),
- Verschlüsselung von Diagnosen nach dem ICD 10-Schlüssel (vgl. dazu Ziff. 15.2.3).

Der Ausschuß hat sich auch über den Stand und die rechtlichen Probleme des **Europol-Übereinkommens** informieren lassen, das vom Europäischen Rat am

26. Juli 1995 verabschiedet und am gleichen Tag unterzeichnet wurde (vgl. ABl. C 316 vom 27.11.95; s. dazu die frühere Entschließung der Datenschutzkonferenz vom 26./27.09.94, im 17. JB, Ziff. 20.9.). Der Senator für Inneres hat zugesagt, den Ausschuß weiterhin rechtzeitig über den Fortgang der Beratungen und die Umsetzung des Übereinkommens zu unterrichten.

9. Technische Datensicherung

9.1 Neue Software - inkompatibel mit bisherigem Zugriffsschutzprogramm

Bislang wurde bei der Verarbeitung sensibler personenbezogener Daten in der bremischen Verwaltung unter den Betriebssystemen MS-DOS und Windows 3.x standardmäßig das Produkt **„SAFEGuard"** eingesetzt. Diese Kombination aus Hard- und Software ermöglicht eine On-line-Verschlüsselung der Festplatte, die automatisch, d. h. ohne Zutun der Zugangsberechtigten erfolgt.

Bei der Markteinführung des neuen Programms **Windows '95** durch den Hersteller, die Fa. Microsoft, zeigte sich allerdings, daß es nicht mit der bisher verwendeten Version von SAFEGuard kompatibel ist. Mit der Einführung einer solchen angepaßten SAFEGuard-Version ist nicht vor Mitte 1996 zu rechnen; sie soll von der Herstellerfirma auf der CeBIT '96 (Mitte März 1996) vorgestellt werden.

Um das bisherige Niveau des Zugriffsschutzes nicht zu gefährden, muß in den Bereichen, in denen aufgrund der Sensibilität der verarbeiteten personenbezogenen Daten SAFEGuard implementiert werden muß, weiterhin die Betriebssystemkombination MS-DOS 6.2x und Windows 3.1x verwandt werden.

Das TuI-Referat der SKP hat als Alternative vorgeschlagen, in geeigneten Fällen statt SAFEGuard die Netzsoftware **Windows NT 3.51** zu einzusetzen. Ob damit ein vergleichbarer Sicherungsstandard erzielt werden kann, prüfe ich derzeit. Ohne dem Ergebnis dieses Programmtests, das ich dann der SKP und den betroffenen Dienststellen zugehen lassen werde, vorgreifen zu wollen, lassen sich schon jetzt folgende Bedingungen für diese Lösung erkennen:

- Die Schutzmechanismen dieser Software greifen nur, wenn sie nicht über ein bestehendes Betriebssystem installiert und das Dateisystem NTFS eingesetzt wird.
- Windows NT 3.51 bietet keine Verschlüsselungsmöglichkeiten an. Das Dateisystem NTFS ist zwar nicht DOS-kompatibel, aber mit entsprechenden Tools ist auch ein Zugriff über DOS möglich. Daher ist in den Bereichen, in denen eine Festplattenverschlüsselung zwingend erforderlich ist, Windows NT 3.51 alleine als Schutz nicht ausreichend.
- Bei der Einrichtung der Arbeitsplatzrechner muß durch Konfiguration des BIOS sichergestellt werden, daß nicht von der Diskette „gebootet" werden kann und der Zugriff auf die Systemkonfiguration des BIOS durch Paßwort geschützt ist.

9.2 Internet: Orientierungshilfe zur Lösung von Datensicherungsproblemen

9.2.1 Zunahme von Anschlußwünschen

Wegen der immer größeren Verbreitung des Internet wächst auch in den öffentlichen Verwaltungen der Wunsch, einen Anschluß an dieses weltweite Netz zu erhalten. Wie groß auch in den bremischen Behörden das Interesse ist, soll die einschlägige Bedarfsumfrage des TuI-Referats der SKP ergeben. Voraussetzung für Anbindungen an das Internet ist jedoch die Klärung der Datensicherungsfragen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte daher ihren zuständigen Arbeitskreis beauftragt, ein **Informationspapier** zu dieser Thematik zu erstellen. Diese Ausarbeitung ist im Dezember 1995 fertiggestellt worden. Ihr wesentlicher Inhalt wird im folgenden wiedergegeben. Die in diesem Papier enthaltenen Empfehlungen stellen für mich die Grundlage dar für Beratungen und Prüfungen in diesem Bereich.

9.2.2 Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

9.2.2.1 Einleitung

Seit einiger Zeit wächst in öffentlichen Stellen der Wunsch nach einem Zugang zu globalen Datennetzen, insbesondere zu dem Internet. Die Netzanbindung soll sowohl zur Informationsgewinnung als auch zur Bereitstellung eigener Informationen für andere dienen.

Dabei ist der Anschluß an das Internet mit erheblichen **Gefährdungen des Datenschutzes und der Datensicherheit** verbunden. Die Risiken resultieren großenteils daraus, daß das Internet nicht unter Sicherheitsaspekten entwickelt wurde. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. So gibt es beispielsweise keine sicheren Mechanismen zur Identifikation und Authentisierung im Netz. Ohne besondere Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen oder sogar manipulieren oder zerstören. Dies ist besonders gravierend, weil angesichts von z. Z. mehr als 40 Millionen Internet-Teilnehmern auch die Zahl der potentiellen Angreifer, die diese Sicherheitslücken ausnützen und somit die am Internet angeschlossenen Verwaltungsrechner bedrohen, sehr groß ist.

Die erstellte Orientierungshilfe soll den für den Betrieb von Netzen der öffentlichen Verwaltung Veranwortlichen deutlich machen, mit welchen **Risiken für die Sicherheit der „internen" Netze** bei einem Anschluß an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können. Die Frage, ob und ggf. unter welchen Bedingungen Verwaltungen personenbezogene Daten über das Internet austauschen dürfen, ist nicht Gegenstand der Orientierungshilfe und muß jeweils konkret untersucht werden.

Die in der Orientierungshilfe entwickelten **Strategien zur Risikobegrenzung** bedürfen im Einzelfall einer weiteren Konkretisierung, wobei neben den beschriebenen Firewall-Architekturen ggf. weitere Maßnahmen zu ergreifen sind, um eine Gefährdung personenbezogener Daten zu vermeiden (etwa Einsatz von Verschlüsselungsverfahren). Angesichts einer sich ständig verändernden Gefährdungslage infolge der „Entdeckung" neuer unerwarteter Sicherheitsprobleme bleiben auch bei Einsatz von Firewall-Systemen erhebliche Restrisiken bestehen.

Der Anschluß an das Internet ist angesichts dieser Gefährdungslage aus Datenschutzsicht nur vertretbar, wenn zuvor eine eingehende Analyse und Bewertung der damit verbundenen Risiken erfolgt ist und die Gefahren durch **technische und organisatorische Maßnahmen** sicher beherrscht werden können. Die nachfolgenden **Empfehlungen** stellen ein Konzentrat aus den weiterführenden, in diesem Bericht nicht abgedruckten Überlegungen dar.

9.2.2.2 Empfehlungen

- Verwaltungsnetze dürfen an das Internet nur angeschlossen werden, wenn und soweit dies erforderlich ist. Die Kommunikationsmöglichkeiten haben sich am **Kommunikationsbedarf** zu orientieren. Dabei ist auch zu prüfen, inwieweit das Behördennetz in anschließbare, nicht anschließbare und bedingt anschließbare Teile segmentiert werden muß und ob die Aufgabe mit einem nicht in das Verwaltungsnetz eingebundenen Rechner erfüllt werden kann.

- Voraussetzung für die Anbindung eines Behördennetzes an das Internet ist das Vorliegen eines schlüssigen **Sicherheitskonzepts** und dessen konsequente Umsetzung. Die Internet-Anbindung darf nur erfolgen, wenn die Risiken durch technische und organisatorische Maßnahmen wirksam beherrscht werden können.

- Die Sicherheit des Verwaltungsnetzes und der Schutz von personenbezogenen Daten, die auf vernetzten Systemen verarbeitet werden, ist durch geeignete **Firewall-Systeme** sicherzustellen, die eine differenzierte Kommunikationssteuerung und Rechtevergabe unterstützen. Dabei sind die Anforderungen, die von den Firewall-Komponenten zu erfüllen sind, vorab zu definieren, wobei sich die Verwaltung ggf. auch externen Sachverstands bedienen sollte.

- Um der Gefahr von Maskeraden und der Ausforschung der Netzstrukturen des geschützten Netzes entgegenzuwirken, ist eine **gesonderte interne Adreßstruktur** zu verwenden. Die internen Adressen sind durch die zentrale Firewall auf externe Internet-Adressen umzusetzen.

- Der ausschließliche Einsatz einer zentralen Firewall-Lösung ist nur dann vertretbar, wenn eine Orientierung am höchsten Schutzbedarf erfolgt, auch wenn dies Nachteile für weniger sensible Bereiche mit sich bringt. Die Frage der Kontrolle interner Verbindungen bleibt bei einer solchen Lösung offen. Ferner ist eine ausschließlich zentrale Lösung mit der Maxime der lokalen Haltung und Verwaltung von sicherheitsrelevanten Daten (Pflege von Benutzerprofilen)

schwer vereinbar. Werden solche Daten nicht durch diejenigen verwaltet, die den verwalteten Bereich direkt überschauen können, besteht die Gefahr erheblicher Differenzen zwischen Realität und sicherheitstechnischem Abbild.

— Das **Konzept gestaffelter Firewalls** kommt den Datenschutzanforderungen an Verwaltungsnetze entgegen, die aus einer Vielzahl verschiedener Teilnetze bestehen, in denen Daten unterschiedlicher Sensibilität von unterschiedlichen Stellen für unterschiedliche Aufgaben verarbeitet werden und in denen dementsprechend jeweils unterschiedliche Sicherheitsanforderungen bestehen. Die mit gesonderten Firewalls abgesicherten Subnetze sollten jeweils einen definierten Übergang zu dem Gesamtnetz erhalten. Die Anbindung des Gesamtnetzes an das Internet sollte stets über ein **zentrales Gateway** erfolgen, das durch eine Firewall geschützt wird.

— Der personelle und sachliche Aufwand für Firewall-Lösungen ist generell hoch. Es ist gleichwohl unverzichtbar, hochspezialisierte Kräfte einzusetzen, um gegen mindestens ebenso spezialisierte Angreifer gewappnet zu sein. Dieser Aufwand ist jedoch stets dann gerechtfertigt, wenn Verwaltungsnetze an das Internet angeschlossen werden sollen, in denen sensible personenbezogene Daten verarbeitet werden.

— Der Betrieb von Firewall-Systemen muß **klaren Richtlinien** folgen. Diese Richtlinien müssen neben Zuständigkeitsregelungen auch Vorgaben über die Protokollierung, die Behandlung von sicherheitsrelevanten Ereignissen und Sanktionen bei Sicherheitsverstößen enthalten.

— Auch bei Einsatz von Firewalls bleiben **Restrisiken** bestehen, denen anwendungsbezogen begegnet werden muß. So bleibt es auch beim Einsatz von Firewalls notwendig, sensible Daten nur verschlüsselt zu übertragen; hierzu gehören neben besonders sensiblen personenbezogenen Daten auch Paßwörter und sonstige Authentifikationsdaten.

— Bei einem unvertretbaren Restrisiko muß auf einen Anschluß des jeweiligen Netzes an das Internet verzichtet werden. Der Zugriff auf Internet-Dienste muß in diesem Fall auf nicht in das Verwaltungsnetz eingebundene Systeme beschränkt werden, auf denen ansonsten keine sensiblen Daten verarbeitet werden.

— Firewall-Konzepte entlasten die dezentralen Verwalter von vernetzten Systemen nicht von ihrer Verantwortung zur Gewährleistung des Datenschutzes; vielmehr erhöhen sich mit der Vernetzung die Anforderungen an die lokale Systemverwaltung, da Administrationsfehler ungleich schwerwiegendere Konsequenzen haben könnten als bei stand alone betriebenen Rechnern.

10. Personalwesen

10.1 Dezentralisierung der Personaldatenverarbeitung - Start für das Projekt PuMa

10.1.1 Senatsbeschluß - Einheitlichkeit der Personaldatenverarbeitung?

Wie bereits im letzten Jahresbericht beschrieben, soll das Verfahren PuMa (Personalverwaltung und -management) in allen senatorischen und nachgeordneten Dienststellen im Rahmen der Personalsachbearbeitung und -budgetierung eingesetzt werden (vgl. 17. JB, Ziff. 8.2.). Der Senat hat im Dezember 1995 den entsprechenden **Beschluß** über die umfassende Einführung der technikunterstützten Verarbeitung von Personaldaten und über den Abschluß der zugehörigen **Dienstvereinbarung** mit dem Gesamtpersonalrat gefaßt und damit die nötige Planungssicherheit hergestellt.

Ich habe die Einführung von PuMa begrüßt als Instrument, den bisherigen ‚Wildwuchs' an unterschiedlichen DV-Anwendungen und Dateien in den einzelnen Personalstellen einzuschränken und durch ein einheitliches EDV-Verfahren eine Verbesserung der Datenschutzstandards bzw. -kontrolle zu erreichen.

Reaktionen von „PuMa-Anwendern" aus der Praxis, etwa in den von der SKP angebotenen Fortbildungsveranstaltungen, deuten jedoch darauf hin, daß das neue Verfahren teilweise an den Bedürfnissen der Personalstellen vorbei entwickelt wurde. Es ist daher zu befürchten, daß einige Behörden eine dienststellenspezifische Änderung der Standard-Version verlangen werden. Ich werde nachdrücklich darauf achten, daß **keine Einzellösungen** eingeführt werden, die das beim PuMa-Verfahren erreichte Datenschutz- und Datensicherungsniveau ver-

fehlen. Die Anpassung an veränderte Nutzungswünsche und -bedingungen muß innerhalb des Verfahrens PuMa und mit den dort vorgesehenen Maßnahmen erfolgen.

Anders ausgedrückt: Die SKP ist zuständig für die PuMa-Verfahrensgestaltung und -pflege bzw. -weiterentwicklung. Dienststellenspezifische Erweiterungen können nur im Einvernehmen mit der SKP und mit Zustimmung des Gesamtpersonalrats erfolgen. Die SKP hat sich bereit erklärt, mich über Änderungswünsche rechtzeitig zu informieren.

10.1.2 Differenzierte Zugriffe

Zentrales Prinzip ist die Differenzierung der Zugriffsbefugnisse. Sie sind in den Dienststellen je nach Anwender unterschiedlich definiert: So ist es **Personalsachbearbeitern** möglich, den ganzen Datenbestand einzusehen, aber nur genau festgelegte Auswertungen zu machen. **Personalplaner** haben keine Begrenzung ihrer Auswertungsmöglichkeiten; allerdings steht ihnen hierfür nur der anonymisierte Datenbestand zur Verfügung. Während der Testphase und in den Anwenderschulungen stellte sich heraus, daß für die auf konkrete Bedienstete bezogene Personaleinsatzplanung sowohl auf den gesamten Datenbestand (lesend) als auch auf freie Auswertungsmöglichkeiten zugegriffen werden muß. Deshalb wurde eine dritte Kategorie der Zugangsberechtigung („Personalreferent") definiert.

10.1.3 Datenschutzkonzept - Beispiele für Vorkehrungen

Die o. a. Dienstvereinbarung über die technikgestützte Verarbeitung von Personaldaten und das dezentrale Verfahren zum Personalkostenmanagement und -Controlling und zur Unterstützung der dezentralen Personalverwaltung (PuMa) enthält in Ziffer 8 Regelungen zum PuMa-Einsatz. Die Anlage B enthält das Verfahrenshandbuch, das Datenschutzkonzept und das Benutzerhandbuch. Ich habe allerdings das umfangreiche Verfahrenshandbuch erst kurz vor Unterzeichnung der Dienstvereinbarung erhalten und behalte mir eine Stellungnahme dazu vor.

Den mir vorgelegten Entwurf eines Datenschutzkonzeptes habe ich kritisch durchgesehen und der SKP Hinweise zur Verbesserung gegeben. Meine Vorschläge wurden in der Mehrzahl angenommen. Dazu nur wenige Beispiele:

- Nach drei Anmeldefehlversuchen erfolgt eine Sperre durch das System, wobei eine Entsperrung nur durch die Systemverwaltung erfolgen darf und schriftlich zu dokumentieren ist.
- Ebenso habe ich nach Kenntnis der Möglichkeiten zum Datenexport aus PuMa in EXCEL oder Winword und damit der Gefahr von unzulässigen Verarbeitungsvorgängen gesperrte Diskettenlaufwerke gefordert. Die SKP ist meiner Anregung gerecht geworden, indem sie bei den Arbeitsplatzrechnern ein Schreiben auf Diskette durch Einstellung im Geräte-Setup verhindert. Sollte in Ausnahmefällen ein Schreibzugriff auf das Diskettenlaufwerk notwendig sein, so wird durch die Installation eines Verschlüsselungsprogramms eine verschlüsselte Speicherung auf den Disketten veranlaßt.
- Die Daten auf den Disketten, mit denen der monatliche Datenaustausch zwischen SKP und Dienststellen erfolgt, sind mit einem sicheren Verfahren verschlüsselt.

10.1.4 Netzsoftware und Systemverwaltung

Trotz meiner Bedenken zum Datensicherungsstandard von Windows NT 3.51 hat die SKP diese Netzwerksoftware für den PuMa-Einsatz vorgesehen. Die von mir kritisierte fehlende Abschottung der Systemverwaltung gegenüber der Protokollierung soll durch eine organisatorische Regelung zunächst für ein Jahr kompensiert werden. Die SKP übernimmt in diesem Zeitraum die Funktion der Datenbankadministration. Nur sie, nicht Mitarbeiter in den Dienststellen, ist dann berechtigt, neue Programmversionen auf die Server zu spielen. Außerdem wurde der Hersteller von Windows NT schriftlich auf die Notwendigkeit der o.a. Abschottung hingewiesen. Die Produktionsfirma hat die Realisierung dieses Features in absehbarer Zeit in Aussicht gestellt (vgl. auch o. Ziff. 9.1).

10.2 Zugangskontrolle und Arbeitszeiterfassung - Trennung statt Integration

In den für die bremischen Dienststellen verbindlichen **Grundsätzen für die gleitende Arbeitszeit** vom 29.05.1995 (Abl. Nr. 59, S. 449) ist unter Nr. 11 die Verpflichtung zur Arbeitszeiterfassung für an der Gleitzeit teilnehmende Beschäftigte geregelt. Die Arbeitszeiterfassung soll grundsätzlich elektronisch erfolgen.

Nr. 19 Abs. 2 der Grundsätze gibt vor, daß das Zeiterfassungssystem als isoliertes (stand alone) System zu installieren ist und keine Koppelung mit anderen EDV-Systemen erfolgen soll.

Ein dieser Vorgabe widersprechendes System hat die SKP eingeführt: Für die Arbeitszeiterfassung sind dort Erfassungsterminals installiert. Die **Arbeitszeiterfassung** erfolgt durch Identifizierung mittels der Karte, die auch für die **Türöffnung** verwendet werden kann. Die Erfassungsterminals sind über die hausinterne Telefonleitung mit dem Rechner verbunden, auf dem sich auch das Programm für die Türöffnung befindet. Arbeitszeit- und **Anwesenheitskontrolle** könnten also technisch gesehen kombiniert werden. Ich habe daher die Verarbeitung der beiden für unterschiedliche Personalverwaltungsaufgaben genutzten Programme auf einem Rechner in einem Schreiben an die SKP problematisiert.

Die SKP hat ihr System zur AZ-Erfassung inzwischen ohnehin gestoppt im Hinblick darauf, daß die BreKom mit der landesweiten Ausschreibung für ein Arbeitszeiterfassungssystem betraut worden ist. Ich habe mit der BreKom erste Gespräche über Datenschutzkriterien für die Systemauswahl geführt.

10.3 Ortszuschlag: Muß der private Arbeitgeber des Ehepartners genannt werden?

10.3.1 Kritik am Erklärungsvordruck

Zahlreiche Beschäftigte im bremischen öffentlichen Dienst haben sich an mich gewandt und moniert, daß die Senatskommission für das Personalwesen (SKP) zur Überprüfung der Anspruchsvoraussetzungen für die Zahlung des Ortszuschlages für Verheiratete in jedem Fall genaue Angaben über das Beschäftigungsverhältnis des Ehegatten verlangt. Insbesondere wenden sich die Beschwerdeführer dagegen, daß auch dann der Arbeitgeber genannt werden soll, wenn zweifelsfrei feststeht, daß es sich hierbei um einen **privaten** Arbeitgeber handelt. Die Betroffenen empfinden diese Offenlegungspflicht als unzulässigen Eingriff in ihre Privatsphäre.

Verkürzt ausgedrückt regeln § 40 Abs. 5 Bundesbesoldungsgesetz (BBesG) für die Beamten und die entsprechende Vorschrift des § 29 Abs. 5 Bundesangestelltentarifvertrag (BAT) für die Angestellten, daß der Ortszuschlag für Verheiratete nur zur Hälfte gezahlt wird, wenn der Ehegatte ebenfalls im öffentlichen Dienst beschäftigt ist; andernfalls wird der volle Ortszuschlag gezahlt. Eine normenklare Regelung, welche Daten der Beschäftigte zur Prüfung dieser Voraussetzungen darlegen muß, gibt es derzeit nicht. Hierzu verlangt die SKP eine Erklärung des Beschäftigten, ob und bei welchem Arbeitgeber der Ehegatte beschäftigt ist. Insbesondere sieht der Erklärungsvordruck vor, daß der Beschäftigte auch dann die genaue Bezeichnung und Anschrift des Arbeitgebers angeben muß, wenn es sich um einen privaten Arbeitgeber handelt, obwohl in diesem Fall eine Halbierung des Ortszuschlages nicht vorgenommen wird.

Ich habe der SKP gegenüber dargelegt, daß aus datenschutzrechtlicher Sicht jedenfalls dann nicht erforderlich ist, genaue Angaben über den Arbeitgeber des Ehepartners zu verlangen, wenn zweifelsfrei ein privates Arbeitsverhältnis vorliegt.

Die SKP beruft sich dagegen allgemein darauf, daß der Beschäftigte zur wahrheitsgemäßen Auskunft darüber verpflichtet sei, wo der Ehegatte beschäftigt ist und in welchem Rechtsverhältnis er steht. Hierzu habe ich der SKP geantwortet, daß sich die Erfüllung der Dienstpflicht am Grundsatz der Verhältnismäßigkeit orientieren muß.

10.3.2 Alternativen

Die SKP hatte sich inzwischen an den Bund/Länder-Arbeitskreis „Besoldung" gewandt und vorgeschlagen, anläßlich der ohnehin geplanten Neuregelung des Ortszuschlagsrechts eine normenklare **Erhebungsvorschrift** in das BBesG aufzunehmen. Der Arbeitskreis hält jedoch die derzeit vorhandenen rechtlichen Möglichkeiten für ausreichend.

Aufgrund dieser Situation habe ich der SKP vorgeschlagen, jedenfalls für die bremische Praxis die Erhebung personenbezogener Daten über dienst- und arbeitsrechtliche Verhältnisse des Ehegatten auf den erforderlichen Umfang zu beschränken. In der Erklärung zum Ortszuschlag sollte eine Rubrik eingerichtet werden, in der erklärt wird, daß der Ehepartner zweifelsfrei im nicht-öffentlichen Bereich beschäftigt ist, und zwar in Industrie oder Handel, oder daß er selbstständig ist. Alternativ könnte diese Frage in mehrere Unterfragen gegliedert werden.

Wegen durchaus möglicher Überschneidungen mit öffentlichen Stellen habe ich darauf verzichtet, den Dienstleistungsbereich (z. B. Beratungsstellen in Steuer-, Rechts- oder Sozialangelegenheiten, Versicherungen, Kreditinstitute) in diese **Differenzierung** mit aufzunehmen. Die Angabe des Arbeitgebers sollte erst in Zweifelsfällen verlangt werden und natürlich in den Fällen, in denen die Frage nach einer Beschäftigung des Ehepartners im öffentlichen Dienst bejaht wird. Außerdem habe ich die SKP gebeten darzulegen, weshalb die Frage nach der Berufsbezeichnung erforderlich ist, und gebeten, ggf. auf diese Angabe zu verzichten.

Kurz vor Redaktionsschluß hat die SKP mitgeteilt, bei der für 1997 vorgesehenen Änderung des Ortszuschlagsrechts sei eine Konkurrenzregelung in der bisherigen Form nicht mehr vorgesehen. Aus diesem Grunde habe der Bund/Länder-Arbeitskreis „Besoldung" beschlossen, bis zur Neuregelung eine meinem Vorschlag entsprechende Umgestaltung des Formblattes „Erklärung zum Ortszuschlag" z. Z. nicht vorzunehmen. Zu dieser Entscheidung habe auch die Tatsache beigetragen, daß die umfassenden Überprüfungsaktionen des vergangenen Herbstes inzwischen abgeschlossen seien. Demzufolge erwarte ich, daß dieses Formblatt **nicht mehr verwendet** wird.

10.4 Amtsarzt - Umfang von Gutachten

Ein Betroffener hat sich an mich gewandt und moniert, daß der amtsärztliche Dienst des Hauptgesundheitsamtes das Ergebnis einer zum Zwecke der Zwangspensionierung durchgeführten amtsärztlichen Untersuchung zusammen mit einer detaillierten Begründung dem Dienstvorgesetzten mitgeteilt hat.

Ich habe sowohl dem Hauptgesundheitsamt als auch dem Dienstvorgesetzten gegenüber dargelegt, daß eine derart umfangreiche Mitteilung an den Dienstherrn dem Grundsatz der Erforderlichkeit der Datenübermittlung für die Aufgabenerfüllung des Empfängers, wie er jetzt auch ausdrücklich in § 23 Abs. 4 des neuen Gesetzes über den Öffentlichen Gesundheitsdienst im Lande Bremen (ÖGDG, vgl. dazu Ziff. 7.1.2) enthalten ist, widersprach. Danach dürfen der Stelle, die die Untersuchung veranlaßt hat, nur das **Ergebnis** der Untersuchung und, soweit erforderlich, **tätigkeitsbezogene Risikofaktoren** übermittelt werden.

Beide Stellen haben inzwischen eingeräumt, daß die Weitergabe dieser Daten unverhältnismäßig war und daß sie in Zukunft die o. a. Rechtslage beachten werden.

10.5 Polizeiärztlicher Dienst - Löschungsfrist für Untersuchungsdaten

Jährlich bewerben sich bei der Bereitschaftspolizei in Bremen mehrere Hundert junge Leute um die Einstellung in den Polizeidienst. Eine der wesentlichen Einstellungsvoraussetzungen ist, daß die Polizeibewerber „polizeidiensttauglich" sind. Sie werden umfangreichen Untersuchungen durch den polizeiärztlichen Dienst unterzogen. Die Untersuchungen basieren auf der bundeseinheitlichen Polizeidienstvorschrift (PDV) 300, die einen umfangreichen Patientenfragebogen enthält.

Auf meine Frage nach der **Aufbewahrungsfrist** für die Untersuchungsdaten insbesondere der abgewiesenen Bewerber teilte der polizeiärztliche Dienst mit, sämtliche Unterlagen müßten nach der sich aus der Berufsordnung für Ärzte ergebenden Dokumentationspflicht über einen Zeitraum von zehn Jahren aufbewahrt werden, und berief sich dafür auf ein entsprechendes Schreiben der SKP aus dem Jahr 1988.

Als weitere Begründung wurde auf die Rechtsprechung des Bundesgerichtshofs hingewiesen, wonach aus dem zwischen dem Arzt und dem Patienten zustandegekommenen Behandlungsvertrag Dokumentationspflichten entstehen. Darauf habe ich erwidert, daß anläßlich einer amtsärztlichen Untersuchung mit dem Untersuchten kein Behandlungsvertrag entsteht. Der Polizeiarzt hat weder einen Auftrag noch eine Befugnis zur Behandlung festgestellter Erkrankungen.

Ich habe den polizeiärztlichen Dienst aufgefordert, die für alle bremischen Behörden geltende Bestimmung des § 22 Abs. 5 BrDSG anzuwenden und die Daten abgewiesener Bewerber unverzüglich zu löschen, sobald feststeht, daß sie nicht eingestellt werden sollen.

Die juristische Meinungsverschiedenheit ist inzwischen durch die Änderung der Rechtslage entschärft. Da die Untersuchung von Bewerbern durch den polizeiärztlichen Dienst zu den **Aufgaben des öffentlichen Gesundheitsdienstes** gehört,

unterliegt er insoweit jetzt dem Gesundheitsdienstgesetz (ÖGD) vom 27. März 1995 (Brem. GBl. S. 175; vgl. dazu Ziff. 7.1.2). Der Senator für Gesundheit beabsichtigt, in der nach § 33 Abs. 3 ÖGD zu erlassenden Rechtsverordnung auch die Löschungsfristen für die polizeiärztlichen Untersuchungsdaten festzulegen.

10.6 Beihilfestelle der SKP: Akteneinsichtsrecht der Innenrevision

Die Senatskommission für das Personalwesen (SKP) beabsichtigt, die neu eingerichtete hauseigene Innenrevision auch mit der **Vorprüfung der Beihilfeverfahren** zu betrauen. Die Innenrevision soll u. a. in unregelmäßigen Abständen eine zeitnahe einzelfallorientierte Vorgangsprüfung (Beihilfefestsetzung vor der Auszahlung) durchführen. Zu diesem Zweck sollen deren Mitarbeiter eine Zugriffsberechtigung zu den Anzeigebildschirmen des Beihilfeabrechnungssystems (vgl. dazu auch 17. JB, Ziff. 8.3) in der Produktion erhalten. Außerdem sollen ihnen bei einer Prüfungsanforderung der Beihilfeantrag, die Kostenbelege (Arztrechnungen, Rezepte usw.) und der Bescheid-Entwurf zur Verfügung gestellt werden. Bisher wurde eine stichprobenartige Vorprüfung durch andere Beihilfesachbearbeiter vorgenommen, so daß eine Offenbarung an außenstehende Bedienstete nicht stattfindet.

Nach meiner Auffassung handelt es sich bei dieser Prüfpraxis um eine unzulässige **Durchbrechung des Trennungsgebotes** nach § 93b Bremisches Beamtengesetz (BremBG). Dieses besagt nicht nur, daß die Beihilfeakte in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden soll; ausdrücklich bestimmt wird auch, daß Zugang zu den Beihilfeunterlagen nur Beschäftigte dieser Organisationseinheit haben sollen. Die SKP vertritt jedoch die Ansicht, das Trennungsgebot gelte lediglich gegenüber der Personalverwaltung, zu der die Innenrevision nicht gehöre.

Diese enge Auslegung würde aber bedeuten, daß die Beihilfesachbearbeitung auch beliebigen anderen Organisationseinheiten außerhalb der Personalverwaltung zugeordnet werden könnte. Insoweit würde die sich aus § 93b Satz 4 BremBG ergebende Zweckbindung unterlaufen. Wenn § 93b Satz 3, 2. Halbsatz BremBG den Zugang zu den Beihilfeakten ausdrücklich den Beschäftigten dieser Organisationseinheit vorbehält, soll damit sichergestellt werden, daß die Mitarbeiter des öffentlichen Dienstes insgesamt hinsichtlich der Offenbarung und Verwendbarkeit ihrer Krankheitsdaten grundsätzlich so stehen sollen wie Arbeitnehmer in der Privatwirtschaft, die ihre Krankheitskosten ja auch nicht mit ihrem Arbeitgeber, sondern allein mit ihrer gesetzlichen oder privaten Krankenversicherung abrechnen.

Ich habe aus diesen Gründen die SKP aufgefordert, von der Absicht, der externen Innenrevision eine Zugriffsberechtigung auf Beihilfedaten zu erteilen, Abstand zu nehmen. Die SKP hält meine Bedenken für nicht begründet, hat aber noch einmal ein Gespräch über die Thematik angeboten.

10.7 Unbeschränkte Auskunft aus dem Bundeszentralregister bei Bewerbungen

Auf Anfrage hat mir der Senator für Inneres mitgeteilt, nach Entscheidung der Senatskommission für das Personalwesen (SKP) könne auf die Einholung unbeschränkter Auskünfte aus dem Bundeszentralregister über Bewerber für den Polizeidienst nicht verzichtet weden.

Ich habe mich daraufhin mit der Bitte um Aufklärung und ggf. Änderung der bisherigen Handhabung in Bremen an die SKP gewandt. § 41 Abs. 1 Nr. 2 Bundeszentralregistergesetz (BZRG) regelt nämlich nicht im einzelnen, zu welchen Zwecken die obersten Landesbehörden **unbeschränkte** Auskünfte, bei denen auch bereits getilgte Eintragungen bekanntgegeben werden, einholen dürfen. Insbesondere ermöglicht eine extensive Anwendung dieser Vorschrift, daß das **Verwertungsverbot** für Tilgungen nicht hinreichend beachtet wird.

Zwar regelt § 52 Abs. 1 Nr. 4 BZRG, daß dieses Verwertungsverbot nicht gilt, wenn der Betroffene die Einstellung in den öffentlichen Dienst beantragt, doch nur unter der einschränkenden Voraussetzung, daß die Einstellung sonst zu einer erheblichen Gefährdung der Allgemeinheit führen würde. Aus dieser Vorschrift läßt sich eine generelle Anfragepraxis gerade nicht ableiten. Im übrigen hat der Senator für Inneres erklärt, ihm sei nicht bekannt, ob die Einholung einer unbeschränkten Auskunft jemals zu einer Nichteinstellung geführt hat.

Zunächst hatte die SKP mitgeteilt, daß - abgesehen von den Rechtsreferendaren und den Referendaren für das Lehramt an öffentlichen Schulen - in allen anderen

Einstellungsfällen eine unbeschränkte Auskunft eingeholt wird. Dies war nach ihrer Ansicht aus Gründen der Einheitlichkeit erforderlich, weil zwischen den senatorischen Behörden kein Konsens über eine einschränkende Handhabung hergestellt werden konnte. Diese Argumentation widerspricht aber gerade dem auf **Differenzierung** nach Beschäftigtengruppen abzielenden Abwägungsgebot des § 52 Abs. 1 BZRG (s.o.).

Ich habe daher Anfang dieses Jahres (1996) die SKP gebeten, ihre Auffassung erneut unter Beachtung des Grundsatzes der Verhältnismäßigkeit zu überprüfen. Die SKP hat zuletzt mit einem Schreiben von Anfang März 1996 an mehrere Ressorts dazu geraten, die allgemeine Überprüfungspraxis aufzugeben und nur noch das Führungszeugnis nach § 30 BZRG zu verlangen. Jetzt kommt es zunächst auf die Reaktionen der senatorischen Behörden an.

10.8 Bewerberlisten in der Presse bei der Magistratsneubildung in Bremerhaven

10.8.1 Der Fall

Im Rahmen des Verfahrens für die Wiederbesetzung der Ämter des Oberbürgermeisters und des Bürgermeisters der Seestadt Bremerhaven fertigte das Personalamt des Magistrats in Amtshilfe für den Stadtverordnetenvorsteher sog. **„Bewerberlisten"** an. Diese der besonderen Vertraulichkeit unterworfenen Listen enthielten neben den Namen der Bewerber auch Informationen über deren beruflichen Werdegang und familiäre Situation. Im Rahmen des Bewerbungsverfahrens sollten die Listen nur die Stadtverordneten, die Mitglieder des Magistrats und der Magistratsdirektor erhalten. Trotz eines schriftlichen Hinweises des Stadtverordnetenvorstehers auf die Vertraulichkeit der Unterlagen gelangten die Listen aber auch an die örtliche **Presse**, die daraufhin, noch bevor sich die kommunalen Gremien mit den Bewerbungen befassen konnten, die Namen eines Großteils der Bewerber mit persönlichen Angaben veröffentlichte.

10.8.2 Der Datenschutzverstoß

Durch den Bruch der Vertraulichkeit beim Umgang mit den Bewerberdaten sind in erheblichem Maße datenschutzrechtliche Bestimmungen verletzt worden. Auch wenn bei der Besetzung hauptamtlicher Stadtratsposten dem Informationsanspruch der Öffentlichkeit Rechnung getragen werden muß, ist das Bewerbungsverfahren doch so zu organisieren, daß neben den Rechten der Stadtverordnetenversammlung auch die **Persönlichkeitsrechte der Bewerber gewahrt** bleiben. Bewerberdaten sind besonders sensibel. Sie unterliegen bei öffentlichen Stellen dem Schutz des § 22 BrDSG i. V. m. §§ 93 ff. Bremisches Beamtengesetz.

Eine **Weitergabe von Bewerbungsunterlagen** an Dritte außerhalb des Bewerbungsverfahrens ohne Zustimmung des Betroffenen ist danach grundsätzlich unzulässig. Dies gilt für biographische oder die Privatsphäre betreffende Details auch noch dann, wenn ab einem bestimmten Zeitpunkt des Verfahrens - nachdem die kommunalen Gremien sich in ausreichendem Maße mit den Bewerbungen befassen konnten - die Bewerber der engeren Wahl in der Öffentlichkeit auch ohne ihre Zustimmung namentlich erwähnt werden können. Hinzu kommt, daß möglicherweise auch ein Verstoß gegen § 10 der Bremerhavener Stadtverfassung vorliegt, wonach die ehrenamtlich Tätigen der Stadt (z. B. Stadtverordnete, ehrenamtliche Magistratsmitglieder) wie städtische Beamte zur Verschwiegenheit (Amtsverschwiegenheit) verpflichtet sind.

10.8.3 Die Reaktion

Ich teilte meine Kritik dem Stadtverordnetenvorsteher mit und bat ihn, alle ihm möglichen Vorkehrungen zu treffen, um bei anstehenden und künftigen Bewerbungsverfahren die Vertraulichkeit beim Umgang mit den Bewerberdaten, auf die die Bewerber einen legitimen Anspruch haben, sicherzustellen. Wenn dies nicht auf andere Weise gewährleistet werden könne, müßte z.B. daran gedacht werden, den Verteilerkreis der Bewerberliste erheblich einzuschränken oder die Bewerbungsunterlagen samt Liste ausschließlich im Büro des Stadtverordnetenvorstehers bereitzuhalten und den Zugang zu ihnen einzuschränken. Auch könne daran gedacht werden, auf die Erstellung einer Bewerberliste gänzlich zu verzichten, es also beim Einsichtsrecht in die Unterlagen zu belassen. Der Hinweis auf die Vertraulichkeit der Unterlagen müsse im Hinblick auf unzulässige Offenbarungen (z.B. an die Presse oder an Parteigremien) präzisiert werden.

Der Stadtverordnetenvorsteher hat als Reaktion auf meine Kritik zwar gewisse **Einschränkungen beim Zugang zu den Bewerberunterlagen** vorgenommen (z. B. Einsicht in alle Bewerbungsunterlagen nur für Stadtverordnete und Magistratsmitglieder im Büro des Stadtverordnetenvorstehers, Übersicht/Kurzfassung nur für Stadtverordnete und Magistratsmitglieder), das grundsätzliche Problem ist jedoch noch nicht befriedigend gelöst. Bei dem nachfolgenden Bewerbungsverfahren für ein weiteres hauptamtliches Magistratsmitglied konnten vor Einstieg in das Auswahlverfahren ebenfalls wieder Namen und Berufsangaben einiger Bewerber der Presse entnommen werden.

Die Stadtverordnetenversammlung Bremerhaven ist aufgefordert, das Verfahren zur Bewerbung und Auswahl hauptamtlicher Magistratsmitglieder neu zu gestalten und dabei auch der Regelung zur Amtsverschwiegenheit der ehrenamtlich Tätigen Nachdruck zu verleihen. Dies könnte im übrigen verbunden werden mit der sich aus dem Bremischen Datenschutzgesetz (§ 16 Abs. 2) ergebenden Notwendigkeit, für vom Magistrat übermittelte personenbezogene Unterlagen „geeignete Vorkehrungen" zur Wahrung von besonderen Amts- oder Berufsgeheimnissen zu treffen („Datenschutzordnung", zur Parallelproblematik für die Bürgerschaft vgl. o. Ziff. 7.1.1.4).

11. Inneres

11.1 Polizei

11.1.1 Journalist als Sicherheitsrisiko - Auskunftsverweigerung durch die Polizei

11.1.1.1 Ablehnung des Auskunftsantrags

Ein Journalist wollte über die Feierlichkeiten zum Tag der Deutschen Einheit am 03. Oktober 1994 in Bremen berichten. Die Akkreditierung wurde ihm durch die Senatspressestelle verweigert. In der Folgezeit versuchte er, die Gründe hierfür ausfindig zu machen. Die Senatspressestelle teilte ihm mit, daß eine Akkreditierung nicht möglich gewesen sei, da die Kriminalpolizei Bremen gravierende **Sicherheitsbedenken** vorgebracht habe. Daraufhin beantragte er, ihm gem. § 34 BremPolG **Auskunft** über die zu seiner Person gespeicherten Informationen zu erteilen und ihm zu diesem Zweck Akteneinsicht zu gewähren.

Dieser Antrag wurde vom Polizeipräsidium mit dem Hinweis auf § 34 Abs. 2 BremPolG **abgelehnt.** Daraufhin wandte sich der Beschwerdeführer an mich und wies darauf hin, daß die Antragsverweigerung sein Recht auf informationelle Selbstbestimmung verletze. Er befürchte, daß ihm bei ähnlichen Veranstaltungen wieder die Akkreditierung verweigert werde und damit die Berufsausübung unmöglich gemacht werde, ohne daß er eine Möglichkeit habe, diese Maßnahme zu überprüfen und zu verhindern.

11.1.1.2 Verweigerungsgründe und Interessenabwägung

Gem. § 34 Abs. 2 BremPolG kann eine Auskunft über zu **präventivpolizeilichen** Zwecken gespeicherte Daten verweigert werden, wenn dadurch die Erfüllung der polizeilichen Aufgaben erschwert oder gefährdet würde. Auch § 19 Abs. 2 BrDSG nennt Gründe, eine Auskunft zu verweigern, soweit es sich um **strafprozessuale** Daten handelt. Die Auskunftserteilung bzw. -verweigerung ist eine Entscheidung mit **Ermessens- bzw. Beurteilungsspielraum.**

Ich habe eine Überprüfung bei der Polizei vorgenommen und festgestellt, daß die Daten, die zur Person des Beschwerdeführers gespeichert sind, eine Auskunftsverweigerung nach den o. g. Vorschriften rechtfertigen können, d.h. daß die Ablehnung innerhalb des Entscheidungsspielraums liegen kann. Allerdings habe ich Zweifel daran, ob das von der Rechtsprechung in Bremen entwickelte Gebot, in dieser Situation eine **Interessenabwägung** vorzunehmen (vgl. OVG Bremen vom 24.02.1987 - Az. 1BA50/86; BVerwG vom 21.06.1993 - Az. 1 B 62.92) ausreichend beachtet wurde. Zwar liegt eine schriftliche Begründung zur Ablehnung der Auskunft beim Polizeipräsidium vor; sie wägt aber nicht die beruflichen Interessen des Beschwerdeführers gegen die Geheimhaltungsinteressen der Polizei ab. Ein Betroffener hat bei Beeinträchtigung seiner beruflichen Tätigkeit ein gesteigertes Interesse an der Offenlegung der über ihn gespeicherten Daten; dies gilt auch und gerade für Journalisten. Insofern ist nach meiner Rechtsauffassung das Polizeipräsidium verpflichtet, **jedes** gespeicherte Datum daraufhin zu überprüfen, ob nach Interessenabwägung nicht doch eine Auskunft erteilt werden kann.

Ich habe aber auch Daten gefunden, die von vornherein einer solchen Auskunftssperre nicht unterliegen können, etwa weil sie den Betroffenen nicht als Täter

oder Verdächtigen, sondern umgekehrt als Geschädigten einer Straftat ausweisen. Insofern habe ich dem Polizeipräsidium angeraten, die Auskunft zu erteilen.

11.1.1.3 Mitteilung der Ablehnungsgründe

Darüber hinaus habe ich bei der Polizei nicht feststellen können, daß eine Entscheidung nach § 19 Abs. 4 BrDSG über die **Mitteilung der Gründe für die Auskunftsverweigerung** getroffen wurde. Zwar gehen die Vorschriften des Bremischen Polizeigesetzes den allgemeinen Vorschriften des Bremischen Datenschutzgesetzes vor, aber nur, soweit sie speziellere Regelungen treffen. Soweit § 34 Abs. 2 BremPolG mit § 19 BrDSG vergleichbare Regelungen enthält, ist die Norm in bezug auf präventiv-polizeiliche Datenverarbeitung vorrangig. § 19 Abs. 4 BrDSG kann aber neben den Auskunftsvorschriften für die Polizei angewendet werden.

Das Polizeipräsidium hat nach meinen Feststellungen in diesem Fall nicht ausreichend zwischen der Nichterteilung der Auskunft und der unterbliebenen Mitteilung der Verweigerungsgründe unterschieden. Ich habe ihm daher empfohlen, erneut zu prüfen, ob der Beschwerdeführer nicht über die Argumente für die Ablehnung informiert werden kann. Die dem Betroffenen vorenthaltenen Verweigerungsgründe sind im übrigen nach § 19 Abs. 4 Satz 2 BrDSG **aufzuzeichnen.**

11.1.2 Verwechslungsgefahr im Polizeicomputer - was tun?

Immer wieder kommt es im Rahmen der polizeilichen Fahndung zur Verwechslung von Personen. Dies trifft insbesondere Personen, deren **Name und Geburtsdatum identisch** sind mit denen einer anderen, die im INPOL-System zur Fahndung und Festnahme ausgeschrieben ist. Diese Übereinstimmung kann für den „unbescholtenen" Betroffenen zu **unangenehmen Folgen** bis hin zu dramatischen Erlebnissen führen. So sind mir Fälle bekannt geworden, in denen jemand am Flugschalter aus der Schlange herausgeholt und festgehalten wurde, oder in denen sich ein Bürger im Hotelzimmer unbekleidet Polizeibeamten mit gezogener Pistole konfrontiert sah. In einem anderen Fall wurde ein Betroffener beim Überqueren der Grenze mit Freunden mehrere Stunden aufgehalten mit der Folge, daß auch die Freunde nicht weiterfahren konnten. Ein Familienvater mußte im Zuge einer Verkehrskontrolle bis zur endgültigen Klärung der Identität warten; die gesamten Angehörigen saßen ebenfalls fest, weil nur er einen Führerschein besaß.

In diesen Verwechslungsfällen rate ich dringend, sich zunächst an den Datenschutzverantwortlichen der zuständigen Polizeidienststelle zu wenden. Mit den Spezialisten für den INPOL-Fahndungsbestand lassen sich in der Regel **weitere eindeutige Personenmerkmale** ermitteln, die dann im Computer dem **Fahndungsdatensatz hinzugefügt** werden, um eine Verwechslung von vornherein zu verhindern oder aber wenigstens eine schnellere Aufklärung zu ermöglichen. Konkret wird dann zu der gesuchten Person ein Vermerk „Nicht identisch mit . . ." gespeichert und das entsprechende Unterscheidungsmerkmal für den nicht gesuchten Bürger wird ergänzt.

Im Berichtsjahr konnte ich wieder mehrere Fälle im Zusammenwirken mit der Bremer Polizei in diesem Sinne lösen.

11.1.3 Datenaustausch zwischen Polizei und Staatsanwaltschaft - Mängel bei der Löschung

Bei der Polizei wird als Vorgangsregistrier- und -nachweissystem das Verfahren ISA (Informations-System-Anzeigen) eingesetzt. Die Staatsanwaltschaft erfaßt ihre Vorgänge in CANASTA (Centrales automatisiertes Namenskartei- und Aktenregistriersystem der Staatsanwaltschaft Bremen).

Die Polizei erfaßt jede Strafanzeige in ISA. Neu gewonnene Daten aus der weiteren Ermittlungsarbeit werden ergänzt. Damit befinden sich alle ihre Daten in der ISA-Datenbank. Bei jeder Erfassung, Nachmeldung, Zusammenführung von Personen, bei Löschung und bei Veränderung berechnungsrelevanter Daten wird vom ISA-Verfahren automatisch ein Programm zur Ermittlung der Löschfrist gestartet. Für die Datenübernahme von der Staatsanwaltschaft werden die ISA-Daten in eine Zwischendatenbank gestellt, von der aus die Staatsanwaltschaft die Daten abruft und in ihr CANASTA-System übernimmt.

Der Ausgang von Ermittlungsverfahren und der dazugehörige Tatvorwurf werden von der Staatsanwaltschaft sowohl in CANASTA als auch in ISA eingegeben. Bei ISA erfolgt nach Übermittlung des Ausgangsgrundes die Festlegung von Aufbewahrungsfristen für das Verfahren.

Durch den Datenaustausch können unnötige Doppelerfassungen von personenbezogenen Grunddaten, die sowohl in ISA als auch in CANASTA zur weiteren Bearbeitung erforderlich sind, vermieden werden. Da beide EDV-Verfahren in der ID Bremen laufen, ist der Datenaustausch dort über eine Zwischendatenbank gesichert.

Bei Prüfungen habe ich häufig festgestellt, daß sich in ISA schon **längst beendete Verfahren ohne Speicherung eines Verfahrensausgangs** befinden. Ursache hierfür sind fehlende oder keinem Verfahren zuzuordnende Ausgangsmeldungen der Staatsanwaltschaft an die Polizei. Dies kommt u. a. bei Abgabe des Verfahrens an andere Staatsanwaltschaften, bei Verbindung mehrerer Ermittlungsverfahren und bei der Mitverurteilung einzelner Täter in anderen Verfahren vor. Da sich die Fristen für die Datenspeicherung bei der Polizei vor allem an dem von der Staatsanwaltschaft übermittelten Verfahrensausgang orientieren, werde ich mich im Rahmen der Ablösung von CANASTA durch SIJUS-Straf (vgl. zu diesem Verfahren Ziff. 12.2) für eine Erweiterung der übermittelten Daten im Interesse einer verbesserten Verfahrenszuordnung in ISA einsetzen. Die Staatsanwaltschaft hat mir bereits zugesagt, daß nach Einführung von SIJUS-Straf an dieser Verfahrensergänzung intensiv gearbeitet wird.

11.1.4 Polizeiauskünfte für Verwaltungsverfahren

Ein Beschwerdeführer hatte beim Landkreis Osterholz einen Antrag auf Erteilung einer Waffenbesitzkarte und einer Berechtigung zum Munitionserwerb gestellt. Im Verwaltungsverfahren wurden auch beim Polizeipräsidium in Bremen Erkundigungen zur Überprüfung der Zuverlässigkeit des Antragstellers (vgl. § 5 i.V.m. § 30 Waffengesetz) eingeholt. Das Polizeipräsidium gab daraufhin eine **umfassende Auskunft** über die Eintragungen in der Kriminalakte und fügte darüber hinaus eine Kopie des Fernschreibens einer anderen Polizeidienststelle mit dem Hinweis über weitere Strafermittlungsverfahren bei.

Ich habe dem Polizeipräsidium daraufhin meine Auffassung mitgeteilt, daß nach § 33 BremPolG derartige Auskünfte aus polizeilichen Dateien und Unterlagen an die Waffenbehörde zwar grundsätzlich zulässig sind, gleichwohl vor der Datenweitergabe in jedem Einzelfall zu prüfen ist, ob sie für das Verwaltungsverfahren bei der anfragenden Stelle **erforderlich** ist.

Bei **Bagatelldelikten,** erst recht, wenn sie bereits lange zurückliegen, wie etwa bei Verstößen gegen das Bremische Schulgesetz oder „Schwarzfahren", sehe ich diese Voraussetzung auch für ein waffenrechtliches Verwaltungsverfahren nicht gegeben. Nicht mitzuteilen waren nach meiner Auffassung auch die Tatsache einer erkennungsdienstlichen Behandlung, die Namen der Eltern des Antragstellers, obwohl seine Identität hinreichend geklärt war, sowie von Verfahrensdaten zu einer dritten Person. Erst recht kann es nicht angehen, daß Erkenntnisanfragen anderer Polizeidienststellen ungeprüft weitergegeben werden. Insbesondere bei Angaben aus zurückliegenden Jahren muß auch der Ausgang des Ermittlungsverfahrens berücksichtigt werden.

Es ist Aufgabe der die Auskunft erteilenden Polizeibehörde, die relevanten Kenntnisse herauszufiltern und nur diese zu übermitteln. Das Polizeipräsidium hat den Vorfall zum Anlaß genommen, seine Hauptabteilungen noch einmal auf die Beachtung dieser Prinzipien hinzuweisen.

11.2 Ausländerzentralregister (AZR)

11.2.1 Verfassungsbeschwerden

Über das am 01. Oktober 1994 in Kraft getretene **Gesetz über das Ausländerzentralregister (AZR-G)** vom 02. September 1994 (BGBl I S. 2265) habe ich im 17. JB unter Ziffer 9.2.1 umfassend berichtet.

Nicht zuletzt auf die von meinen Kollegen und mir in ihren Tätigkeitsberichten geäußerten verfassungsrechtlichen Bedenken stützen sich die **Verfassungsbeschwerden,** die im September 1995 beim Bundesverfassungsgericht eingereicht wurden. Beschwerdeführer sind nicht nur ausländische, sondern auch deutsche Staatsangehörige, insbesondere Bürger mit doppelter Nationalität. Gerügt werden u.a. die Ungleichbehandlung im Vergleich mit deutschen Mitbürgern, Verstöße gegen die Zweckbindung, die Erhebung der Daten bei Dritten und die Einschränkung der Auskunftsrechte.

11.2.2 Sicherungsmängel im Verfahren

Meine **Prüfungen bei den Ausländerämtern** Bremen und Bremerhaven haben bestätigt, daß trotz der im AZR-G und in der dazu ergangenen Durchführungsverordnung vorgesehenen Datenschutz- und -sicherungsregelungen sowie -vorkehrungen das Register weiter mit dem bisherigen Altverfahren betrieben wird, das den rechtlichen Vorgaben nicht entspricht.

In diesem Altverfahren ist z. B. keine hinreichende **Protokollierung** der Abrufe und Dateneingaben gewährleistet. So kann z. B. im Nachhinein nicht mehr festgestellt werden, welcher angeschlossene Nutzer für welche Eingabe oder Datensatzveränderung verantwortlich ist. Die Paßworte werden nicht zeitabhängig gewechselt. Diese Unzulänglichkeiten werden auch von den Mitarbeitern der Ausländerämter beklagt, da sie sich ggf. Abrufe zurechnen lassen müssen, die sie selbst gar nicht veranlaßt haben.

11.2.3 Kontrolle

In meinen Kontrollrechten als Landesbeauftragter werde ich durch die derzeitige Ausgestaltung des AZR-Verfahrens nachhaltig eingeschränkt, da ich keine Möglichkeit zur Anforderung der auf bremische Abrufe bezogenen, wenn auch unvollständigen (s. o.) Protokolle habe. Wenn ich die Datenverarbeitung der bremischen Ausländerämter prüfen will, muß ich um Amtshilfe beim Bundesbeauftragten für den Datenschutz nachsuchen, um diese Protokolle zu erhalten, statt sie direkt beim Bundesverwaltungsamt (Abt. Ausländerzentralregister) anfordern zu können. Hier bestehe ich auf einer Verfahrensänderung zur **Sicherung meiner vollen Kontrollmöglichkeit.**

Zwischen dem Bundesbeauftragten für den Datenschutz einerseits und dem Bundesverwaltungsamt bzw. dem Bundesinnenministerium andererseits werden derzeit Gespräche geführt, um die genannten Probleme zu lösen.

Auf bremischer Ebene erwarte ich vom Senator für Inneres, daß er auf eine schnelle Beseitigung des gesetzwidrigen Zustandes dringt und ggf. auch die Innenministerkonferenz mit diesen Fragen befaßt.

11.2.4 Allgemeine Verwaltungsvorschrift zum AZR-G

Den vom Bundesinnenminister erarbeiteten Entwurf für eine Allgemeine Verwaltungsvorschrift zum AZR-G (AVV) hat mir der Innensenator vor wenigen Wochen zur datenschutzrechtlichen Stellungnahme übersandt. Der Entwurf in der jetzigen Fassung ist nach meiner Ansicht eher noch **weniger „datenschutzfreundlich"** als das Gesetz selbst. Einige Vorschriften sind so gefaßt worden, daß der im AZR-G noch enthaltene Ermessensspielraum für die Ausländerbehörden oder die Registerbehörde zu Lasten der Ausländer reduziert wird oder ganz entfällt. So ist z. B. die Erteilung der Auskunft mit zahlreichen Beschränkungen versehen und setzt ggf. komplizierte Rückfragen bei anderen Stellen voraus.

Ich hoffe, daß der Innensenator meine Vorschläge aufgreift und gegenüber dem Bundesinnenministerium vertritt.

11.3 Feuerwehr

11.3.1 Die „Umstände" von Unfallverletzten - Rettungsdienste versus Krankenkassen

Die Krankenkassen verlangen von der Feuerwehr im Rahmen der Abrechnung der **Krankentransporte** und der **Rettungseinsätze** umfangreiche Informationen über die Durchführung des jeweiligen Einsatzes. Erfragt werden nicht nur der Name, die Anschrift, die Krankenkasse sowie Art, Zeitpunkt und Umfang der von den Rettungsdiensten erbrachten Leistung, sondern auch die **„Umstände"**, in denen der Betroffene vorgefunden wurde. Gemeint sind damit Hinweise wie z. B. „Verletzung durch Schlägerei", „alkoholisiert" oder „Drogen"; sie sollen von den Rettungsassistenten in dem Einsatzprotokoll unter der Spalte „Ergänzende Angaben/Begründung" festgehalten werden.

Die Feuerwehr Bremen hat Bedenken gegen die Übermittlung dieser Daten und hat mich daher um datenschutzrechtliche Beratung gebeten.

Die Krankenkassen fordern diese Angaben unter Hinweis auf § 3 der im Dezember 1995 erlassenen Richtlinie über Form und Inhalt des Abrechnungsverfahrens mit den „sonstigen Leistungserbringern". Sie berufen sich darauf, diese Daten auch in der Vergangenheit von der Feuerwehr erhalten zu haben. Sie begründen die Notwendigkeit ferner damit, daß mit Hilfe dieser ergänzenden Angaben besser beurteilt werden könne, ob sie zur Kostenerstattung verpflichtet sind.

Nach § 3 der o. a. Richtlinie, die auf der Grundlage von § 302 Abs. 2 des V. Buchs des Sozialgesetzbuches (SGB V) erlassen wurde, sind (nur) die für die Leistungsabrechnung **erforderlichen** Daten von den Leistungserbringern (z. B. Optikern, Hebammen, Physiotherapeuten und eben den Rettungsdiensten) an die Krankenkassen zu übermitteln. Angaben wie z. B. Alarmierungszeitpunkt, Zeit des Erreichens des Einsatzortes, Zeitpunkt der Krankenhausaufnahme und vor allem die besonderen „Umstände" werden von den Rettungsdiensten lediglich als Nachweis eines ordnungsgemäßen Einsatzablaufs notiert und stehen in den meisten Fällen in keinem Zusammenhang mit den kassenrelevanten Leistungsdaten. Auch bestehen hohe Fehlerrisiken, insoweit subjektive Eindrücke und Annahmen des Rettungspersonals in einer besonders „stressigen" Einsatzsituation wiedergegeben werden.

Deshalb halte ich ebenso wie eine Reihe meiner Kollegen die Übermittlung dieser über die Abrechnungserfordernisse hinausgehenden Daten nicht für zulässig. Ggf. muß die Krankenkasse bei Zweifeln an ihrer Leistungspflicht den Versicherten selbst befragen. Hinzu kommt, daß bei der anschließenden Behandlung in einem Krankenhaus die Krankenkasse aus den eigenen Unterlagen den Bezug zum Rettungseinsatz herstellen kann.

Das Abstimmungsverfahren zwischen der Feuerwehr und den Krankenkassen ist noch nicht abgeschlossen. Ich werde weiter berichten.

11.3.2 Notrufaufzeichnung - keine Zweckentfremdung für Disziplinarverfahren

In der neuen Feuerwehreinsatzleitzentrale Bremens wurde eine moderne digitale **Gesprächsdatenaufzeichnungsanlage** installiert. Damit werden Fernsprech- und Funknotrufe aufgezeichnet. Grundlage dafür sind die Bestimmungen des Brandschutzgesetzes und Rettungsdienstgesetzes. Die Aufzeichnung dient ausschließlich dem Nachweis eines korrekten Einsatzes sowie ggf. für staatsanwaltschaftliche Maßnahmen bei Verdacht auf Straftaten wie z. B. Brandstiftung.

Dagegen habe ich die Verwertung der von der Notrufanlage registrierten Telefonate in einem Fall für nicht zulässig erklärt, in dem es um etwas völlig anderes ging, nämlich um die disziplinarrechtliche Bewertung einer Unterhaltung zwischen zwei Feuerwehrbeamten. Insoweit liegt keine durch § 12 Abs. 2 BrDSG zugelassene Zweckänderung vor. Das Aufzeichnungsband ist deshalb nach Ablauf der üblichen Frist von sechs Monaten zu löschen und darf nicht für diesen anderen Zweck länger aufbewahrt werden.

12. Justiz

12.1 Presse- und Öffentlichkeitsarbeit der Ermittlungsbehörden

12.1.1 Fallsituationen mit Datenschutzverstoß

Immer wieder müssen Bürger hinnehmen, daß ihre Namen oder sonstige Angaben aus ihrer Privatsphäre nach einer Straftat - sei es als Tatverdächtige, sei es als Geschädigte - bereits am nächsten Tag in den Medien veröffentlicht werden. Ein Meinungsaustausch unter den Datenschutzbeauftragten hat ergeben, daß vor allem folgende Fälle immer wieder vorkommen: Sitzungslisten werden mit den Namen der Angeklagten und dem Tatvorwurf weitergegeben, Anklageschriften oder der Anklagesatz werden vor der Hauptverhandlung der Presse bekannt, Informationen über Ermittlungsverfahren gegen Abgeordnete werden vor Aufhebung ihrer Immunität publik gemacht oder Polizei oder Staatsanwaltschaft nehmen Fernsehteams bei der Durchführung einer richterlich angeordneten Hausdurchsuchung oder von sonstigen Fahndungseinsätzen mit (sogenanntes Reality-TV).

Wie die Informationen an die Journalisten gelangen, können die von den Betroffenen eingeschalteten Datenschutzbeauftragten nicht immer aufklären. Ein wichtiger Ansatzpunkt ist dabei die Überprüfung von Praxis und Rechtsgrundlagen der **amtlichen Mitteilung personenbezogener Daten aus Strafverfahren.**

12.1.2 Verwaltungsvorschriften und gesetzlicher Regelungsbedarf

Der **Datenschutzausschuß** hat zur Unterrichtung über die Situation in Bremen in seiner Sitzung vom 20.11.1995 das Thema „Öffentlichkeitsarbeit bei der Justizverwaltung und der Polizei" behandelt. Dazu hat er Berichte des Senators für Justiz und Verfassung über die Arbeit der Justizpressestelle, die auf einer vom Generalstaatsanwalt in Abstimmung mit der senatorischen Behörde erlassenen

Anordnung beruht, und des Polizeipräsidiums über die Anordnung für den dienstlichen Verkehr der Polizei mit Presse, Rundfunk und Fernsehen aus dem Jahre 1992 entgegengenommen.

Das Spannungsfeld zwischen dem grundgesetzlich abgesicherten **Informationsanspruch der Medien** und dem **Schutz des Persönlichkeitsrechts** der von Strafverfahren Betroffenen wird ebenso wie in Bremen auch in anderen Bundesländern durch im einzelnen unterschiedliche Verwaltungsvorschriften geregelt, die über die bundesweit einheitlich geltenden Richtlinien über das Straf- und Bußgeldverfahren (RiStBV) hinausgehen. Zum Teil wird von der Staatsanwaltschaft verlangt, daß bei jeder Auskunft abgewogen werden muß zwischen dem Informationsinteresse einerseits und einer möglichen Beeinträchtigung der Unschuldsvermutung, der Persönlichkeitsrechte von Beschuldigten sowie der Verpflichtung zu einem fairen Verfahren andererseits. In manchen Länderregelungen ist der Betroffene vor einer Presseauskunft über das Vorliegen einer Anzeige oder der Einleitung von Ermittlungen zu informieren. Manche Justizministerien verbieten auch, einzelne Ermittlungsschritte oder vorläufige Wertungen des Ermittlungsstandes preiszugeben. Auf der anderen Seite finden sich Bundesländer mit Vorschriften, die weite Ermessensspielräume lassen.

Die Konferenz der Datenschutzbeauftragten hat demgegenüber festgestellt, daß für die Weitergabe bzw. Veröffentlichung von personenbezogenen Daten durch Justiz und Polizei an die Medien **Verwaltungsvorschriften nicht ausreichend** sind, sondern **bereichsspezifische gesetzliche Grundlagen** zu schaffen sind, und zwar unabhängig von der Frage, ob und inwieweit dem Bundes- oder dem Landesgesetzgeber die Gesetzgebungskompetenz zukommt. Die wichtigsten Forderungen der Datenschutzbeauftragten sind in der Konferenzentschließung vom 9./10. November 1995 zusammengefaßt (abgedr. unter Ziff. 20.15)

Ich habe diesen Beschluß dem Senator für Justiz und Verfassung im November 1995 zugeleitet. Mir geht es dabei vor allem darum, daß bis zur Schaffung gesetzlicher Grundlagen jedenfalls die einschlägigen justiz- bzw. polizeiinternen Anordnungen in Bremen (s. o.) den deutlich gewordenen Datenschutzrisiken bei der Öffentlichkeitsarbeit der Strafverfolgungsbehörden angepaßt werden. Eine Antwort steht noch aus. Auch der seinerzeitigen Vorsitzenden der Justizministerkonferenz, der Ressortchefin in Sachsen-Anhalt, habe ich die Entschließung zugesandt; sie hat mich darüber informiert, den Text an ihre Kolleginnen und Kollegen weitergegeben zu haben.

12.2 SIJUS-Straf - noch immer Datenschutzdefizite

12.2.1 Stand der Einführung

SIJUS-Straf ist zur Unterstützung der Automation des Geschäftsstellenbetriebes und der Kanzleitätigkeiten bei den Staatsanwaltschaften entwickelt worden (vgl. ausführl. 17. JB, Ziff. 10.3.). Dieses EDV-Verfahren soll z. Z. bei ca. 50 Staatsanwaltschaften des Bundesgebietes eingesetzt werden. Die Programmweiterentwicklung und -ergänzung erfolgt nach Abstimmung mit allen Anwenderländern im Anwenderkreis.

Bei der Staatsanwaltschaft Bremen werden nacheinander alle Geschäftsstellen organisatorisch und technisch auf SIJUS-Straf umgestellt. Bei der Zweigstelle in Bremerhaven wird derzeit das Verfahren in zwei Geschäftsstellen eingeführt.

12.2.2 Notwendige Datenschutz- und Datensicherungsmaßnahmen

Im Berichtsjahr habe ich in Gesprächen mit der Staatsanwaltschaft und dem Senator für Justiz und Verfassung meine Datenschutzanforderungen für den Einsatz von SIJUS-Straf, die ich bereits im letzten Jahresbericht angesprochen hatte (vgl. 17. JB, Ziff. 10.3.3.), präzisiert. Meine Beratung erfolgte trotz der Entscheidung, die Entwicklung und Einführung des Verfahrens auch ohne ausreichende gesetzliche Grundlage zu betreiben. Mir geht es dabei darum, einen angesichts der Sensibilität strafprozessualer Daten angemessenen Schutz- und Sicherungsstandard zu erreichen.

Folgende Maßnahmen sind aus meiner Sicht vorrangig zu realisieren:

- Protokollierung von Systemverwaltertätigkeiten und ausreichende Zugriffssicherungen für die Anmeldung der Systemverwaltung;
- Sperrung der Diskettenlaufwerke bei angeschlossenen PC; sofern dies nicht möglich ist, gilt als Mindestforderung eine Schreibsperre für die Diskettenlaufwerke oder eine verschlüsselte Datenspeicherung auf Disketten;

- nach wiederholt mißlungenen Anmeldeversuchen sollte durch eine automatische Sperre der Zugang zum Terminal/PC blockiert werden, bis eine Entsperrung durch die Systemverwaltung vorgenommen wird;
- Schutzmaßnahmen zur Einhaltung regionaler und strukturell differenzierter Arbeitsansätze durch Vergabe verschiedener Zugriffsrechte für die einzelnen Anwender (z. B. WirtschaftsStA, JugendStA, Dezernenten, Geschäftsstellen, Bremen/Bremerhaven);
- Verbesserung des Rückmeldeverfahrens über den Ausgang des Verfahrens an die Polizei (vgl. Ziff. 11.1.3);
- Schaffung von On-line-Anschlüssen nur im Rahmen der gesetzlichen Regelungen und
- Erstellung eines Datensicherungs-Konzepts, dessen notwendigen Inhalt ich im einzelnen aufgelistet habe.

Zurückhaltend bis ablehnend war die Reaktion auf meine Bedenken gegenüber Diskettenlaufwerken, auf die ohne großen technischen Aufwand Daten aus SIJUS-Straf kopiert werden können. Hier erwarte ich allerdings von der Staatsanwaltschaft eine der Schutzwürdigkeit der Daten entsprechende Maßnahme zur Verhinderung der Datenübertragung auf Disketten am einzelnen Terminal.

12.2.3 Datenübernahme aus dem Altverfahren CANASTA

Im 1. Quartal 1996 sollen die Daten aus dem Altverfahren CANASTA in den SIJUS-Datenbestand übernommen werden. Durch die Ablösung des CANASTA-Verfahrens ist der Datenaustausch mit der Polizei (vgl. o. Ziff. 11.1.3) neu zu gestalten, da er jetzt nicht mehr innerhalb der ID Bremen stattfindet. Obwohl diese Maßnahme unmittelbar bevorsteht, ist weder bei der ID Bremen noch bei der Polizei genau bekannt, wie der Datenaustausch in Zukunft erfolgen soll.

Ich habe den Senator für Justiz und Verfassung auf dieses Problem aufmerksam gemacht und darauf hingewiesen, daß das bisherige Verfahren erst dann aufgegeben werden kann, wenn wenigstens gewährleistet ist, daß alle dort getroffenen Datenschutz- und Datensicherungsmaßnahmen auch für das neue Verfahren SIJUS-Straf angewendet werden.

12.2.4 Datenzugriff der Generalstaatsanwaltschaft

Da bereits die Staatsanwaltschaft Bremen über eine Standleitung mit der Zweigstelle Bremerhaven verbunden ist, soll durch die Anbindung auch der Generalstaatsanwaltschaft die Ausweitung zu einem **landesweiten Informationssystem** erfolgen. Der automatisierte Datenaustausch zwischen einzelnen Staatsanwaltschaften ist nach den Vorschriften des Verbrechensbekämpfungsgesetzes nur über das bundesweite Informationssystem SISY (ausführl. dazu 17. JB, Ziff. 10.2.) vorgesehen. Solange der Datenaustausch über dieses beim Bundeszentralregister geführte Verfahren (noch) nicht möglich ist, darf er auch bremenintern nicht über den von den Vorschriften des Verbrechensbekämpfungsgesetzes zugelassenen Umfang hinausgehen.

Auch für die Wahrnehmung der Aufsichtsfunktion benötigt die Generalstaatsanwaltschaft nicht den On-line-Anschluß mit Zugriff auf alle in SIJUS-Straf gespeicherten Daten.

12.2.5 Echtbetrieb nur mit Datenschutzkonzept

Nach den mit dem Senator für Justiz und Verfassung und der Staatsanwaltschaft geführten Gesprächen habe ich meine Forderungen weiter präzisiert. Mir wurde von beiden Gesprächspartnern zugesagt, daß sie umgehend mit der Überarbeitung des bisher vorliegenden Entwurfs für ein Datenschutzkonzept beginnen werden.

Bei der Besprechung stand auch die Frage an, ab wann die **Testphase** als beendet betrachtet werden kann. Der Einsatz von SIJUS-Straf wird im **Echtbetrieb** erfolgen, sobald die Daten aus dem Altverfahren CANASTA in SIJUS-Straf übernommen (s. o. Ziff. 12.2.3) und programmtechnisch alle unnötig gespeicherten Daten gelöscht worden sind.

Bis dahin muß ein abgestimmtes **Datenschutzkonzept** vorliegen. Auch muß gewährleistet sein, daß sich die automatisierte Datenübermittlung der Staatsanwaltschaft an das System ISA der Polizei über den Ausgang der Ermittlungs- und Strafverfahren (vgl. Ziff. 11.1.3) zumindest auf dem bisherigen Stand fortsetzen läßt.

12.3 Mitteilung von Daten aus Strafverfahren an gemeinnützige Organisationen

In Strafverfahren besteht die Möglichkeit, das Verfahren gegen die Zahlung einer Geldbetrages an eine gemeinnützige Einrichtung einzustellen. Zu diesem Zweck werden von den Gerichten und der Staatsanwaltschaft **Überweisungsvordrucke** ausgehändigt, aus denen nach dem Ausfüllen Name und Kontonummer des Betroffenen sowie das Aktenzeichen des Strafverfahrens ersichtlich sind. Gehen die Zahlungsanweisungen bei den Organisationen ein, können diese - wie darüber hinaus auch die Kreditinstitute - erkennen, daß es sich bei der Überweisung nicht um eine freiwillige Spende, sondern um die Erfüllung einer **gerichtlichen Auflage** handelt. Eine Erhebung über den Zeitraum von einem Jahr hat für 1990/1991 ergeben, daß in 1.921 Fällen für 184 gemeinnützige Einrichtungen Geldbeträge zu entrichten waren.

Ich hatte den Senator für Justiz und Verfassung bereits 1991 darauf hingewiesen und darum gebeten, ein anderes Verfahren zu ermöglichen, so daß keine personenbezogenen Daten aus Strafverfahren an gemeinnützige Einrichtungen weitergeleitet werden (14. JB, Ziff. 2.3.6., s. a. 16. JB, Ziff. 6.3.). Der Datenschutzausschuß und die Bremische Bürgerschaft haben mich in diesem Anliegen unterstützt und den Senat gebeten, ein anderes Verfahren ohne unverhältnismäßigen Eingriff in das Persönlichkeitsrecht der Betroffenen zu finden (vgl. Bürgerschafts-Drucks. 13/1169, Ziff. 6.3.).

Der Senator für Justiz und Verfassung hat mich nunmehr darüber unterrichtet, daß es ihm gelungen ist, eine **Lösung** des Problems zu finden. Die aus datenschutzrechtlicher Sicht erfreuliche Regelung sieht u. a. folgendes vor:

1. Gerichte und Staatsanwaltschaft sind verpflichtet sicherzustellen, daß die Zahlungspflichtigen zwischen unmittelbarer Zahlung an die Einrichtung und Zahlung über die Landeshauptkasse an die Einrichtung wählen können.
2. Den Zahlungspflichtigen soll neben einem unmittelbaren Zahlungsweg die Möglichkeit angeboten werden, an die Landeshauptkasse zu zahlen, die die Zahlung anonym an die gemeinnützige Einrichtung weiterleitet.
3. Die Zahlungspflichtigen sind entweder über ein Merkblatt oder mit dem der Zahlungspflicht zugrundeliegendem Bescheid auf die beiden möglichen Zahlungswege hinzuweisen.

12.4 Gerichtsvollzieher: Diskretion bei Vollstreckungsmaßnahmen

Im Berichtszeitraum hat es wiederholt Beschwerden über Zwangsvollstreckungsmaßnahmen von Gerichtsvollziehern gegeben. Hierzu zählen Nachfragen bei Nachbarn über den Aufenthalt des Schuldners unter Nennung des Grundes. Weiteres Beispiel: Die Androhung einer Zwangsöffnung auf einem von dem Gerichtsvollzieher entworfenen Formblatt, das dieser ohne Briefumschlag in den Briefkasten des Schuldners geworfen hatte und das dann der über einen Zweitschlüssel verfügenden Nachbarin bekannt wurde. Auch der Einwurf einer Postkarte in den Briefkasten eines Mehrfamilienhauses hat den Zorn eines Bürgers erregt.

Weitere Fälle betrafen die offene Anbringung einer Nachricht über die Schlösserauswechslung nach einer Zwangsöffnung, die Pfändung eines PKW im Beisein einer dritten Privatperson und die Bekanntgabe der Pfändung des PKW gegenüber dem Mitarbeiter des Firmeninhabers.

In allen Fällen habe ich mich mit den Gerichtsvollziehern in Verbindung gesetzt, mir über den tatsächlichen Sachverhalt ein Bild gemacht und - soweit erforderlich und möglich - Vorschläge für eine datenschutzgerechte Praxis unterbreitet. Sie wurden durchweg akzeptiert, eine Berücksichtigung in ähnlich gelagerten Fällen wurde versprochen. So habe ich z. B. erreicht, daß Nachrichten an die Schuldner nicht mehr auf Postkarten, Klebezetteln o.ä., sondern nur noch in **verschlossenen Umschlägen** zugestellt werden. Allerdings lassen sich, und auch dies teile ich ggf. den Eingebern mit, einige Zwangsvollstreckungsmaßnahmen nicht unter Ausschluß der Öffentlichkeit oder ohne Kenntnis der Nachbarschaft durchführen.

12.5 Gerichts-Fax an den falschen Empfänger: Kündigung

Ein gerichtlich angesetzter Termin drohte zu „platzen", weil dem Anwalt einer Partei noch keine Akteneinsicht gewährt worden war. Hierauf hatte der Mandant

den Richter per Telefax hingewiesen. Daraufhin entschloß sich der Richter kurzerhand, eine Reihe von Seiten aus der Strafakte an die Fax-Adresse abzusenden, die auf der Fernkopie aufgedruckt war. Leider war diese Nummer nicht der private Fax-Anschluß des Beschwerdeführers, sondern er hatte das Gerät seines Arbeitgebers benutzt.

Der Arbeitgeber las die Auszüge aus der Strafakte seines Mitarbeiters, worauf es nach Darstellung des Beschwerdeführers zur Kündigung kam, da es auch um Wirtschaftsstraftaten bzw. Steuerdelikte ging.

Ungeachtet meiner gesetzlich beschränkten Kontrollbefugnis gegenüber Gerichten und der Tatsache, daß § 147 StPO nur eine Akteneinsicht für den Verteidiger und nicht für den Beschuldigten selbst vorsieht, habe ich den Amtsgerichtspräsidenten angeschrieben und auf die **Risiken des Telefax-Verkehrs** hingewiesen.

Der Präsident des Amtsgerichts hat den Vorfall zum Anlaß genommen, die Mitarbeiter seines Hauses auf die datenschutzrechtlichen Anforderungen bei der Benutzung von Fax-Geräten hinzuweisen. Dabei hat er unterstrichen, daß besonders sensible personenbezogene Daten, wie etwa über Personalangelegenheiten, gesundheitliche Verhältnisse, Ordnungswidrigkeiten und strafbare Handlungen, grundsätzlich nicht per Fax übermittelt werden sollten. Sollte die Übersendung derartiger Daten wegen Zeitmangels im Einzelfall nur noch per Fax möglich sein, sei darauf zu achten, daß dies nur mit Einwilligung des Betroffenen erfolge. Gesendet werden dürfe nur an ein Gerät, das der Betroffene ausdrücklich für den Empfang von Schriftstücken autorisiert habe. Auf die richtige Eingabe der Rufnummer sei ebenso zu achten wie darauf, daß die Fernkopie nur dem vorgesehenen Empfänger zur Kenntnis gelange. Im übrigen hat er auf die mit mir abgestimmten **Telefax-Regeln für die bremischen Dienststellen,** die **im Behördentelefonbuch abgedruckt** sind, hingewiesen.

13. Bildung, Wissenschaft und Kunst

13.1 Erhebungen an Schulen - Vermischung von Lehrtätigkeit, Ausbildung und Forschung

13.1.1 Evaluationsstudie zur Gesundheitsförderung

An bremischen Schulen werden zahlreiche Datenerhebungen, Untersuchungen oder wissenschaftliche Studien durchgeführt, etwa für Examensarbeiten von Studenten, für Dissertationen, für pädagogische Fragestellungen der Schulbehörden oder für Zwecke der universitären Forschung (vgl. ausführl. bereits 17. JB, Ziff. 11.1, 11.2.). Gelegentlich betätigen sich auch Lehrerreferendare im Zusammenhang mit ihrer zweiten Prüfungsarbeit für den Lehrerberuf in dieser Weise. Am Beispiel der **Evaluationsstudie zur Gesundheitsförderung** an einem Bremer Gymnasium soll erläutert werden, welche Verquickungen dabei möglich sind und wie Datenschutz an Schulen nicht realisiert werden sollte.

Ausgangspunkt für die Evaluationsstudie war ein **Unterrichtsversuch im Fach Sport,** den dieses Gymnasium in der Zeit vom 21.08.95 (Beginn des Schuljahres) bis zum 22.12.95 (Beginn der Weihnachtsferien) durchführte. Dieser Schulversuch fand in den 11. Klassen der Schule verpflichtend für alle Schüler statt. Ein der Schule zur Ausbildung zugewiesener und in der 11. Klasse im Fach Sport unterrichtender Referendar führte diesen Unterrichtsversuch zusammen mit einer Kollegin durch. Er hat über den Unterrichtsversuch auch seine Referendarsarbeit für das 2. pädagogische Staatsexamen geschrieben.

Der Unterrichtsversuch wurde begleitet von **medizinischen, sportmedizinischen und verhaltenswissenschaftlichen Datenerhebungen** bei den Schülern zu Beginn und am Ende des Unterrichtsversuchs. Die Daten sollen im Rahmen einer wissenschaftlichen Studie aufbereitet und ausgewertet werden. Die medizinische Datenerhebung erfolgte durch niedergelassene Ärzte, die sportmedizinische Datenerhebung zum Teil durch die Schüler, zum Teil durch die beteiligten Lehrer, die verhaltenswissenschaftliche Datenerhebung in Form von Fragebögen erfolgte durch die beteiligten Lehrer. Betroffen waren 46 Schüler.

Die **Eltern** der Schüler waren vorher über den Unterrichtsversuch und die sportmedizinische und verhaltenswissenschaftliche Evaluation informiert worden und hatten bis auf einen Fall die Zustimmung zur Teilnahme ihres Kindes am Unterrichtsversuch erklärt. Eine besondere **Einwilligung** zur Verarbeitung der erhobenen Daten im Rahmen der geplanten Evaluationsstudie wurde erst bei der Abschlußdatenerhebung, anfangs jedoch nicht eingeholt. Die Datenerhebungen erfolgten ohne Namensangabe der Schüler unter Verwendung einer ausgelosten Codenummer. Der Personenbezug der Daten konnte hierdurch jedoch nicht ausgeschlossen werden.

13.1.2 Kritikpunkte

Bei meiner datenschutzrechtlichen Befassung mit der Studie aufgrund mehrerer **Beschwerden** mußte ich zunächst feststellen, daß mit den Datenerhebungen bereits begonnen war, bevor die Datenschutzbelange geklärt waren. So war den Betreibern der Studie z. B. unklar, welches **Datenschutzrecht** für das betroffene Gymnasium gilt und nach welchen Regelungen sich die personenbezogene Datenverarbeitung im Zusammenhang mit der Evaluationsstudie beurteilt. Insbesondere war nicht festgestellt worden, ob das Bremische Schuldatenschutzgesetz zur Anwendung kommen mußte.

Als zweites mußte ich feststellen, daß die Erziehungsberechtigten zwar über den Unterrichtsversuch und die beabsichtigte Evaluation informiert waren und bis auf einen Fall ihre Zustimmung zur Teilnahme ihrer Kinder an dem Unterrichtsversuch erklärt hatten. Diese Teilnahmeerklärung schloß aber nicht die vom Datenschutzrecht verlangte **Einwilligung in die geplante Datenverarbeitung** für Zwecke der Evaluationsstudie ein. Für die Datenerhebungen am Ende der Studie wurde deshalb eine neugefaßte Einwilligungserklärung verwendet.

Drittens mußte ich feststellen, daß die Schule nur den Unterrichtsversuch selbst und die Nutzung der pädagogischen Erfahrungen im Rahmen der Referendarsarbeit vertreten wollte, mit der Datenerhebung und Datennutzung zu Zwecken einer wissenschaftlichen Forschungsarbeit (Evaluationsstudie) aber nichts zu tun haben wollte und konnte.

Schließlich mußte ich feststellen, daß der unterrichtende Lehrer, der Referendar in Ausbildung und der interessierte Forscher identisch waren. Aus dieser Gemengelage resultierten erhebliche Zweifel hinsichtlich der wirklich freiwilligen Teilnahme der Schüler an den Datenerhebungen für die Studie und hinsichtlich der zugesicherten Anonymität der Daten. Außerdem wird bei einer solchen Bündelung die **notwendige funktionelle Trennung** der Bereiche Schule und Forschung aufgehoben und eine zweckgebundene Verarbeitung der erhobenen Daten gefährdet.

13.1.3 Datenmaterial vorläufig unter Verschluß

Ich habe versucht, durch Hinweise und Empfehlungen das Forschungsvorhaben so zu gestalten, daß es datenschutzrechtlichen Anforderungen genügt. Bis zur Abschlußdatenerhebung im Dezember 1995 war dies nur teilweise geglückt. Deshalb habe ich von der Schule, da ihre Lehrer hier tätig waren und sie eine besondere Verantwortung für ihre Schüler hat, verlangt, das bei den beteiligten Lehrern befindliche Datenmaterial bis zur endgültigen Klärung der offenen Datenschutzfragen unter Verschluß zu nehmen. Von einer Beanstandung habe ich bisher noch Abstand genommen.

13.1.4 Erfahrungen und Konsequenzen

Aus der Erfahrung mit diesem Vorhaben müssen folgende Datenschutzüberlegungen abgeleitet werden:

- Die datenschutzgerechte Gestaltung einer Untersuchung oder wissenschaftlichen Forschung an Schulen sollte vor ihrem Beginn erfolgen. Nachträgliche Korrekturen sind mißlich und vielfach unzulänglich. Orientierung können hier die von mir erarbeiteten Merkblätter zum Datenschutz bei Forschungsvorhaben (vgl. 17. JB, Ziff. 11.3.) bzw. zum Datenschutz bei Erhebungen, Untersuchungen und Forschungsvorhaben an Schulen (vgl. 17. JB, Ziff. 19) geben.
- Erklärungen zur Teilnahme an Unterrichtsversuchen oder dergleichen sind nicht gleichzusetzen mit **Einwilligungserklärungen** zur personenbezogenen Datenverarbeitung. Das Datenschutzrecht enthält hierfür eindeutige Regelungen.
- Die Bündelung der Rollen des unterrichtenden Lehrers bzw. auch des Referendars in Ausbildung und des datenerhebenden Forschers ist problematisch. Sie gefährdet die Einhaltung der Erfordernisse der **funktionellen Trennung von Schule und Forschung**, der Unabhängigkeit der Forschung, der Freiwilligkeit der Teilnahme der Schüler sowie der Zweckbindung und Anonymität der Daten bei ihrer Verarbeitung.
- Das **Datenschutzrecht für Schulen** sollte möglichst für alle Schulträger und -typen **vereinheitlicht** werden. Derzeit ist für viele Beteiligte unklar, welches Gesetz (BDSG, BrDSG, BremSchulDSG, kirchliches Datenschutzrecht) für sie

gilt. Zudem gibt es rechtliche Unterschiede, die die Akzeptanz und Transparenz nicht gerade fördern. Dies könnte - ähnlich wie bei den Krankenhäusern - z. B. dadurch geschehen, daß man nicht nur die öffentlichen Schulen im Lande Bremen, sondern auch die unter das Privatschulgesetz fallenden Schulen in das spezifische Datenschutzgesetz für Schulen einbindet. Denkbar wäre aber auch, in das Privatschulgesetz einen Verweis auf das Bremische Schuldatenschutzgesetz aufzunehmen.

13.2 Wohnsitzüberprüfung bei Schülern - was ist die Meldebestätigung wert?

13.2.1 Polizist überprüft Hauptwohnsitz von Schülereltern

Durch eine Eingabe erfuhr ich, daß der Senator für Bildung, Wissenschaft, Kunst und Sport in Fällen, in denen für die Zuweisung eines Schülers zu einer öffentlichen Schule bei mehreren Wohnsitzen der **Hauptwohnsitz** maßgeblich ist und die senatorische Dienststelle den von den Schülern bzw. deren Erziehungsberechtigten gemachten Angaben keinen Glauben zu schenken vermag, über die Meldebehörde sog. **„Wohnsitzfeststellungsprüfungen"** durchführen läßt.

Es reicht der Schulbehörde in diesen Fällen angeblich nicht aus, auf Informationen, die ihr von der Meldebehörde nach § 30 Abs. 1 Bremisches Meldegesetz (BremMeldG) bzw. nach § 10 Abs. 1 Bremische Meldedatenübermittlungsverordnung (BremMeldDÜV) übermittelt wurden (z.B. Hauptwohnsitz des Schülers) oder auf amtliche Dokumente, die ihr von Schülern bzw. deren Erziehungsberechtigten zur Bestätigung ihrer Wohnsitzangaben vorgelegt wurden, zurückgreifen zu können. Da die Meldebehörde selbst über keinen eigenen Ermittlungsdienst verfügt, läßt sie die Überprüfungen von den Bezirksdiensten der örtlich zuständigen Polizeireviere durchführen.

In dem mir durch die Eingabe bekannt gewordenen Fall hatte sich der Vater des betroffenen Schülers insbesondere darüber beklagt, daß der uniformierte Polizeibeamte des zuständigen Reviers sich auch in der Nachbarschaft über ihn und seine Familie erkundigt hatte. Die Nachbarn hätten somit einen falschen Eindruck gewonnen, der das Ansehen seiner Familie erheblich beeinträchtige.

13.2.2 Kontroverse Rechtspositionen

Der Senator für Bildung, Wissenschaft, Kunst und Sport begründet das dargestellte Verfahren damit, daß bestehende melderechtliche Festsetzungen (Hauptwohnung, Nebenwohnung) für die Zuweisung eines Schülers zu einer Schule allein nicht ausreichend seien. Um den Bestimmungen des Schulrechts entsprechen zu können, müsse es ihm möglich sein, bei begründeten Zweifeln die Wohnsitzangaben des Schülers überprüfen zu können. Da er diese Überprüfungen nicht selbst vornehmen könne, sei er auf die Amtshilfe der Meldebehörde angewiesen. Gem. § 21 BremMeldG sei diese berechtigt, das Melderegister von Amts wegen fortzuschreiben, wenn sich gespeicherte Daten geändert haben oder wenn neue oder weitere Daten zu speichern seien. Bei der Wahrnehmung dieser Aufgabe bediene sich die Meldebehörde der Hilfe der Bezirksdienste der Polizeireviere.

Die Begründung des Senators für Bildung, Wissenschaft, Kunst und Sport halte ich für unzutreffend. Die Schulbehörde hat bei ihrer schülerbezogenen Datenverarbeitung neben den Bestimmungen des Schulrechts vor allem die des Gesetzes zum Datenschutz im Schulwesen zu beachten. Keine dieser Bestimmungen sieht Datenerhebungen der Schulbehörde (als Teil der Datenverarbeitung) bei anderen Behörden vor. Auch eine Befugnis, selbständig Ermittlungen durchführen zu können, hat die Behörde nicht. Zweifel an den Wohnsitzangaben eines Schülers können deshalb nur mit Hilfe eigener Unterlagen der Behörde, die z. B. die nach 10 Abs. 1 BremMeldDÜV übermittelten Daten enthalten, oder anhand amtlicher Dokumente, z. B. Melde- oder Wohnsitzbescheinigung bzw. Ausweis, ausgeräumt werden. Denkbar wäre auch eine aktuelle individuelle Melderegisterauskunft auf der Basis von § 30 Abs. 1 BremMeldG, in deren Rahmen evtl. die auf tatsächlichen Anhaltspunkten beruhenden Zweifel an den Wohnsitzangaben des Schülers der Meldebehörde mitgeteilt werden könnten (§ 11 Abs. 1 Gesetz zum Datenschutz im Schulwesen). Maßgebend ist aber in jedem Fall das, was die **Meldebehörde** amtlich dokumentiert bzw. nachweist.

Der Senator für Bildung, Wissenschaft, Kunst und Sport will sein Verfahren zur Wohnsitzfeststellungsprüfung überdenken und Vorschläge zu einer Veränderung unterbreiten. Er beharrt allerdings auf seiner Auffassung, daß auch er nach Schul- und Melderecht derartige Überprüfungen veranlassen könne und daß die melderechtlichen Festsetzungen für schulrechtliche Entscheidungen (Zuordnung eines Schülers zu einer öffentlichen Schule) nicht allein entscheidend seien.

14. Gesundheit, Jugend und Soziales

14.1 Wirtschaftlichkeit sozialer Dienste und Einrichtungen versus Beratungs- und Sozialgeheimnis?

14.1.1 Gegenläufige Entwicklungen in der Gesetzgebung

Wie in Zeiten der Krise öffentlicher Finanzen und der Privatisierung öffentlicher Dienstleistungen nicht anders zu erwarten, werden auch im Bereich kommunaler Sozialarbeit, d. h. der Kinder-, Jugend- und Sozialhilfe, neue Steuerungsmodelle wie Controlling, Budgetierung und dezentrale Ressourcenverwaltung propagiert und implantiert. Nicht zuletzt mit Hilfe automatisierter Verarbeitung von zusätzlichen und signifikanteren Daten soll der Mittelabfluß transparent gemacht und mit weniger Ressourcen effizienter gearbeitet werden.

Gegen diese Zielsetzung ist aus Datenschutzsicht, das versteht sich von selbst, nichts einzuwenden. Wachsamkeit ist jedoch deshalb geboten, weil allzuleicht die Belange der Klienten aus dem Blickfeld geraten. In diesem Zusammenhang besteht auch die Gefahr, daß **Sozial- und Beratungsgeheimnis** zu ihren Lasten, aber auch zu Lasten der inhaltlichen Zielsetzungen der Sozialarbeit ausgehöhlt werden. Allerdings hat der Gesetzgeber in den vergangenen Jahren die Anforderungen an die Fachlichkeit von Sozialarbeit, zugleich auch die **Rechtsposition des Datenschutzes gestärkt:**

- Seit 1991 dürfen Mitarbeiter von Trägern öffentlicher Jugendhilfe die Daten, die ihnen Klienten zum Zwecke persönlicher und erzieherischer Hilfe anvertraut haben, nach Maßgabe des § 65 KJHG nur mit deren Einwilligung oder aufgrund gesetzlicher Befugnis anderen gegenüber offenbaren - und dies gilt auch innerhalb ihrer Dienststelle.
- Der Träger der öffentlichen Jugendhilfe hat nach § 61 Abs. 4 KJHG sicherzustellen, daß dieser besondere Vertrauensschutz auch bei Einrichtungen und Diensten der Träger der freien Jugendhilfe gewährleistet ist, soweit er diese in Anspruch nimmt, d. h. sie bezuschußt und sich so davon entlastet, die geförderten Leistungen selbst erbringen zu müssen.
- Mit der Neuregelung des Sozialdatenschutzes in 1994 ist in § 35 SGB I das Sozialgeheimnis um die Verpflichtung erweitert worden, auch innerhalb des Leistungsträgers sicherzustellen, daß Sozialdaten nur Befugten zugänglich sind und nur an diese weitergegeben werden.

In einem gewissen **Spannungsverhältnis** dazu stehen Regelungen

- wie § 67c Abs. 3 SGB X, wonach Sozialdaten, soweit erforderlich, für Zwecke der Aufsicht, der Kontrolle, der Rechnungsprüfung und von Organisationsuntersuchungen genutzt werden dürfen,
- und wie § 93 Abs. 2 BSHG, der die öffentlichen Träger der Sozialhilfe verpflichtet, mit den nicht-öffentlichen Trägern von Einrichtungen Pflegesatzvereinbarungen zu treffen, die eine Prüfung von Wirtschaftlichkeit und Qualität der Leistungen ermöglichen.

Meine Erfahrungen gerade im Berichtsjahr zeigen, daß Effizienz und Sparsamkeit einerseits und Datenschutz und Beratungsgeheimnis andererseits durchaus miteinander zu vereinbaren sind. Dies verwundert nicht, ist doch sowohl der Sozialarbeit als auch dem Datenschutz die Aufgabe gestellt, die Autonomie der Klienten sozialer Dienste und Einrichtungen zu stärken.

14.1.2 Schutz des Beratungsgeheimnisses innerhalb des Amtes für Soziale Dienste Bremen (AfSD) - Ende gut, alles gut?

Nicht zuletzt zu Aufsichts- und Kontrollzwecken hat die **Wirtschaftliche Jugendhilfe** als die Stelle, die im Einzelfall über die Gewährung kostenwirksamer Maßnahmen der Jugendhilfe - etwa einer Heimunterbringung oder den Einsatz einer Familienhelferin - entscheidet, seit jeher für sich in Anspruch genommen, ihrer Entscheidung alle die Unterlagen zugrunde zu legen und zu ihren Fallakten zu nehmen, die bereits der **ambulante Sozialdienst** für seinen Entscheidungsvorschlag genutzt und zu seinen Akten genommen hat.

Die Berichterstattung über mein Bemühen, dieses rechtlich fragwürdige Übermaß an Datenverarbeitung zu beseitigen, durchzieht meine Jahresberichte der vergangenen sieben Jahre. Zuletzt hatte ich unter Ziff. 12.3.6 meines 17.JB darüber berichtet, daß im Mai 1994 mit mir abgestimmte Dienstanweisungen in Kraft gesetzt worden seien, die einen vom ambulanten Sozialdienst nach Vordruck zu

erstellenden **Hilfeplan** zur alleinigen Grundlage der Kostenentscheidung der Wirtschaftlichen Jugendhilfe machten und damit den innerdienstlichen Datenfluß unter Beachtung des Beratungsgeheimnisses auf das erforderliche Maß begrenzten. Ich hatte weiter mitgeteilt, daß eine Prüfung aber gezeigt habe, daß dies in der Regionalabteilung Ost des AfSD bis Ende 1994 noch nicht ausreichend umgesetzt worden sei. Inzwischen hat diese aber, damit auf meine formelle datenschutzrechtliche Beanstandung reagierend, mitgeteilt, man habe die als Stichproben gezogenen Akten im geforderten Umfang bereinigt.

Im Berichtsjahr habe ich bei **Prüfungen** in den anderen Regionalabteilungen Süd, Mitte/West und Nord des AfSD festgestellt, daß die nach dem Zufallsprinzip gezogenen **Fallakten** der Wirtschaftlichen Jugendhilfe seit dem Mai 1994, dem Zeitpunkt des Inkrafttretens der **Dienstanweisungen**, durchweg nur noch Unterlagen enthalten, die für die Kostenentscheidung tatsächlich benötigt werden. Die Doppelspeicherung von medizinischen Gutachten, psychosozialen Diagnosen und Entwicklungsberichten ist beseitigt. Offensichtlich hat man das zur Umsetzung der Dienstanweisungen Erforderliche veranlaßt.

In den Gesprächen mit Sachbearbeitern der wirtschaftlichen Jugendhilfe habe ich keine Klagen darüber gehört, daß Informationsmängel sie daran hinderten, ihre Aufgaben zu erfüllen. Was ich gehört habe, ist die Klage von Sozialarbeitern/Sozialarbeiterinnen über Mehrarbeit, aber auch die Feststellung, ihre Arbeit sei durch die formale Verpflichtung, die Grundlagen für die Kostenentscheidung aus ihrer fachlichen Zuständigkeit heraus eigenverantwortlich - in Kooperation mit Kindern, Jugendlichen und deren Eltern - zu erstellen, professionalisiert worden. Eine andere Frage ist, ob die derzeit genutzten Vordrucke nicht entbürokratisiert werden können.

Ich habe dem Jugendressort gegenüber die Erwartung ausgesprochen, an der **Überarbeitung** der Dienstanweisungen und der Vordrucke genauso beteiligt zu werden, wie es bei deren Erarbeitung der Fall war. Kurz vor Redaktionsschluß dieses Berichts hat mir das AfSD die Entwürfe für eine geänderte Dienstanweisung und für neue Vordrucke zur Stellungnahme zugeleitet, die allerdings wieder neue Fragen aufwerfen.

Die - noch von der vorigen Senatorin in Aussicht gestellte - Befassung in der zuständigen Fachdeputation bzw. im Jugendhilfeausschuß soll nach Aussage der zuständigen Abteilung in der senatorischen Dienststelle im Frühjahr 1996 mit meiner Beteiligung stattfinden. Der Datenschutzausschuß hat das Ressort gebeten, ihm bis zum 30. Juni 1996 über das Ergebnis der Prüfung zu berichten.

14.1.3 Wirtschaftlichkeitsprüfung bei freien Trägern mit klientenbezogenen Daten - eine stete Versuchung?

Würde ein Sozialhilfeträger - sei es auf der Grundlage einer Prüfvereinbarung nach § 93 Abs. 2 BSHG, sei es unter Androhung finanzieller Sanktionen - zum Zwecke der Prüfung von Wirtschaftlichkeit und Qualität subventionierter Leistungen routinemäßig und anlaßunabhängig Klientendaten bei in freier Trägerschaft arbeitenden Einrichtungen der Sozialhilfe erheben und auf Dauer speichern, so wäre dies sicher eine Aufforderung zur Verletzung beruflicher Schweigepflichten und eine Beeinträchtigung schutzwürdiger Belange der betroffenen Klienten. Folge wäre es, daß zentrale Dateien entstünden, in denen höchst sensible Daten von Klienten gesammelt würden, die z. T. gesellschaftlich diskriminierten Randgruppen angehören. Derartige Datensammlungen wecken Begehrlichkeiten auf Nutzung zu unterschiedlichsten Zwecken und auf unbestimmte Zeit. Derartiges von vornherein zu verhindern, habe ich mich wiederholt bemüht (vgl. 17.JB, Ziff. 12.3.7.1.).

Inzwischen habe ich vom Magistrat **Bremerhaven** die beruhigende Aussage erhalten, daß sich das dortige Sozialamt in **Pflegesatzvereinbarungen** lediglich das Recht ausbedinge, aus begründetem Anlaß die zur Überprüfung notwendigen Unterlagen und Auskünfte zu erhalten. Vorbehaltlich einer Präzisierung von Umfang und Dauer von Erhebung und Speicherung und der Vorkehrungen zur Einhaltung der Zweckbindung ist dagegen nichts einzuwenden.

Der Senat hat in seiner Stellungnahme zu meinem 17. Jahresbericht seine Bereitschaft erklärt, mein Angebot aufzugreifen, mich an der Ausgestaltung der **Prüfvereinbarungen** zu beteiligen, allerdings unter dem Vorbehalt, zuvor sei abschließend zu klären, welche Anforderungen an seine Dokumentations- und Berichtspflichten, insbesondere vom Rechnungshof, gestellt würden. Dem habe

ich entgegengehalten, daß auch für die Rechnungsprüfung nur die rechtlich zulässig ohnehin zur Aufgabenerfüllung gespeicherten Daten zur Verfügung stünden. Ich habe daraus den Vorschlag abgeleitet, mich bereits vor abschließender Klärung der Anforderungen des Rechnungshofs an der Vorbereitung der Prüfvereinbarungen zu beteiligen. Der **Datenschutzausschuß** hat das Ressort um **Berichterstattung** zum gegebenen Zeitpunkt gebeten (vgl. Bürgerschafts-Drucks. 14/210, zu 17. JB, Ziff. 12.3.6.). Inzwischen gibt es ein Gesprächsangebot des Ressorts.

Eine Eingabe des Datenschutzbeauftragten des Diakonischen Werks hat Aktualität und Brisanz der Thematik unterstrichen. Danach hatte das Sozialressort zu Planungszwecken unter Androhung finanzieller Sanktionen vom Diakonischen Werk Bremen als Träger eines Übergangswohnheims für **Obdachlose** verlangt, eine Fülle von Daten zu übermitteln, z. B. Wartelisten einschließlich der Bedarfsnachweise, Indikation und Hilfeplanung der Betreuungsfälle während eines bestimmten Zeitraums. Inzwischen hat auf meine Intervention hin das Sozialressort seine Anforderung durch den Zusatz ergänzt, man erwarte zwar die Übermittlung von Daten, aus denen sich der Umgang mit Einzelfällen erkennen läßt. Die betroffenen Klienten sollten allerdings nicht identifizierbar sein.

14.2 Mietwucher bei Wohnungen für Sozialhilfeempfänger und Flüchtlinge - Datenschutz als Kontrollhindernis?

Wird in den Medien berichtet, der Datenschutz hindere eine Behörde am gebotenen Handeln, so sollte man das nicht immer für bare Münze nehmen.

Ein Beispiel: Im August 1995 berichtete die örtliche Presse, es sei nicht selten, daß ein und dieselbe Wohnung dem Sozialamt gleich **mehrfach vermietet** wird. Den Vorteil hat allein der geldgierige Vermieter, die Nachteile zusammengepferchte Flüchtlinge oder andere Sozialhilfeempfänger, die Steuerzahler und die Nachbarn, letztere wegen der bau- und feuerpolizeiwidrigen Zustände bei Überbelegung von Wohnraum.

All dies zu verhindern ist die gesetzliche Aufgabe des Sozialressorts. Es gilt, ein Verfahren zu entwickeln, das Doppelvermietung effektiv und einfach verhindert, zugleich aber nicht alle, die Wohnungen für Asylbewerber und Sozialhilfempfänger vermieten, zu des Mietwuchers Verdächtigen abstempelt. Genau dies aber wäre der Fall, wenn diese Vermieter zwecks Überprüfung auf Dauer in einer Datei gespeichert würden.

Dies ist aber auch gar nicht erforderlich. Ein **automatisierter Abgleich** der ohnehin schon über **PROSOZ** (dazu Ziff. 14.3) gespeicherten Vermieter und Wohnungen könnte es erlauben, bei Auffälligkeiten einzelne Wohnungen zu überprüfen, zugleich aber sicherstellen, daß die durch den Abgleich gewonnenen Daten im übrigen unverzüglich automatisiert gelöscht werden.

In der Berichterstattung aus der Sitzung der Bremischen Bürgerschaft am 07.09.1995 hieß es, ich hätte Bedenken gegen einen Datenabgleich. Das Gegenteil war aber der Presse schon am 19.08.1995 zu entnehmen gewesen. Überdies hatte ich bereits mit Schreiben vom 21.08.1995 dem Sozialressort meine Unterstützung angeboten. Am 26.09.1995 fand daraufhin eine Besprechung zwischen Amt für Soziale Dienste, Bauordnungsamt und einem Vertreter meiner Dienststelle statt, auf der man sich über die gebotenen und zulässigen Schritte einig war. Das Sozialressort hat aber bis Redaktionsschluß dieses Jahresberichts noch keinen **Verfahrensvorschlag** vorgelegt.

14.3 PROSOZ-Verfahren - Umsetzung des überarbeiteten Datenschutzkonzeptes in die Praxis

14.3.1 Prüfkriterien

In meinem 16. JB habe ich unter Ziff. 8.7.2 darüber berichtet, daß ich bei einer datenschutzrechtlichen Prüfung Funktionserweiterungen des dialogorientierten Verfahrens zur Berechnung der Sozialhilfe „PROSOZ" festgestellt hatte. Eine Anpassung der ursprünglichen Datenschutzkonzeption im Zusammenhang mit der Installation entsprechender Datensicherungsfunktionen war nicht erfolgt.

Inzwischen lag eine an die **Weiterentwicklung** des Systems angepaßte Datenschutzkonzeption vor (vgl. Ziff. 12.3.1 meines 17. JB), deren Umsetzung ich an einzelnen Arbeitsplätzen und in der ADV-Verbindungsstelle im Berichtsjahr hinsichtlich folgender Inhalte geprüft habe:

1. Umfang der MS-Windows-Installation auf den PROSOZ-Rechnern,
2. Umsetzung der Dienstanweisung des Sozialressorts für den Umgang mit PROSOZ, MS-Windows und MS-Word,
3. Verfahren der Änderung von Organisationsschlüsseln für Einzelfälle oder Gruppen,
4. Verfahren der automatischen Dunkelschaltung für die Arbeit mit MS-Windows bzw. MS-Word,
5. Überwachung der Dienstanweisung für den Umgang mit PROSOZ, MS-Windows und MS-Word durch den Datenschutzbeauftragten des Sozialressorts,
6. Tätigkeit des Datenschutzbeauftragten für den Bereich Wirtschaftliche Hilfen,
7. Einzelfallbearbeitung durch die ADV-Verbindungsstelle,
8. Testverfahren für neue Programmversionen und
9. Zugriffsschutz auf Diskettenlaufwerke an DKR (Dienststellenkoordinations)- und Sachbearbeitungsplätzen.

14.3.2 Fehlende Vorkehrungen

Die Umsetzung der neuen Datenschutzkonzeption ist **teilweise** erfolgt, wie z.B. die Änderung der Paßwortorganisation bei der ADV-Verbindungsstelle, von der aus durch die Nutzung des Programms RACF keine Einsicht mehr in die Paßworte vorgenommen werden kann.

Folgende Punkte sind bisher nicht realisiert worden bzw. müssen aufgrund der neuen Konzeption zusätzlich berücksichtigt werden:

- Zuleitung der automatisch erstellten Belege der Übernahme von Zugriffsberechtigungen durch die ADV-Verbindungsstelle an die betroffenen Sachbearbeiter/innen,
- Reduzierung der MS-Windows-Funktionen um den Dateimanager und die Systemsteuerung an den Sachbearbeitungsarbeitsplätzen,
- Sicherstellung der Einhaltung der Löschfristen in bezug auf PROSOZ-Daten verarbeitende Texte sowie ihre Trennung (auf Verzeichnisebene) von Texten mit anderen Inhalten,
- Konfigurierung der Rechner gem. Ziff. 4.8.1 des Datenschutzkonzeptes, in der die Abschaltung des Bildschirmes durch Aktivierung des Bildschirmschoners von MS-Windows sowie ein diesbezüglicher Paßwortschutz vorgesehen sind,
- Durchführung von stichprobenartigen Kontrollen durch den Datenschutzbeauftragten der senatorischen Dienststelle und Vorlage der Unterlagen über bereits durchgeführte Stichproben,
- Bestellung eines Datenschutzbeauftragten für den Bereich Wirtschaftliche Hilfen und
- Sperrung der Diskettenlaufwerke, auch an den Arbeitsplätzen der Dienststellenkoordinator/innen, soweit Daten aus der Fallsachbearbeitung auf den Rechnern verarbeitet werden und Einrichtung einer außerhalb dieses Arbeitsbereiches liegenden Systemverwaltung.

Ich stelle diese Datensicherungsfragen mit voller Absicht so ausführlich dar, sind sie doch prototypisch für Anforderungen in besonders sensiblen Verarbeitungsbereichen. Und: Bei allem, was erreicht worden ist, ist es nur unzureichend gelungen, die insbesondere durch die Integration von Textverarbeitungsfunktionen entstandene **Sicherheitslücke** im Bereich des technischen Datenschutzes durch eine entsprechende Dienstanweisung zu kompensieren.

Bisher habe ich noch keine Antwort zum Stand der vollständigen Umsetzung der o.g. Maßnahmen erhalten.

14.4 Schwangerschaftsabbruch - Schutz der Vertraulichkeit bei der Kostenübernahme

Bis zum 31.12.1995 wurden im Lande Bremen die Kosten von straffreien Schwangerschaftsabbrüchen von den **Sozialämtern** übernommen. Auf meine Fragen nach dem Schutz der Vertraulichkeit im Antrags- und Entscheidungsverfahren (vgl. 17. JB, Ziff. 12.2.2.2.) haben mir die Sozialhilfeträger zufriedenstellende Antworten gegeben.

Seit 01.01.1996 müssen aufgrund des inzwischen in Kraft getretenen Schwangeren- und Familienhilfeänderungsgesetzes die Schwangeren die Kostenübernahme bei den **gesetzlichen Krankenkassen** beantragen, die ihrerseits wiederum mit den Trägern der Sozialhilfe abrechnen. Im gesamten Verfahren - so das Gesetz - ist das Persönlichkeitsrecht der Frauen unter Berücksichtigung der besonderen Situation der Schwangerschaft zu achten. Daraus habe ich Krankenkassen und Sozialhilfeträgern gegenüber den Schluß gezogen, daß

— die Datenverarbeitung möglichst zu minimieren ist, um den **Eingriff in die Privatsphäre der Frauen möglichst gering** zu halten,

— die gespeicherten Daten nur für den Zweck der Gewährung der gesetzlichen Leistungen vorgehalten und genutzt, d.h. die Daten nicht mit anderen Daten zusammengeführt werden dürfen, eine Nutzung und Zweckänderung durch technische und organisatorische Vorkehrungen ausgeschlossen und die Daten nach Erreichung des erlaubten Zwecks unverzüglich gelöscht werden müssen und

— die Krankenkassen den Trägern der Sozialhilfe im Wege der Abrechnung keine personenbezogenen Daten über Schwangere übermitteln dürfen.

Bei Redaktionsschluß waren die Vorbereitungen für die gesetzlich angeordnete Umstellung noch nicht abgeschlossen, meine Vorstellungen von den beteiligten Stellen aber im Grundsatz akzeptiert worden. Die **Krankenkassen** wollen nur ein Minimum an Daten bei der Antragstellung erheben, auf ihrer Grundlage zur Vorlage an die Ärzte eine Kostenübernahmeerklärung ausstellen, die erhobenen Daten ohne Personenbezug dem Sozialhilfeträger zuleiten und nach Kostenerstattung durch diesen ihren Datensatz löschen. Die **Ärzte**, die den Schwangerschaftsabbruch vornehmen, sollen ihrerseits über die **Kassenärztliche Vereinigung** abrechnen, die die Daten ohnehin nur kurzfristig speichert und durch § 295 SGB V gehalten ist, die Abrechnungsdaten nicht auf die einzelnen betroffenen Frauen bezogen an die Krankenkassen zu übermitteln.

14.5 Schulfahrten und Sozialgeheimnis

Seit jeher sind Schulfahrten große Erlebnisse für die Schüler. Ihnen wird ein hoher pädagogischer und sozialer Stellenwert beigemessen. Deshalb sollen möglichst alle Schüler einer Klasse an ihnen teilnehmen, auch die Schüler, deren Eltern die Kosten nicht aus eigenen Mitteln aufbringen können. Sie können deshalb hierfür einen **Zuschuß von der Sozialhilfe** beantragen.

Ging die Fahrt in ein Bremer Schullandheim, so mußten die Eltern bislang - darauf hatten sich Bildungs- und Sozialressort für die Schulen der Stadtgemeinde Bremen geeinigt - ein **Formblatt** vorlegen, auf dem Schulleitung oder Klassenlehrer/in die erstattungsfähigen Kosten der Fahrt aufschlüsselten. Hatte die Fahrt ein anderes Ziel, so mußten die Eltern sich auf einem anderen Formblatt die Kosten und zusätzlich Zweck, Ablauf und inhaltliche Schwerpunkte bescheinigen lassen und die Zustimmung der **Schulleitung** beibringen.

Jedenfalls waren Schüler bzw. Eltern gezwungen, die Schule um Ausstellung der Formulare zu bitten und die Tatsache offenzulegen, daß sie diese zur Beantragung von Sozialhilfe benötigten. Überdies bestand die Gefahr, daß Eltern deshalb ihre Kinder von der Teilnahme an der Fahrt abhielten.

Dabei bestand gar keine Notwendigkeit für den damit verbundenen **Eingriff in das Sozialgeheimnis** der Betroffenen. Beschwerdeführende Eltern hatten mir ein Schreiben gezeigt, in dem die Klassenlehrerin ohnehin allen Eltern fast sämtliche sozialhilferelevanten Daten mitgeteilt hatte. Folglich schlug ich vor, künftig die Lehrer und Lehrerinnen zu veranlassen, in ihre Schreiben, mit denen sie alle Eltern über die Modalitäten einer Klassenfahrt informieren, von vornherein die für die Sozialhilfe erheblichen Angaben aufzunehmen. Diese Schreiben könnten dann bei der Beantragung von Sozialhilfe vorgelegt werden.

Bildungs- und Sozialressort haben erfreulich schnell und positiv reagiert und **Formblätter für Elternrundschreiben** verbindlich vorgeschrieben, die auch zur Beantragung der Kosten bei den Sozialämtern benutzt werden können. Die Neuregelung soll dem Vernehmen nach von einzelnen Lehrern als zu bürokratisch kritisiert worden sein. Dabei sollte aber nicht vergessen werden, daß sie den Schutz des Persönlichkeitsrechts sozialhilfebedürftiger Eltern und Schüler gewährleistet und ihnen einen Behördengang erspart.

15. Arbeit

15.1 Automatisierung der Datenverarbeitung im Gesundheitswesen - Entwicklungen und Risiken

15.1.1 Ende des Patientengeheimnisses oder neuer Gesundheitsdatenschutz?

Zu den persönlichsten und heikelsten Daten eines Menschen gehören die über seine Gesundheit bzw. seine Krankheiten. Die **ärztliche Schweigepflicht** soll es dem Patienten erleichtern, seinem Arzt, bei dem er Heilung oder Linderung sucht, seine Beschwerden anzuvertrauen. Liegen die Voraussetzungen hierfür überhaupt noch vor?

Schlagworte wie **Patientenchipkarten**, Privatliquidation ärztlicher Honorare über **Verrechnungsstellen**, Übergabe von Patienten an den **Praxisnachfolger**, Angabe ärztlicher Diagnosen auf **Abrechnungsunterlagen, Qualitätskontrollen** durch administrative Instanzen, **Codierung** von Diagnosen und **„shared care"** durch Experten verschiedener Fachrichtungen illustrieren, in welchem Maße die Vertraulichkeit zwischen Patient und Arzt bereits aufgehoben ist.

Gesetzgeber und Gerichte haben, immer wieder angestoßen durch Datenschützer, sich bemüht, dieser durch technische, fachliche und finanzielle Gründe vorangetriebene Entwicklung zu steuern und ihr Grenzen zu ziehen. Jüngst haben die Instanzen der Europäischen Union neue Akzente gesetzt: Die neue **EU-Datenschutzrichtlinie** stellt bei der Verarbeitung von Gesundheitsdaten, soweit der Betroffene seine Einwilligung nicht gegeben hat, in Art. 8 Abs. 3 sowohl an die verfolgten Verarbeitungszwecke als auch an die agierenden Personen besonders hohe Anforderungen. Eine Möglichkeit der Umsetzung wäre ein bundeseinheitliches umfassendes Gesundheitsdatenschutzgesetz.

15.1.2 Die Öffentlichkeit nimmt Notiz

Die Automatisierung der Datenverarbeitung im Gesundheitswesen nimmt in meiner Prüf-, Beratungs- und Öffentlichkeitsarbeit einen breiten Raum ein (vgl. zuletzt 17. JB, Ziff. 13.1). Inzwischen widmen auch die **Medien** dem Thema ihre Aufmerksamkeit.

Stein des Anstoßes ist das gesetzliche Verbot für Krankenkassen, Abrechnungen der Erbringer von Gesundheitsleistungen (z.B. von Ärzten, Zahnärzten, Krankenhäusern, Apotheken) anzuerkennen, wenn sie nicht maschinenlesbar oder auf maschinell lesbaren Datenträgern übermittelt worden sind. Dieses in § 303 Abs. 3 SGB V verhängte Verbot sanktioniert die gesetzliche Verpflichtung der genannten Leistungserbringer, ihre **Abrechnungsunterlagen EDV-gerecht** zu übermitteln. Bezweckt sind die Rationalisierung der Gesundheitsverwaltung insgesamt und die Kontrolle der Leisungserbringer (auch der Versicherten/Patienten?) durch bessere Auswertbarkeit der Daten. Voraussetzung und Folge sind die Ausstattung aller Beteiligten mit EDV-Anlagen und die Entwicklung und Installierung entsprechender Programme.

Mit Hilfe der entstehenden **Infrastruktur** wird es den Krankenkassen technisch möglich sein, nicht nur die Leistungserbringer, sondern auch die Versicherten zu kontrollieren. Der Fachausdruck hierfür ist **„versichertenbezogene Transparenz des Leistungsgeschehens"**. Im Klartext zielt dies ab auf die Feststellung, welche Leistungen aufgrund welcher Diagnosen für einzelne Versicherte abgerechnet worden sind. Befürchtungen werden geäußert, administrative Gesundheitsberatung, Kontrolle und risikobezogene Selektion rückten in den Bereich des Machbaren und könnten bei Zuspitzung der Finanzierungsdefizite im Gesundheits- und Sozialwesen auch gesetzlich erlaubt werden.

15.1.3 Konflikt um EDV-gerechte Abrechnungsunterlagen

Zur Zeit allerdings haben die beteiligten Stellen noch damit zu tun, die **Umsetzungsschwierigkeiten** zu überwinden. Das **Automatisierungsgebot** an die Kassen und Leistungserbringer gilt bereits seit Inkrafttreten des Gesundheitsreformgesetzes zum 01.01.1989, das **Abrechnungsverbot** an die Kassen bei nicht EDV-gerechten Datenträgern seit Inkrafttreten des Gesundheitsstrukturgesetzes am 21.12.1992 mit Wirkung vom 01.01.1995. Dieses Datum wurde aber seitens der verantwortlichen Stellen nicht eingehalten.

Nun wollten Kassen und Bundesminister für Gesundheit zum 01.01.1996 mit der Gesetzesgeltung ernst machen, d.h. keine Vergütung der Leistungsträger vornehmen bzw. zulassen, wenn diese die Abrechnungsunterlagen nicht EDV-gerecht einreichen. Seitdem ist die öffentliche und juristische **Auseinandersetzung** entbrannt:

- Die **Zahnärzte** weigern sich, unterstützt durch ihre Bundesvereinigung, die Daten im von Kassen und Bundesschiedsstelle geforderten Umfang zu liefern. Sie beklagen, daß die Fülle der Daten es den Kassen gestatten würde, entgegen dem Gesetz den Abrechnungsdatensatz **versichertenbezogen** auszuwerten (vgl. dazu Ziff. 15.2.2.1).
- **Ärzteinitiativen** laufen Sturm gegen die Verpflichtung, die im gesetzlich vorgeschriebenen Datensatz enthaltenen Diagnosen wie gefordert zu codieren **(ICD-10-Schlüssel).** Sie argumentieren, der Code zwinge sie dazu, diskriminierende Angaben über ihre Patienten zu machen und könne zu verhängnisvollen Übermittlungsfehlern führen (vgl. dazu Ziff. 15.2.3).

Die Ärzte und Zahnärzte haben vorerst erreicht, daß sie zumindest bis zum 31.12.1997 weiter **konventionell** abrechnen dürfen. Es ist zu begrüßen, daß jetzt nicht mehr nur Datenschützer, Patientenstellen/Gesundheitsläden und einige „alternative" Ärzte ihre Probleme mit dem Einzug der EDV in die Gesundheitsverwaltung artikulieren, wurde bislang doch im übrigen unwidersprochen behauptet, EDV im Gesundheitswesen diene ausschließlich der **Qualitätsverbesserung** und der **Kostensenkung** und gefährde in keiner Weise Belange der Versicherten/Patienten (so zuletzt vertreten von der Bundesregierung in ihrer Antwort auf eine Anfrage der Fraktion Bündnis 90/DIE GRÜNEN, BT-Drs. 13/3001 vom 14.11.95). Die öffentliche Auseinandersetzung über die Folgen der EDV für das **Persönlichkeitsrecht** von Versicherten/Patienten ist nun eröffnet.

Wie einseitig bislang argumentiert wurde, zeigt folgendes Beispiel: Es wurde beklagt, das Leistungsgeschehen sei zu wenig transparent, es sei nicht möglich, zu kontrollieren, ob Ärzte und Krankenhäuser abgerechnete Leistungen erbracht haben oder ob die erbrachten Leistungen sinnvoll sind. Die EDV solle dies ändern. Es wurde allerdings nicht daran gedacht, die einzelnen Betroffenen selbst zu aktivieren, etwa indem sie einen Ausdruck der Abrechnungsunterlagen erhalten, mit dessen Hilfe sie den Leistungserbringern selbst auf die Finger schauen können - eine merkwürdige Unterlassung.

15.1.4 Stand der Technik contra rechtliche Regulierung

15.1.4.1 Spannbreite des EDV-Einsatzes

Aufgabe des Datenschutzes ist es, darauf zu achten, daß im Kräftespiel von Verbands-, Wirtschafts- und Politikinteressen das Recht auf informationelle Selbstbestimmung der betroffenen Versicherten/Patienten nicht völlig aus dem Blickfeld gerät. Andernfalls - so meine Einschätzung - wird die Entwicklung dahin gehen, daß die Gesundheitsdaten der Bürgerinnen und Bürger zwischen Ärzten, Krankenhäusern, Kassen, kassenübergreifenden Vermittlungs-, Auswertungs- und Prüfstellen, Krankheitsregistern und Forschungseinrichtungen frei „floaten", ohne daß dem einzelnen Betroffenen Ausmaß, Art und Zwecke der Verarbeitung seiner Daten transparent wären, geschweige denn, daß er Einfluß darauf nehmen könnte. Ihm könnten so sein gesundheitliches Verhalten, frühere Arztbesuche oder Erkrankungen entgegengehalten werden, wenn er damit nicht zu rechnen braucht.

Noch ist dies gesetzlich **nicht** erlaubt. Die rechtlichen Vorgaben drohen aber durch die technischen Möglichkeiten überspielt zu werden. Die Entwicklung von Interessen und Technik geht tendenziell in Richtung administrativer Kontrolle der Ärzte, anderer Erbringer von Gesundheitsdiensten und letztlich auch der Patienten.

Die **Spannbreite des EDV-Einsatzes im Gesundheitswesen** erstreckt sich von

- einem vom Anwender selbst entwickelten Programm mit beschränkten Möglichkeiten der Datenerhebung, eingeschränkten zweckgebundenen Funktionen zur Verarbeitung und integrierten Datensicherungsfunktionen (Amtsärztliche Dateien in den bremischen **Gesundheitsämtern** Bremen, dazu nachfolgend Ziff. 15.3.1),
- über die Beschaffung multifunktionaler Standardsoftware, deren Funktionen das gesetzlich zugelassene Maß weit überschreiten (Patientendatei des Sozialpsychiatrischen Dienstes des **Gesundheitsamts** Bremen, vgl. u. Ziff. 15.3.2),
- über zentrale Datenbanken in **Krankenhäusern** mit intern erhobenen Daten (vgl. u. Ziff. 15.4)
- bis zu den zentralen Datenbanken der **Krankenkassen,** deren Inhalte an vielen anderen Stellen erhoben und von dort übermittelt worden sind (vgl. die Beispiele unter Ziff. 15.2).

15.1.4.2 Risiken

Die **Risiken** wachsen durch den Einsatz mächtiger Standardsoftwareprodukte und mit dem Abstand der Datenverarbeitung vom ursprünglichen Erhebungszweck.

In den Krankenkassen laufen maschinenlesbar von den Kassenärztlichen Vereinigungen, den Ärzten, den Apotheken (über ihre Rechenzentren), den Krankenhäusern und anderen Leistungserbringern übermittelte Gesundheitsdaten zusammen. Diese vom ursprünglichen Informationszusammenhang am Erhebungsort „entfremdeten" Daten werden nun für eigene Zwecke der Krankenkassen verarbeitet. Die für den Laien (und auch für den Experten?) kaum noch zu übersehende Anzahl von Verarbeitungszwecken muß nun - und hier ist der negative Qualitätssprung - für eine datenschutzgerechte Verarbeitung nachträglich sichergestellt werden. Einen ersten Versuch wird die AOK Bremen im Zusammenhang mit den Verschreibungsdaten (vgl. das Projekt TARZAN, u. Ziff. 15.2.4) unternehmen. Über dieses Verfahren hinaus wird die Entwicklung **komplexer Datensicherungs- und Steuerungssysteme** für den gesamten „Gesundheitsdatenpool" erforderlich sein, um gesetzliche Vorgaben und technische Möglichkeiten aus ihrem Widerspruch zu lösen.

Es entsteht eine **Datenflut**, die nur schwerlich durch technische und organisatorische Vorkehrungen einzudämmen und auf das gesetzlich zugelassene Maß zu begrenzen sein wird.

15.1.5 Kriterien für die Beurteilung von EDV-Systemen im Gesundheitswesen

Bevor ich über meine Beratungs- und Prüfungstätigkeit des Jahres 1995 im einzelnen berichte, will ich zusammenfassen, an welchen Kriterien ich mich dabei orientiert habe:

- Ich sehe die Automatisierung der Datenverarbeitung im Gesundheitswesen als ein **Gesamtprojekt** an, dessen maßgebliches Ziel Kostenbegrenzung bzw. -senkung ist. Belange der Versicherten/Patienten wie Qualitätsverbesserung oder Transparenz des Geschehens ihnen gegenüber treten in den Hintergrund. Datenaustauschverträge, Diagnosecodierung oder Einsatz von Chipkarten sind nur Bausteine des Gesamtprojekts und aus seiner Logik heraus zu beurteilen.
- Die Aufgabe des Datenschutzbeauftragten besteht darin, den **Freiraum** zu erhalten, der es Versicherten/Patienten erlaubt, sich an den Arzt ihres Vertrauens zu wenden und in Kooperation mit diesem eigenverantwortlich über den Umgang mit ihrer Gesundheit bzw. Krankheit zu bestimmen. Dieser Freiraum würde durch die - per EDV technisch mögliche - Kontrolle des gesundheitlichen Verhaltens bzw. des Lebensstils des Einzelnen durch administrative Systeme per Datenauswertung abgeschafft.
- Die gesetzlich vorgegebenen **Zweckbindungen** der Datenspeicherung und -nutzung sind einzuhalten. Das SGB V und andere Gesetze enthalten differenzierte Regelungen dafür, welche versicherten- und arztbezogenen bzw. anonymisierten Daten die Kassen für welche Zwecke und für welche Zeiträume in konventionellen bzw. automatisierten Verfahren speichern bzw. nutzen dürfen. Automatisiert gespeicherte Daten unterliegen - so sieht es § 284 Abs.1 S.2 bis 4 SGB V vor - einer besonders strengen Zweckbindung und Löschfrist. Auf die Einhaltung dieses gesetzlich angeordneten Ausgleichs zwischen technischen Möglichkeiten der Auswertung und juristisch vorgegebene Grenzen werde ich besonders achten.
- Trotz zunehmender Komplexität der Datenverarbeitung und begrenzter Möglichkeiten, ihre Rechtmäßigkeit technisch sicherzustellen, werde ich darauf achten, daß die erforderlichen **Vorkehrungen** zur Einhaltung der Zweckbindung und rechtzeitigen Löschung getroffen werden.

15.2 Gesetzliche Krankenversicherung

Es folgen Beispiele für die unter Ziff. 15.1 dargestellte Entwicklung aus dem Bereich der **gesetzlichen Krankenversicherung**, mit denen ich mich im Berichtsjahr auseinanderzusetzen hatte.

15.2.1 Chipkarten mit medizinischen Daten

15.2.1.1 Unveränderte Kernforderungen

Als logische Konsequenz der Einführung der gesetzlich vorgesehenen Krankenversichertenkarte als Chipkarte (vgl. hierzu 17. JB, Ziff. 13.1.1.1) wird die Nut-

zung der bei Krankenkassen, Kassenärztlichen Vereinigungen, Ärzten und Krankenhäusern bereitgestellten technischen Ausstattung für das Speichern und Auslesen von medizinischen Daten der Versicherten auf Chipkarten vorangetrieben (vgl. 17. JB, Ziff. 13.1.1.4). Diese werden **Patienten- oder Gesundheitskarten** genannt zur Unterscheidung von der **Krankenversichertenkarte**, auf der nur administrative und Identifikationsdaten, aber keine medizinischen Daten des Versicherten gespeichert werden dürfen.

Ich werde weiter dafür eintreten, daß die Patienten/Versicherten nicht nur formal Inhaber der Chipkarten mit ihren medizinischen Daten sind, sondern daß sie tatsächlich darüber bestimmen können, ob sie eine Karte nutzen wollen, welche Daten zu welchen Zwecken auf ihnen gespeichert werden und wer diese Daten lesen und in sein Datenverarbeitungssystem eingeben darf. Wird dies nicht sichergestellt, so ist die Chipkarte mit medizinischen Daten genauso wie die Krankenversichertenkarte nur ein administratives Hilfsmittel, im Gegensatz zu dieser aber eines, mit dessen Hilfe der Austausch medizinischer Informationen zwischen den Beteiligten am Gesundheitswesen, und zwar ohne Transparenz und Selbstbestimmung für die Karteninhaber selbst, vervielfältigt zu werden droht.

15.2.1.2 Neue Kartenprojekte

Im Berichtszeitraum ist der Öffentlichkeit eine Reihe **neuer Projekte** zur Einführung von Chipkarten mit medizinischen Daten vorgestellt worden. Dies hat die Datenschutzbeauftragten des Bundes und der Länder dazu veranlaßt, auf ihrer Konferenz im November 1995 in einer neuen Entschließung die datenschutzrechtlichen Anforderungen ihres Beschlusses vom März 1994 (abgedr. im 17. JB, Ziff. 20.1) fortzuschreiben (vgl. u. Ziff. 20.15). Als ihr turnusmäßiger Vorsitzender habe ich im Auftrag der Datenschutzkonferenz der **Arbeitsgemeinschaft „Karten im Gesundheitswesen"**, zu der sich maßgebliche Betreiber, Entwickler und Befürworter von Kartenprojekten zusammengeschlossen haben, vorgeschlagen, gesprächsweise die beiderseitigen Positionen auszutauschen und weiterzuentwickeln. Inzwischen wird ein Zusammentreffen für das Frühjahr 1996 vorbereitet. Einem Papier, in dem ein Arbeitskreis der Arbeitsgemeinschaft datenschutzrelevante Thesen vorgelegt hat, entnehme ich, daß in wesentlichen Punkten die Auffassungen gar nicht so weit auseinander gehen dürften.

Andererseits zeigt die Erfahrung, daß der Datenschutz in der Praxis einzelner Anwendungen dann doch gegenüber anderen technischen, finanziellen und Nutzungsinteressen all zu schnell ins Hintertreffen zu geraten droht, wird dem nicht von verantwortlicher Seite und durch eine **kritische öffentliche Auseinandersetzung** entgegengesteuert. Geschieht dies aber nicht, dann werden die Chipkarten mit medizinischen Daten ein Baustein des oben unter Ziff. 15.1 kritisierten **technokratischen Gesamtsystems**, und dies ohne jede gesetzliche Grundlage.

15.2.2 Maschinengerechte Datenübermittlung an die Krankenkassen

15.2.2.1 Gefährdung des Patientengeheimnisses

Wie alle anderen Leistungserbringer müssen auch Ärzte und Zahnärzte ihre **Abrechnungsdaten** - in diesem Fall über die Kassenärztlichen bzw. Kassenzahnärztlichen Vereinigungen - den Kassen **EDV-gerecht** übermitteln. Ich hatte in diesem Zusammenhang kritisiert, daß in vertraglich festgelegten Fällen unter Verstoß gegen § 295 Abs. 2 SGB V die Kassen instandgesetzt werden sollen, Diagnosedaten zu den unterschiedlichsten Zwecken **versichertenbezogen** auszuwerten. Diese Kritik bezog sich im Vorjahr auf Einzelheiten des zwischen der Kassenärztlichen Bundesvereinigung und den Spitzenverbänden der Krankenkassen auf Bundesebene abgeschlossenen Datenaustauschvertrages (vgl. 17. JB, Ziff. 13.1.1.3).

Derzeit wehrt sich die Kassenzahnärztliche Bundesvereinigung gegen weitgehend identische, den Zahnärzten durch einen Schiedsspruch auferlegte Übermittlungsverpflichtungen mit publizistischen und juristischen Mitteln. Die Zahnärzte richten ihre Kritik vor allem dagegen, daß

- sie mehr Daten übermitteln sollen, als ihrer Auffassung nach für die Honorarabrechnung erforderlich sind, d.h. sie vermuten, daß die Kassen mit der Verarbeitung dieser Daten andere Zwecke als die gesetzlich zugelassenen verfolgen könnten,
- auch ohne ausdrückliche vertragliche Gestattung allein die Fülle **fallbezogener** (d. h. nicht **unmittelbar** auf den einzelnen Versicherten bezogener) Daten

es den Kassen technisch ermöglichen wird, durch elektronischen Abgleich die von den Abrechnungsunterlagen betroffenen einzelnen Versicherten doch zu identifizieren und versichertenbezogene Auswertungen zu den unterschiedlichsten Zwecken vorzunehmen.

Ohne in diesem, auch vor den Sozialgerichten anhängigen Konflikt direkt Partei ergreifen zu wollen, sehe ich in der Auseinandersetzung eine Bestätigung meiner Auffassung,

- daß die Automatisierung der Datenverarbeitung neue Gefahren für Persönlichkeitsrechte von Versicherten/ Patienten birgt, und
- daß es gilt, die gesetzlich vorgeschriebene Differenzierung der Datenverarbeitung für die unterschiedlichen Zwecke rechtlich und technisch strikt umzusetzen (vgl. zu dem Beispielsfall des Bremer Projekts TARZAN u. Ziff. 15.2.4).

Die Datenschutzbeauftragten von Bund und Ländern bereiten derzeit eine gemeinsame Stellungnahme vor. Dabei gilt es zu bedenken, daß es einerseits den Kassen möglich sein muß, ihre Aufgaben einschließlich der Kostenkontrolle effizient wahrzunehmen, daß aber andererseits der Gesetzgeber hierfür einen bestimmten Rahmen mit **genau definierten Prüf- und Kontrollbefugnissen** geschaffen hat.

15.2.2.2 Einschaltung einer Datenannahme- und Verteilstelle

Die Datenschutzbeauftragten hatten sich im Berichtszeitraum damit auseinanderzusetzen, daß die **Ersatz-, Betriebs- und Innungskrankenkassen** für die bei ihnen einzureichenden Abrechnungsunterlagen aller Leistungserbringer ein privates Telekommunikationsunternehmen mit der Einrichtung einer zwischengeschalteten **Datenannahme- und -verteilstelle** beauftragen wollen. In Bremen sind von diesem Vorhaben u.a. die Handelskrankenkasse und mehrere Betriebskrankenkassen betroffen.

Nachdem klargestellt war, daß das o.a. Unternehmen als Datenverarbeiter im Auftrag der Kassen nach Maßgabe des § 80 SGB X **ohne Kenntnisnahme** des Inhalts der durchfließenden Daten nur technische Hilfsfunktionen durch Bereitstellung von Leitungskapazitäten und Zuordnung von Abrechnungsdaten zu den einzelnen Kassen ausüben wird und technische Datensicherungsvorkehrungen ausreichend sichergestellt sind, haben die Datenschutzbeauftragten keine grundsätzlichen Bedenken erhoben. Gleichwohl gilt es darauf zu achten, daß die Funktionen der Datenannahme- und -verteilstelle nicht so erweitert werden, daß die beauftragte Firma oder andere nicht-öffentliche Stellen zentrale Datenverarbeitungsfunktionen übernehmen, bei denen sie Kenntnis vom Inhalt der Abrechnungsdaten nehmen müssen. Dann wären Arzt- bzw. Sozialgeheimnis ernstlich in Frage gestellt.

15.2.2.3 Verschlüsselung bei der Übermittlung von Leistungsdaten

Genau wie der Bundesbeauftragte und andere Landesbeauftragte für den Datenschutz für ihre Zuständigkeitsbereiche habe ich gegenüber den Verbänden der Leistungserbringer und der Kassen im Lande Bremen die Forderung erhoben, daß alle EDV-gerecht übermittelten **Leistungsdaten** ab sofort zu **verschlüsseln** seien, gleich ob die Daten direkt oder über kassen(zahn)ärztliche Vereinigungen und/oder eine Datenannahme- und -verteilstelle an die Kassen übermittelt werden. Dies ist nach § 78a SGB X als technische Vorkehrung zum Schutze der sensiblen, rechtlich durch das Arzt- bzw. Sozialgeheimnis besonders geschützten Daten angesichts ihrer leichten elektronischen Auswertbarkeit und der Nutzung allgemeiner Übertragungswege (Leitungen, Postversand) zwingend geboten.

Die Reaktion der verantwortlichen Stellen war widersprüchlich. Hieß es bei einer Besprechung im Bundesministerium für Gesundheit zunächst, alle Gesprächsteilnehmer einschließlich der Kassen und des Gastgebers hätten sich darauf verständigt, sämtliche Daten zu verschlüsseln, lehnte das Ministerium kurz darauf genauso dies ab. Hieß es einerseits, bereits ab 01.01.96 stünden die erforderlichen Verfahren zur Verschlüsselung zur Verfügung, wurde von anderer Seite argumentiert, die Frist sei nicht einzuhalten. Noch kurz vor Jahresende 1995 wurde auf einschlägige Arbeiten in Arbeitsgruppen verwiesen.

Anscheinend fehlt den Beteiligten immer noch die Übersicht, ab wann die Abrechnungsdaten überhaupt maschinell übermittelt werden können und wenn ja, inwieweit dies verschlüsselt geschehen soll bzw. kann. Inzwischen hat der AOK-Bundesverband erklärt, binnen vier Monaten nach Auftragserteilung könne die Verschlüsselungssoftware bereitstehen.

Die Datenschutzbeauftragten halten ihre Forderungen aufrecht. Sie werden sich allenfalls damit einverstanden erklären, daß übergangsweise Disketten mit unverschlüsselten Abrechnungsdaten per Post versandt werden, sofern eine höherwertige Versendungsart (z.B. Einschreiben mit Rückschein) gewählt wird. Bei Übermittlung auf dem Leitungsweg, bei Einschaltung einer Datenannahme- und Verteilstelle (vgl. Ziff. 15.2.2.2) oder bei Versendung von Disketten als einfacher Brief oder Paket wird auf eine Verschlüsselung bestanden.

15.2.3 Codierung der Diagnosen (ICD-10-Schlüssel)

Zugleich mit der Automatisierung der Datennübermittlung zu Abrechnungszwecken hatte der Gesetzgeber den **Ärzten** und **Krankenhäusern** die **Codierung** der in diesem Zusammenhang zu übermittelnden Diagnosen nach einem bestimmten festgelegten Schlüssel, dem **ICD-10-Schlüssel**, vorgeschrieben (vgl. bereits 17. JB, Ziff. 13.1.1.2).

Während die auf der Krankenversichertenkarte gespeicherte Krankenversichertennummer die elektronische Zuordnung von Abrechnungsdatensätzen zu den einzelnen Versicherten/Patienten ermöglicht, eröffnet die Codierung der Diagnosen die Auswertung der Datensätze nach bestimmten **medizinischen** Kritierien, nach Wunsch auch **versichertenbezogen.** Die Codierung erhöht zudem die Gefahr, daß Verdachts- oder Ausschlußdiagnosen bei ihrer Übermittlung als bestätigte Diagnosen gewertet oder gerade in ihrer Bedeutung umgekehrt werden.

Überhaupt führt die auf eine Zahl verkürzte Angabe einer Diagnose zu einem **Informations- und Kontextverlust,** der bei schematischer Auswertung zu falschen fallübergreifenden Aussagen, aber auch zu verhängnisvollen Etikettierungen und Diskriminierungen Einzelner führen kann. Diese Gefahr galt zwar bereits für die im Klartext als Stichwort genannte Diagnose auf Abrechnungsunterlagen, wird aber potenziert durch die mit der Codierung einhergehende automatisierte Auswertbarkeit.

Die vehemente **öffentliche Kritik** wandte sich vor allem dagegen, daß eine Reihe der vorgeschriebenen Codierungsziffern weniger die Diagnose von Krankheiten transportierten als unangepaßtes Verhalten denunzierten. Als Beispiele wurden die Schlüssel für „antisoziale Persönlichkeit", „oppositionelles Verhalten" des jugendlichen Patienten, „Erziehungsfehler der Eltern", „exzessive sexuelle Lust" oder „Konflikte mit Vorgesetzten" genannt. Es war allerdings kein Arzt gezwungen, diese fragwürdigen Codierungen zu nutzen; überhaupt ist nicht zu erkennen, wie auf sie eine Honorarforderung gestützt werden kann.

Das Bundesministerium für Gesundheit hat schnell reagiert und die offen **diskriminierenden Schlüssel** für unangepaßtes Verhalten außer Kraft gesetzt. Zwar mag der angeordnete ICD-10-Schlüssel, von der Weltgesundheitsorganisation WHO für globale Statistik- und Forschungszwecke entwickelt, für diese Verwendung geeignet sein, für die Abrechnung ärztlicher Leistungen jedenfalls wird dies mit plausiblen Gründen bestritten. Nach meiner Aufassung sind die in diesem Fall aufgetretenen disfunktionalen Auswirkungen typisch für den technokratischen Perfektionismus, der sich zunehmend auch in der Gesundheitsverwaltung bemerkbar macht.

Inzwischen ist - ohne Gesetzesänderung - **die Codierungspflicht** um weitere zwei Jahre **verschoben** worden, in deren Verlauf der Code unter Beteiligung des Bundesbeauftragten für den Datenschutz **überarbeitet** werden soll. Es bleibt abzuwarten, ob die Kritik von Verbänden und Medien, angestoßen von Ärzten, Patientenstellen und Datenschutzbeauftragten, zur Abkehr von einer **Schematisierung** führt, die die Individualität des Patientenen bzw. Versicherten aus dem Auge zu verlieren droht. Meine Kollegen und ich werden uns intensiv in diese Debatte einschalten.

15.2.4 Das Projekt TARZAN der AOK - Anpassung an die Rechtslage

In dem dargestellten Kontext sehe ich auch das Projekt TARZAN, mit dem ich mich in den vergangenen Jahren intensiv auseinandergesetzt habe (vgl. ausführl. 17. JB, Ziff. 13.1.2.). In Kooperation mit dem Senator für Arbeit als zuständiger Rechtsaufsichtsbehörde habe ich im Berichtsjahr die Zusage der AOK Bremen/Bremerhaven erreicht, ihr Projekt TARZAN, in dessen Rahmen sie seit Beginn des Jahres 1993 die Daten aus ärztlichen Verschreibungen **versichertenbezogen** für unterschiedlichste Zwecke auf unbestimmte Zeit automatisiert auf Datenbändern speicherte, **aufzugeben.** Im Januar 1996 sind zunächst die versicherten- und die arztbezogenen Merkmale gelöscht worden, die aus Verschreibungen der Jahre

1993/94 gespeichert waren. Im Januar 1997 soll das Datematerial für 1994 und so fortlaufend gelöscht werden.

Künftig will die AOK die Daten nur noch insoweit vorhalten, als dies zur Erfüllung ihrer Aufgaben gesetzlich erlaubt ist. Das SGB V bietet hierfür in § 284 und anderen Vorschriften differenzierte Rechtsgrundlagen. Dazu zwei Beispiele:

— Zur **Überwachung der Wirtschaftlichkeit der Leistungserbringung** nach § 106 SGB V müssen die Kassen Verschreibungsdaten versichertenbezogen für ein Jahr speichern (vgl. § 297 Abs. 2 Satz 2). Danach aber darf - jedenfalls nicht zum Zweck der Wirtschaftlichkeitsprüfung - der Versichertenbezug nicht mehr herstellbar sein, mit Ausnahme der Verschreibungen solcher Ärzte, die der Prüfungsausschuß für die Stichprobenprüfung von höchstens 2 % der Ärzte pro Quartal ausgewählt hat.

— Für Zwecke der **Auskunft an Versicherte** müssen die Verschreibungsdaten seit 01.01.1996 für höchstens zwei Jahre gespeichert werden (vgl. § 305 SGB V in der seither geltenden Fassung).

Diese **differenzierten Zugriffs- und Löschungsregelungen** sind durch technische Vorkehrungen im EDV-System zu verankern. Die AOK Bremen/Bremerhaven hat zugesagt, bis März 1996 den Entwurf eines solchen Konzepts vorzulegen.

15.3 Gesundheitsämter

15.3.1 Gegenläufige Verarbeitungstendenzen

Durch die nachfolgend beschriebenen EDV-Projekte der **Gesundheitsämter Bremen** und **Bremen-Nord** werden insbesondere zwei Aspekte deutlich, die sowohl Chancen als auch Risiken der Automation in dem besonders sensiblen Bereich der Verarbeitung von Gesundheitsdaten verdeutlichen.

Als **Chance** ist die Beschränkung der Verarbeitung von Gesundheitsdaten im **amtsärztlichen Dienst** des Gesundheitsamtes **Bremen-Nord** auf das zulässige Maß und die Ermöglichung einer datenschutzgerechten Weiterverarbeitung durch ein im Gesundheitsressort entwickeltes Programm zu sehen, das drei wesentliche Aspekte integriert, die zu einer datenschutzgerechten Automatisierung führen.

Die Menge der zu erhebenden Daten orientiert sich direkt an konkreten Aufgabenbereichen. Die Verarbeitungsfunktionen garantieren die Zweckgebundenheit der Verarbeitungsprozesse, d.h. ihre Möglichkeiten überschreiten an keiner Stelle den gesetzlich vorgegebenen Rahmen. Und: Das Programm integriert erforderliche Datensicherungsmaßnahmen (vgl. u. Ziff. 15.3.2).

Als **Risiko** ist der Funktionsumfang eines für den Einsatz im **sozialpsychiatrischen Dienst** des Gesundheitsamtes **Bremen** geplanten, insbesondere für Arztpraxen entwickelten Standardsoftwareproduktes zu sehen. Dieses sollte zunächst für den Zweck der automatisierten Abrechnung mit den Krankenkassen installiert werden. Die fertige Standardlösung bietet jedoch eine Fülle von darüber hinausgehenden Verarbeitungsfunktionen, mit denen sich die Abläufe des gesamten Beratungsgeschehens automatisiert darstellen lassen (vgl. u. Ziff. 15.3.3).

15.3.2 Beratungsgeheimnis versus amtsärztliche Tätigkeit - Trennung der Datenbestände

Die **Karteien der amtsärztlichen Dienste** in den Gesundheitsämtern Bremen und Bremen-Nord (vgl. zuletzt 16. JB, Ziff. 8.5.2) wurden mit dem Ziel des differenzierten Zugangs zu den Akten der einzelnen Untersuchten nach unterschiedlichen Untersuchungsanlässen, der Neuordnung des Gesamtbestandes und der Aussortierung von Altakten mit Hilfe eines vom Gesundheitsressort selbst entwickelten **EDV-Programms** unter Beachtung der Vertraulichkeits-und Zweckbindungsgebote des Gesetzes über den öffentlichen Gesundheitsdienst (vgl. o. Ziff. 7.1.2) in Abstimmung mit mir **neu organisiert.**

In den Datenbanken werden zentral Patientenstammdaten gespeichert, jedoch keine Untersuchungsergebnisse oder diagnostische Daten. Gespeichert werden der Untersuchungsanlaß - die Art der Untersuchungsanlässe ist festgelegt und entspricht dem gesetzlichen Auftrag der amtsärztlichen Untersuchungspflicht -, das Untersuchungsdatum und gegebenenfalls die Wiedervorlagedaten. Zu löschende Daten werden listenmäßig automatisch vom System ausgegeben, damit die entsprechenden Akten vernichtet werden können. Die automatisierte Aktenzeichenvergabe ermöglicht eine differenzierte Speicherung der Akten und einen differenzierten Zugriff auf sie.

Die Anwendung soll nach Abschluß der Testphase in einer sog. Access Runtime-Umgebung eingesetzt werden, so daß Änderungen der Funktionalitäten durch die Anwender selbst ausgeschlossen werden. Änderungen der Datenstruktur werden mit meiner Dienststelle abgestimmt und protokolliert, ebenso Änderungen der Funktionalitäten der Anwendung, insbesondere bei Erweiterungen im Bereich der Abfragen und Auswertungen.

Insgesamt handelt es sich infolge der engen Beschränkung der Datensätze, Zugriffe und Auswertungsmöglichkeiten sowie wegen der getroffenen Datensicherungsmaßnahmen verbunden mit den entsprechenden Dokumentationen um ein positives Beispiel für ein **datenschutzgerechtes Automatisierungsprojekt.**

15.3.3 Sozialpsychiatrische Beratung und Therapie - Vetraulichkeit gefährdet?

Der Sozialpsychiatrische Dienst (SPsD) des Gesundheitsamts Bremen ist auf der Grundlage von § 118 Abs.2 SGB V seit Anfang 1995 als **„Psychiatrische Institutsambulanz"** zugelassen und rechnet seither seine Behandlungsleistungen wie niedergelassene Psychiater mit den Krankenkassen ab. Positive Konsequenz: Der SPsD kann sich damit z. T. über Einnahmen refinanzieren, wird von Kassen und Ärzteverbänden als Teil der ambulanten Gesundheitsversorgung anerkannt und veranlaßt, seine Leistungen im einzelnen zu dokumentieren und nachzuweisen. Unmittelbare Auswirkung ist es, daß der SPsD seine **Abrechnungsunterlagen EDV-gerecht** einreichen muß. Angesichts dessen, daß es sich um die Daten psychiatrischer Patienten handelt, ist - nicht anders als im Zusammenhang mit der Abrechnung von niedergelassenen Psychotherapeuten und psychiatrischen Krankenhäusern - dem **Therapiegeheimnis** und dem Bedürfnis der Patienten nach Schutz vor Kontrolle und Ausgrenzung in besonderer Weise, etwa durch Verschlüsselung, Zugriffssperren und Löschroutinen, Rechnung zu tragen.

Nun verfolgt aber der SPsD die Vorstellung, seine Datenverarbeitung nicht nur zwecks Abrechnung, sondern **insgesamt** zu automatisieren, d. h. auch Diagnosen, Arztberichte, Rehabilitationsgesamtpläne und Gutachten auf miteinander vernetzten PC zu speichern. Technisch wäre dies leicht zu realisieren, liegt doch bereits das Angebot einer Softwarefirma für eine fertige Standardlösung zur Verwaltung von Patientenstammdaten einschließlich der Gesundheitsdaten vor.

Hier ist jedoch Wachsamkeit geboten: Ihre **berufliche Schweigepflicht** verbietet es den Ärzten, Psychologen und Sozialarbeitern des SPsD, Daten ihrer Klienten ohne weiteres automatisiert zu speichern. Das neue Bremische Gesetz über den Öffentlichen Gesundheitsdienst (ÖGDG, vgl. Ziff. 7.1.2) setzt dem Vorhaben, EDV über die Abrechnung mit den Kassen hinaus einzusetzen, aus wohlerwogenen Gründen enge Grenzen. Zum Schutz der Patienten und der Vertraulichkeit ihrer Beratung und Therapie bestimmt das ÖGDG in seinen §§ 31 bis 33:

- Aus **freiwilliger** Inanspruchnahme von Beratungsangeboten erhobene Patientendaten darf der ÖGD in jedem Fall nur mit Einwilligung des Betroffenen weiterverarbeiten. Tut er dies, muß er gewährleisten, daß die Daten nicht für Überwachungs- und Zwangsmaßnahmen genutzt werden, es sei denn, hierfür gäbe es eine gesetzliche Befugnis, etwa im PsychKG (vgl. dazu Ziff. 7.2.3).
- Patientendaten dürfen grundsätzlich nur gespeichert werden, soweit es für weitere Beratungen, Hilfen oder Untersuchungen unerläßlich ist. Die Unterlagen mit Gesundheitsdaten sollen ohnehin möglichst den Betroffenen überlassen und nicht im Amt gespeichert werden.

Sofern nur die Datenverarbeitung zwecks Abrechnung mit den Krankenkassen entsprechend den bundesgesetzlichen Vorgaben automatisiert und die dabei gebotene Datensicherung gewährleistet wird, habe ich gegen die Installation eines EDV-Systems im SPsD des Gesundheitsamts keine Bedenken. Ich habe aber das Gesundheitsressort darum gebeten, vorerst nur ein **auf die Abrechnung begrenztes DV-System** einzusetzen. Weiterhin erwarte ich, daß vor einer Erweiterung von dessen Funktionen in Abstimmung mit mir ihre Vereinbarkeit mit dem ÖGDG überprüft und - wie in § 33 Abs. 3 ÖGDG vorgesehen - durch **Rechtsverordnung** Umfang, Dauer und zugelassene Zwecke von Erhebung und Speicherung von Patientendaten konkretisiert werden. Das Ressort hat sich bisher nicht dazu geäußert.

15.4 Krankenhäuser

15.4.1 Entwicklungsrichtung: Zentrale Patientendatenbank

15.4.1.1 Ursachen des zunehmenden EDV-Einsatzes

Die Ausgestaltung und Organisation der EDV in den Krankenhäusern entwickelt sich zunehmend dynamisch.

Die durch SGB V und Bundespflegesatzverordnung 95 eingeforderten strukturellen und finanziellen Änderungen, etwa durch die **obligatorische maschinenlesbare Abrechnung** der Leistungserbringer mit den Krankenkassen und die Erweiterung der angeordneten Datensätze (vgl. o. Ziff. 15.2.2), führen zu einer Veränderung der DV-Prozesse in den Krankenhäusern in Richtung auf ein **entscheidungsorientiertes Informations- und Berichtswesen.** Der Informationsfluß innerhalb der Teilbereiche eines Krankenhauses wird dadurch qualitativ und quantitativ erhöht bzw. erst ermöglicht. Selbst wenn infolge der Startschwierigkeiten die Krankenhäuser - jedenfalls im Lande Bremen - bis zum 01.07.96 noch konventionell und mit reduziertem Datensatz abrechnen dürfen, ist die **Automatisierung der Abläufe** innerhalb des gesamten Krankenhausbetriebs abzusehen.

Die angestrebte Schaffung einer größeren Transparenz des medizinischen und pflegerischen Leistungsprozesses und der Bewertung des Leistungsgeschehens, die Gewinnung notwendiger Informationen zur Betriebssteuerung und die angestrebte Verbesserung der Qualität der Krankenversorgung durch Optimierung medizinischer und administrativer Abläufe erfordern eine klare logische und physikalische Strukturierung aller relevanten Daten. Zentrum der entsprechenden Zuordnungen kann nur der **Stammdatensatz** des Patienten/der Patientin sein, da diese(r) die zentrale Person ist, die Leistungen erhält, Kosten verursacht, in verschiedenen medizinischen Bereichen durch unterschiedliche Fachkräfte versorgt wird und entsprechende Datenspuren hinterläßt. Konsequenterweise werden die ärztlichen und administrativen Daten in einer **zentralen Datenbank** gespeichert, auf die sich alle denkbaren Auswertungsstrategien anwenden lassen.

15.4.1.2 Zugriffsschutz gefährdet?

Der **technische Datenschutz** gerät dadurch in die **Defensive.** Er muß die nicht mehr zweckgebunden gespeicherten Patientendaten wieder einer zweckgebundenen Verfügbarkeit zuordnen.

Es geht nicht mehr darum, die Erhebung und Verfügbarkeit der Patientendaten in funktionellen Teilbereichen zu strukturieren, die bisher in der Regel von anderen Teilbereichen **physikalisch** getrennt waren. Vielmehr handelt es sich um über definierte Schnittstellen verbundene oder noch zukünftig zu verbindende für Einzelanwendungen konzipierte Softwaresysteme mit komplexen integrierten Möglichkeiten zur Datensicherung, um Standardsoftwareprodukte mit einzelnen Modulen für einzelne Aufgabenbereiche und mit einer differenzierten Steuerung für das Gesamtsystem oder um eine Kombination von beidem.

Zukünftig werden alle den Patienten bzw. die Patientin direkt oder indirekt beschreibenden Daten im Krankenhaus zentral verfügbar sein. Dies belegen die von mir nachfolgend beschriebenen Beispiele (Ziff. 15.4.2 u. 15.4.3). Diese neue Konfiguration könnte zu einem Verstoß gegen § 3 Krankenhausdatenschutzgesetz (KHDSG) führen, wonach einzelne Mitarbeiter/innen oder Organisationseinheiten Zugriff nur auf die **für die jeweiligen Aufgaben erforderlichen** Patientendaten haben dürfen. Die Einschränkung dieser Verfügbarkeit erfolgt aber erst nachträglich durch komplexe Steuerungsmechanismen auf unterschiedlichen Systemebenen.

15.4.2 ZKH Links der Weser - Ergebnisse der Datenschutzkontrolle

15.4.2.1 Prüfungsgrundlagen

Ausgangspunkt der Prüfung waren die Aufgabenerfüllung durch den **betrieblichen Datenschutzbeauftragten** und die sich aus den **gesetzlichen Dokumentationspflichten** ergebenden Unterlagen (vgl. §§ 8 BrDSG i. V. m. § 1 Abs.4 KHDSG u. § 9 KHDSG i. V. m. § 37 BDSG; vgl. auch 15.JB, Ziff. 10.1).

Die Dokumentationspflichten sind der EDV-Abteilung zugeordnet. Sie führt ein ständig aktualisiertes **Geräteverzeichnis** (inklusive Software-Verzeichnis), das Bestandteil eines **umfassenden Datenschutzkonzeptes** ist. Darin sind u. a. die Verantwortlichkeiten und Zuständigkeiten im EDV-Bereich bis auf die Ebene der Stand-alone-PC sowie Berechtigungskonzepte für alle Systeme beschrieben. Darüber hinaus enthält es eine Beschreibung der Vernetzung, Bedingungen der Wartung (insbesondere der Fernwartung) und Dienstanweisungen. Die durch dieses differenzierte Konzept geschaffene Transparenz der EDV-Struktur ermöglichte trotz der Verfahrenskomplexität eine stichprobenartige technische Prüfung, deren Ergebnisse im Rahmen der Gesamtstruktur bewertet werden können.

Es gibt zur Zeit ein logisches Netz, an das im Rahmen der Standardsoftware R/3 der Firma SAP die Bereiche Patientenverwaltung/Abrechnung, Finanzabteilung sowie Controlling und EDV angeschlossen sind. Subnetze bestehen in der Personalabteilung und im Laborbereich. Stand-alone-PC werden u.a. im Rahmen von Textverarbeitung und in der Ambulanz genutzt.

Die technische Datenschutzprüfung bezog sich auf die Bereiche **PC-Konfiguration** in Ambulanz und medizinischer Klinik, **Fernwartung** und das o. a. **R/3-System.** Bei letzterem ging es jedoch nur um den Teilbereich der Zugriffsmöglichkeiten aus den Abteilungen Patientenaufnahme (u.a. Verarbeitung von Daten der Krankenversichertenkarte), Rechnungswesen und Organisation/Controlling. In meinem Prüfbericht habe ich daher keine Aussagen über die von der Systemverwaltung auf Systemebene des R/3-Systems getroffenen Datensicherungsmaßnahmen und über die Kontrolle der Systemverwaltung selbst gemacht.

15.4.2.2 Ergebnisse

Festgestellte geringfügige Mängel in der PC-Konfiguration des PC in der **Ambulanz** und der **medizinischen Klinik** wurden umgehend abgestellt. Bei der **Fernwartung** bleibt als kritischer Punkt vor allem, daß bei der softwarebedingten Behebung von Fehlern in Ausnahmefällen der Zugriff auf Patientendaten möglich ist; eine technische Alternative ist insoweit - jedenfalls derzeit - kaum erkennbar.

Bei der Überprüfung der **abteilungsbezogenen Zugriffsmöglichkeiten** im Rahmen des R/3-Systems ergab eine Stichprobe, daß Umfang und Inhalte der insoweit überprüften Datenfelder sich innerhalb der gesetzlichen Vorgaben bewegten. Für einige durch das System vorgegebene Felder bestehen allerdings noch keine inhaltliche Definitionen (z. B. für das Feld „Risiko"); diese werden nachträglich erfolgen. Die getroffenen Datensicherungsmaßnahmen entsprechen dem gesetzlich geforderten Standard. Es ist gegebenfalls erforderlich, den Export personenbezogener Daten aus dem SAP-System in Standardsoftware zu verhindern bzw. entsprechend den gesetzlichen Vorgaben zu steuern.

Als **Gesamtergebnis** konnte ich für den überprüften Teil der Datenverarbeitung erfreulicherweise feststellen, daß das ZKH Links der Weser organisatorisch und technisch adäquate Datenschutzmaßnahmen ergriffen hat. Ich erwarte allerdings, daß die fortschreitende EDV-Entwicklung weiterhin differenziert und zeitgleich im Datenschutzkonzept berücksichtigt wird und die entsprechenden Sicherungsvorkehrungen realisiert werden. Nur so ist gewährleistet, daß die Verarbeitung der Patientendaten wie bisher transparent und das Schutzniveau stabil bleibt.

Das Krankenhaus hat mich bisher gem. § 27 Abs. 4 BrDSG im Vorfeld umfassend über die EDV-Entwicklung informiert. Die dadurch eröffnete Möglichkeit der **frühzeitigen Beratung** werde ich weiterhin gern in Anspruch nehmen.

15.4.3 ZKH Bremen-Ost - Ergebnisse der Nachprüfung

Aufgrund der in meinem 16. Jahresbericht dargestellten Prüfergebnisse (vgl. 16. JB, Ziff. 8.4.1.3) waren **Nachbesserungen** in folgenden Bereichen erforderlich:

— Eigenentwicklung von Programmen,

— Funktionstrennung zwischen Entwicklung, Anwendung und Systemverwaltung sowie

— Transparenz und Kontrolle der Systemverwaltung.

Der Senat hat in seiner Stellungnahme zu meinem 16. JB die Erfüllung dieser Anforderungen zugesagt (vgl. Bürgerschafts-Drucks. 13/972, S. 11, zu 8.4.1.3).

Eine erneute Überprüfung im Berichtszeitraum hat folgenden Sachstand ergeben:

Das Krankenhaus hatte versichert, daß die **eigenentwickelten** Verfahren „Medizinische Dokumentation im Archiv" und „vorläufige Patientenaufnahme" auslaufen würden. 1995 sollten im Rahmen der medizinischen Dokumentation nur noch Restdaten aus dem Jahr 1994 abschließend bearbeitet werden. Eine Programmdokumentation ist zwar erstellt und damit das Verfahren transparent geworden, die grundsätzliche Problematik der Eigenentwicklungen bleibt aber gleichwohl bestehen. Die Ablösung erfolgt durch das Verfahren „MEDICAL-CONTROL" der Firma DATA-PLAN.

In dem Verfahren zur vorläufigen Patientenaufnahme wurden weder das Programm noch die Eigenentwicklung noch die Transparenz der Systemverwaltung verbessert. Den Einsatz eines neuen datenschutzgerechten Verfahrens hat das Krankenhaus bereits für den Jahreswechsel 1994/1995 zugesagt, bisher aber noch nicht realisiert.

Erhebliche Mängel gibt es nach wie vor bei der **Funktionstrennung zwischen Entwicklung, Anwendung und Systemverwaltung:**

Im Bereich der medizinischen Dokumentation wurden Anwendung und Entwicklung durch Herausnahme der Entwicklerin aus dem Anwendungsbereich getrennt. Die Wirksamkeit der Maßnahme ist allerdings wegen der nicht veränderten Kriterien zur Eigenentwicklung teilweise aufgehoben. So ist z. B. der Quellcode des Verfahrens im Anwendungsbereich weiterhin verfügbar. Die Funktionen Entwicklung und Systemverwaltung sind bisher weder im Verfahren zur medizinischen Dokumentation noch in der ambulanten Patientenaufnahme separiert worden.

Schließlich sind auch keine technischen oder organisatorischen Maßnahmen zur Verbesserung der **Transparenz und Kontrolle der Systemverwaltung** ergriffen worden. Die EDV-Abteilung hat mit dem Datenschutzbeauftragten des Hauses bisher kein internes Kontrollverfahren verabredet.

Da zukünftig keine Eigenentwicklungen mehr vorgenommen werden sollen, hatte ich unter der Voraussetzung einer fristgemäßen Ablösung beider Verfahren deren Weiterverwendung hingenommen. Die Frist für den Ersatz des Verfahrens der ambulanten Patientenaufnahme ist jedoch seit einem Jahr abgelaufen; der Ersatz des Verfahrens zur medizinischen Dokumentation wäre Anfang 1996 fällig gewesen.

Das Krankenhaus Bremen-Ost plant umfassende Veränderungen im EDV-Bereich im Zusammenhang mit der Erstellung eines neuen Organisationskonzeptes für dieses Jahr und hat eine Lösung der noch anstehenden Datenschutzprobleme unter Berücksichtigung der Verhältnismäßigkeit zugesagt. Daher habe ich von der Verwaltungsleitung verlangt, daß die Mängel im Jahr 1996 endlich behoben werden und **ein alle Anwendungsbereiche des Hauses umfassendes Datenschutzkonzept** vorgelegt wird. Im Hinblick darauf habe ich bis jetzt von einer Beanstandung gem. § 29 BrDSG abgesehen.

16. Wirtschaft und Häfen

16.1 Neue Gewerbeordnung - neues DV-Verfahren?

Am 01. Januar 1996 ist die novellierte Gewerbeordnung endlich in Kraft getreten. Sie enthält nunmehr **bereichsspezifische Datenverarbeitungsregelungen.** So wird vorgeschrieben, wie und zu welchen Zwecken die Gewerbemeldestellen Daten erheben und an wen sie die Angaben übermitteln dürfen.

Jetzt geht es darum, umgehend dieser neuen Rechtslage entsprechende **Gewerbemeldeverfahren** im Lande Bremen einzuführen. In mehreren früheren Jahresberichten (vgl. zuletzt 16. JB, Ziff. 9.1) habe ich darauf aufmerksam gemacht, daß das in der Stadt Bremen mit dem Einwohnermeldesystem verknüpfte DV-Verfahren den datenschutzrechtlichen Vorgaben nicht entspricht. Trotz der langen Übergangsphase seit der Verabschiedung der novellierten Gewerbeordnung im November 1994 gibt es noch immer kein datenschutzgerechtes Gewerbemeldeverfahren. Ich kenne zwar die mehrjährigen Bemühungen des Innensenators, die Gewerbeordnung EDV-technisch umzusetzen, konkrete Konzepte liegen mir aber noch nicht vor.

16.2 Transeuropäisches Netz: Informationssystem für die Häfen

16.2.1 Das Projekt EIES

Mit Förderung der Europäischen Union wird derzeit u. a. beim Hafensenator Bremens das **EUROPEAN INFORMATIONS EXCHANGE SYSTEM (EIES)** konzipiert. Darüber hat er mich im September 1995 unterrichtet. An dem Projekt nehmen außer den bremischen Häfen auch die Häfen von Brest und Bordeaux in Frankreich und von Santander in Spanien teil. In den jeweiligen Häfen und deren Regionen schließt das Projekt neben den eigentlichen Hafenbehörden auch Forschungsinstitute und die Hafenwirtschaft mit ein. So beteiligen sich in Bremen z. B. Schiffsmakler, Spediteure, Reeder, Umschlagsbetriebe, der Zoll, die Feuer-

wehr, das Bremer Institut für Betriebstechnik und angewandte Arbeitswissenschaft (BIBA), das Institut für Seeverkehrswirtschaft und Logistik (ISL) und die Datenbank Bremische Häfen (dbh).

Alle diese Einrichtungen und Betriebe sind (in kleinen Bereichen über BrePos) oder werden untereinander vernetzt und sollen über electronic mail Informationen und Daten austauschen können. Gedacht ist in der Weiterentwicklung an ein **modernes Hochgeschwindigkeitsnetz** für die Übertragung von Multimedia-Angeboten und für Videokonferenzen. Mit dieser Kommunikationsform können bei besonderen Situationen (Unfälle, Umweltgefahren oder -schäden, Gefahrguttransporte und -gefahren) die Experten von Feuerwehr, Seeberufsgenossenschaft, Wasserschutzpolizei, Hafeninspektion, versendenden Spediteure, die Makler usw. genaue Gefahrenanalysen in Bild und Ton vornehmen und Maßnahmen absprechen. Daneben können Informations- und Werbedaten der beteiligten Betriebe, Einrichtungen und Häfen ausgetauscht und verbreitet werden.

16.2.2 Die datenschutzrechtliche Dimension

Dieses System, d. h. die auch grenzüberschreitende Übertragung von Bildern und Daten über Schiffsbewegungen und besondere Gefahrenlagen, ist insoweit datenschutzrechtlich relevant, als mit schiffsbezogenen Angaben auch personenbezogene Daten von Mitarbeitern, verantwortlichen Eigentümern, Verfügungsberechtigten, Crewmitgliedern u. a. mitgeteilt werden. **Für Datenübermittlungen aus bremischen Häfen** sind dabei zunächst die Datenschutzbestimmungen des Bremischen Hafengesetzes (§ 6a) und der Hafenordnung (§§ 55 ff) sowie ergänzend das Bremische Datenschutzgesetz (§§ 13, 16 und 17) anzuwenden. Bei Datentransfers ins Ausland ist - so verlangt es auch die EU- Datenschutzrichtlinie (vgl. dazu Ziff. 5.1) von den nationalen Gesetzgebern - die Vergleichbarkeit des Schutzniveaus im Zielland zu prüfen. Die derzeit mit Häfen am Projekt beteiligten anderen Staaten Frankreich und Spanien erfüllen aufgrund ihrer eigenen Datenschutzgesetzgebung diese Voraussetzung.

Ich habe gerne dem Wunsch des Häfensenators entsprochen, dieses europäische Pilotprojekt datenschutzrechtlich zu begleiten.

17. Bauwesen

17.1 Anschriften von Bauherren an das Statistische Bundesamt

Der Senator für Bau, Verkehr und Stadtentwicklung hat mir ein Schreiben des **Statistischen Bundesamtes** vorgelegt, wonach dieses offensichtlich sämtliche Bauordnungsbehörden im Bundesgebiet gebeten hat, ihm „auf freiwilliger Grundlage" **Anschriften-Verzeichnisse von Bauherren und Bauträgern** genehmigter Bauvorhaben zur Verfügung zu stellen. Ziel dieser Aktion des Statistischen Bundesamtes ist es, sich an die Betroffenen zu wenden und sie um die freiwillige Überlassung ihrer Abrechnungsunterlagen zu bitten. Das Bundesamt will mit den Daten Informationen für die Umstellung der **Baupreisindizes** auf das Jahr 1995 als neues Basisjahr gewinnen. Dazu will es ein neues Wägungsschema zur Gewichtung der Preisreihen für einzelne Bauleistungen ausarbeiten.

Da diese Erhebung nicht zur Durchführung einer gesetzlich geregelten amtlichen Bundesstatistik erfolgt, besteht insoweit keine Rechtspflicht für Auskünfte an das Statistische Bundesamt. Auch liegen die Voraussetzungen für eine Datenübermittlung ohne Einverständnis der Betroffenen nach § 13 Abs. 1 BrDSG nicht vor. Daher habe ich die Bauordnungsbehörden in Bremen und Bremerhaven gebeten, die erwünschten Anschriften nur mit vorheriger **Einwilligung** der Bauherren zu übermitteln. Außerdem habe ich die anderen Datenschutzbeauftragten des Bundes und der Länder hierüber informiert, die, soweit sie zu dieser Frage Stellung genommen haben, meine Auffassung teilen.

18. Finanzen

18.1 Fragebogen zum häuslichen Arbeitszimmer

Durch eine Eingabe bin ich auf einen von den Bremer Finanzämtern verwandten **Fragebogen** zur steuerlichen Beurteilung von **Aufwendungen für ein häusliches Arbeitszimmer** aufmerksam gemacht worden. Mit diesem Fragebogen werden z.B. Angaben über die Art, den Anschaffungszeitpunkt und die Kosten der Raumausstattung (z. B. Möbel, Geräte, Dekoration) erhoben. Außerdem sollen Grundrißskizzen und Fotos der gesamten Wohnung und des Arbeitszimmers beigefügt

werden. Dabei sollen die Nutzungsart der einzelnen Räume, Balkone, Terrassen und Loggien gekennzeichnet, aber auch Fenster, Türflächen, Schiebetüren und Wanddurchbrüche angegeben werden.

Die Erhebung derart detaillierter Angaben halte ich für „normale" Steuererklärungen für überzogen und daher nicht zulässig. In der Regel werden Informationen über die Art und den zeitlichen Umfang der Nutzung des Arbeitszimmers sowie über das Verhältnis der Arbeitszimmer-Fläche zu den übrigen Räumen ausreichen. Ausnahmen mit weitergehendem Informationsbedarf (z. B. mehrere Arbeitszimmer in einer Wohnung etc.) sind selbstverständlich denkbar, können dann aber durch Rückfrage beim Steuerpflichtigen geklärt werden.

Die Oberfinanzdirektion sagte eine **Überarbeitung der Vordrucke,** in Abstimmung mit den übrigen Oberfinanzdirektionen, zu.

18.2 Fragebogen zu privaten PC

Ein anderer nicht weniger bemerkenswerter Fragebogen der Finanzbehörden betrifft die steuerliche Berücksichtigung der Aufwendungen für **private Computer,** die **dienstlich** genutzt werden. So werden z. B. Angaben zum Betriebssystem und zur Programmiersprache (!) verlangt sowie eine Beantwortung der Frage, ob mit dem Gerät komplizierte Berechnungen vorgenommen werden.

Bei der Konzeption dieses Vordrucks ging die Steuerbehörde offensichtlich davon aus, daß höhere Anschaffungspreise auch als Indiz für eine dienstliche oder überwiegende dienstliche Benutzung des privaten Computers gewertet werden können. Ist schon diese Annahme angesichts der Marktentwicklung der letzten Jahre durchaus zweifelhaft, kommt hinzu, daß das Formular die Computerentwicklung bei den inzwischen veralteten sog. 286/386er Rechnern enden läßt.

Auch in diesen Fällen sollte mithin der Steuerbürger nur mit solchen Fragen behelligt werden, die aktuelle und strikt auf die steuerliche Erfassung bezogene Informationen erheben. Ich habe deshalb von der OFD eine Überarbeitung dieses Vordrucks erbeten.

19. Datenschutz in der Privatwirtschaft

19.1 Das bundesweite Telefonverzeichnis auf CD-ROM - ein unzulässiges Adreßregister

Schon vor Jahren (vgl. 14. Jahresbericht, Ziffer 1.6.2) hatte ich darüber berichtet, daß die CD (= Compact Disc) zunehmend als Massendatenspeicher in der Datenverarbeitung verwendet wird und daß ein Tochterunternehmen der damaligen Deutschen Bundespost Telekom dazu übergegangen ist, das Telefonbuch mit allen oder regionalisierten Eintragungsdaten auch auf CD-ROM (= Compact Disc - Read Only Memory) herauszugeben. Schon damals habe ich auf die großen Risiken für das informationelle Selbstbestimmungsrecht des Einzelnen hingewiesen, die mit dieser Form der Informationsbereitstellung verbunden sind, sowie auf Defizite bei den datenschutzrechtlichen Regelungen.

In der Zwischenzeit sind weitere private Anbieter auf dem Markt, die Telefonbuchdaten auf CD-ROM für handelsübliche Personalcomputer in entsprechender Ausstattung (z. B. CD-ROM-Laufwerk; DOS-Betriebssystem, Windows) vertreiben. Auch das Tochterunternehmen der Deutschen Telekom AG hat ihr Angebot erweitert (z. B. Einbeziehung weiterer Kundenverzeichnisse der Telekom).

Stand bisher der Preis für diese CD-ROM ihrer größeren Verbreitung im Wege, so ist seit Mitte 1995 diese Schranke weitgehend weggefallen. Die Telefon-CD-ROM eines privaten süddeutschen Unternehmens wird seither für weniger als 50,-- DM in Kaufhäusern, Computerläden etc. verkauft.

Auf dieser Telefonbuch-CD-ROM sind die Daten aller etwa 135 Telefonbücher der Bundesrepublik Deutschland enthalten, wobei bestimmte Eintragungen (z. B. Werbeeinträge oder Eintragungen in größerer Schrift) derzeit noch ausgenommen sind. Die etwa dreißig Millionen Datensätze sollen durch Abscannen der Telefonbücher, einer allgemein zugänglichen Datensammlung, gewonnen worden sein. Bis Ende 1995 sollen etwa sieben- bis achthunderttausend Stück dieser Telefon-CD-ROM verkauft worden sein.

Mit dieser CD-ROM und ihrem Such- und Auskunftsprogramm ist es nicht nur möglich, unbekannte Telefonnummern zu ganz oder teilweise bekannten Namen und vollständigen und unvollständigen Anschriften zu suchen und auszugeben

(wie beim Telefonbuch und der Telefonauskunft), sondern auch die zu einer bekannten Telefonnummer unbekannte oder nur teilbekannte Anschrift eines Teilnehmers (sog. Invert-Suche). Möglich ist außerdem, die Telefonnummern einzelner Häuser oder Straßen oder ganzer Ortsteile zu suchen und sortiert auszugeben. Denkbar ist ferner, die Daten der Telefon-CD-ROM in den Datenbestand einer speziellen PC- oder DV-Anwendung zu übernehmen und mit anderen Datenbeständen zu verknüpfen (z. B. zu Marketing- und Werbezwecken, im Versand- und Adreßhandel etc.).

Die Datenschutzaufsichtsbehörden sahen sich veranlaßt, angesichts des hohen Verbreitungsgrades dieser CD-ROM und vieler Bürgereingaben sich eingehender mit der datenschutzrechtlichen Problematik und Zulässigkeit derartiger Verzeichnisse auf CD-ROM zu beschäftigen. Folgende Fälle werden unterschieden:

— Kundenverzeichnisse der Deutschen Telekom AG und anderer Telekommunikations(TK)-Dienstleistungsunternehmen

— Herausgabe derartiger Verzeichnisse durch Unternehmen, die nicht als TK-Dienstleistungsunternehmen zu verstehen sind

19.1.1 Kundenverzeichnisse der Deutschen Telekom AG und anderer TK-Dienstleistungsunternehmen

Soweit die Deutsche Telekom AG oder andere TK-Dienstleistungsunternehmen personenbezogene Daten ihrer Vertragskunden verarbeiten, beurteilt sich die Zulässigkeit der Führung von Kundenverzeichnissen und der Auskunftserteilung über Teilnehmernummern derzeit noch ausschließlich nach den §§ 10, 11 TDSV bzw. §§ 10, 11 UDSV. Danach dürfen die vorgenannten Stellen Verzeichnisse ihrer Kunden, mit denen sie Vertragsverhältnisse über Telekommunikationsdienstleistungen unterhalten, in Form von Druckwerken oder elektronischen Verzeichnissen veröffentlichen oder veröffentlichen lassen. In diese Verzeichnisse darf der Kunde mit Name und Anschrift eingetragen werden, soweit er nicht verlangt, daß die Eintragung ganz oder teilweise unterbleibt. Auf sein gegenüber dem Telekommunikationsunternehmen bestehendes Widerspruchsrecht ist der Kunde hinzuweisen.

Die Funktion der öffentlichen Kundenverzeichnisse besteht darin, daß aus ihnen Auskünfte über die Teilnehmernummern von Telekommunikationsanschlüssen erteilt werden dürfen. Demgemäß beschränken § 11 TDSV und § 11 UDSV die Nutzung der Kundenverzeichnisse darauf, daß im Einzelfall durch Auskunftsstellen des jeweiligen Unternehmens, das Telekommunikationsdienstleistungen erbringt, Auskunft über die Teilnehmernummer des jeweiligen Anschlusses erteilt werden darf. Hat ein Betroffener seiner Eintragung in das Kundenverzeichnis widersprochen, darf eine Auskunft über die jeweilige Teilnehmernummer nicht erteilt werden. § 11 Abs. 3 TDSV bzw. § 11 Abs. 3 UDSV sehen außerdem vor, daß über die Teilnehmernummer hinausgehende Auskünfte nur erteilt werden dürfen, wenn der Kunde sein Einverständnis schriftlich erklärt hat. Für die Fälle, in denen Anschlußinhaber bei Inkrafttreten der vorgenannten Verordnungen bereits in ein Kundenverzeichnis eingetragen waren, muß die Auskunft unterbleiben, wenn er widersprochen hat. Auf dieses Widerspruchsrecht ist der Betroffene ebenfalls ausdrücklich hinzuweisen.

Will ein Telekommunikationsunternehmen die Erteilung von Auskünften über die Teilnehmernummern einem Tochterunternehmen oder einem sonstigen Dritten übertragen, ist dies gemäß § 11 Abs. 1 Satz 2 TDSV bzw. § 1 Abs. 1 Satz 2 UDSV nur zulässig, wenn diese Stelle verpflichtet wird, die personenbezogenen Daten der Kunden lediglich für Auskunftszwecke zu verarbeiten und zu nutzen sowie die §§ 10, 11 der TDSV bzw. UDSV einzuhalten. Die vorgenannten Bestimmungen regeln also,

— welche personenbezogenen Daten der Kunden von Telekommunikationsunternehmen in ein öffentliches Kundenverzeichnis aufgenommen werden dürfen,

— für welche Zwecke die Kundenverzeichnisse durch die betroffenen Telekommunikationsunternehmen genutzt werden dürfen und

— wie dem Recht auf informationelle Selbstbestimmung durch Informationspflichten, Widerspruchsrechte und das Erfordernis der Einwilligung Rechnung zu tragen ist.

Ob die getroffenen Abwägungen des Verordnungsgebers allerdings die neuen technischen Möglichkeiten zur Darstellung und Nutzung der öffentlichen Kundenverzeichnisse und die damit verbundenen Risiken genügend berücksichtigten,

kann bezweifelt werden. So habe ich z. B. Zweifel, daß die Erstellung von Straßenlisten sortiert nach Hausnummern bzw. Teilnehmernamen oder die überregionale Selektionsmöglichkeit nach Namen noch als Auskunftserteilung im Sinne des § 11 Abs. 1 TDSV angesehen werden kann. Auch die problemlose Übernahme der CD-ROM-Daten in eigene DV-Anwendungen interessierter Firmen und Datenverarbeiter ist kritisch zu sehen. Deshalb haben die Datenschutzbeauftragten immer wieder eine Stärkung der Rechtsposition der Telefonkunden gefordert. Ihnen muß ein selektives Widerspruchsrecht gegen die Aufnahme und Veröffentlichung ihrer Daten in elektronische Verzeichnisse eingeräumt werden. Die derzeitigen Möglichkeiten, die Aufnahme ganz oder teilweise zu verhindern, sind nicht ausreichend.

19.1.2 Kundenverzeichnisse anderer Herausgeber

Bei Herstellern von Verzeichnisses, die nicht selbst TK-Unternehmen sind, könnte bereits fraglich sein, ob die Speicherung, Nutzung und weitere Verarbeitung der in öffentliche Kundenverzeichnisse aufgenommenen personenbezogenen Daten durch die abschließenden Regelungen der §§ 10,11 der TDSV bzw. der UDSV ausgeschlossen sind. Hierfür spricht, daß die vorgenannten Regelungen detaillierte Bestimmungen über den Umfang der in Kundenverzeichnissen zu speichernden Daten, den Nutzungszweck und die Wahrung der Rechte Betroffener enthalten. Darüber hinaus enthält der jeweilige § 11 Abs. 1 der vorgenannten Verordnungen ausdrückliche Regelungen auch für den Fall, daß Auskünfte über Kunden nicht durch das Telekommunikationsunternehmen selbst, sondern in dessen Auftrag durch Dritte erteilt werden sollen.

Folgt man dieser Auffassung nicht, beurteilt sich die Herausgabe derartiger Verzeichnisse auf CD-ROM nach § 29 Abs. 1 Nr. 2 BDSG. Diese Norm sieht vor, daß personenbezogene Daten aus allgemein zugänglichen Quellen (z. B. Telefonbücher) zum Zwecke der Übermittlung entnommen und gespeichert werden dürfen, wenn nicht das **schutzwürdige Interesse** des Betroffenen am Ausschluß der Speicherung **offensichtlich überwiegt.**

Diese Ausnahme liegt vor, wenn die Verwendungsbeschränkungen und Gestaltungsrechte der Telefonkunden, wie sie TDSV und UDSV gewähren, mißachtet werden. Dies gilt insbesondere, wenn die sog. **Invert-Suche** erlaubt wird, wie dies bei der oben (vgl. Ziff. 19.1) erwähnten Telefon-CD-Rom einer süddeutschen Firma der Fall ist. Diese Suchform ermöglicht vom Anschlußinhaber unerwünschte Kontakte Dritter, wie Hausbesuche, direkte Ansprache o. ä.

Ich habe die Auffassung der für dieses Herstellerunternehmen zuständigen baden-württembergischen Aufsichtsbehörde, wonach die Herausgabe elektronischer Telefonbücher in dieser Form **unzulässig** ist, auch öffentlich unterstützt.

Die Rechtslage wird sich zugunsten der Telefonteilnehmer ändern, wenn die **neue TDSV** (dazu o. Ziff. 6.2.6) in Kraft getreten sein wird.

19.2 Immer Ärger mit den Banken? - Ausgewählte Beschwerdefälle

19.2.1 Kontoeröffnung: Warum eine Ausweiskopie?

Ein Bremerhavener Kreditinstitut war dazu übergegangen, unter Hinweis auf Vorschriften des **Geldwäschegesetzes** und der **Abgabenordnung** generell bei einer Kontoeröffnung Fotokopien der vorgelegten Ausweisdokumente anzufertigen. Gegen diese Praxis wandte sich die Beschwerde eines Bürgers.

Die Bank war zwar bereit, in diesem Einzelfall eine Ausnahme zu machen, beharrte aber generell auf der nach ihrer Auffassung auch vom Bundesaufsichtsamt für das Kreditwesen verlangten Handhabung.

Die Kreditwirtschaft ist zwar verpflichtet, nach den o. a. Gesetzen Aufzeichnungen aus Dokumenten vorzunehmen, die eine **eindeutige Identifizierung** des Kunden ermöglichen. Sinn und Zweck dieser Vorschrift ist es nämlich, daß niemand auf einen falschen Namen für sich oder einen Dritten ein Konto einrichten kann. Das Kreditinstitut hat mit anderen Worten die Rechtspflicht, sich bei der Kontoeröffnung Gewißheit über Person und Anschrift der Verfügungsberechtigten zu verschaffen und diese Angaben festzuhalten.

Hierzu sind aber in der Regel Name, Anschrift und Geburtsdatum, ggf. noch die Nummer des Dokuments und die Ausstellungsbehörde, ausreichend. Nicht erforderlich sind dagegen die weiteren aus einer Ausweiskopie ersichtlichen Informationen wie z. B. Haar- und Augenfarbe, Größe oder Aussehen (Lichtbild).

Auf meine Intervention hin hat die betroffene Bank die Frage des Umfangs der Legitimationsprüfung noch einmal dem Bundesaufsichtsamt für das Kreditwesen vorgelegt, das geantwortet hat, daß die **schriftliche Aufzeichnung** genüge. Das Kreditinstitut hat mir daraufhin zugesichert, in Zukunft auf eine Ausweiskopie zu verzichten und eine entsprechende Arbeitsanweisung für die Mitarbeiter des Hauses zu erlassen.

19.2.2 Kontoantrag: Zu viele Fragen

Immer wieder beklagen sich Bürger über die vielen Angaben, die ihnen bereits bei einer **Kontoeröffnung** abverlangt werden. Im Fall einer Bremer Bürgerin, die sich an mich gewandt hat, enthielt das **Antragsformular** u. a. detaillierte Fragen zur beruflichen Stellung (Selbständige/r, Angestellte/r, Arbeiter/in, Beamtin/Beamter, in Ausbildung, im Ruhestand sowie weitere Angaben zu Beruf und Branche) und zu Familienstand und -situation (verheiratet, ledig, verwitwet, geschieden, Anzahl der unterhaltsberechtigten Kinder).

Dabei ging es noch nicht einmal um die Einrichtung eines Girokontos mit Überziehungskredit, sondern um die Eröffnung eines rein auf Guthabenbasis geführten Kontos für ein **Sparbuch.** Der Vordruck sah keine Differenzierung nach Kontoarten vor; es fehlte ein Hinweis darauf, ob in jedem Fall alle abgefragten Daten vollständig angegeben werden müssen.

Ich vertrete die Auffassung, daß dieser **Datenkatalog** bei Eröffnung eines Sparkontos **zu umfangreich** und daher eine derart weitgehende Erhebung und Speicherung von Kundenangaben nicht zulässig ist. Es fehlt der nach § 28 Abs. 1 BDSG erforderliche unmittelbare sachliche Zusammenhang der „überschüssigen" Daten mit dem konkreten Vertragsverhältnis (Bankvertrag/Kontoeröffnung).

Da es sich um Formulare eines Kreditinstitutes handelt, das bundesweit agiert, werde ich diesen Vorgang im Abstimmungsgremium der obersten Aufsichtsbehörden für den Datenschutz weiterverfolgen, um eine koordinierte Reaktion sicherzustellen.

19.2.3 Kontoführung: Adreßänderung ohne Kundenauftrag

Eine Frau hatte sich nach der Trennung von ihrem Mann eine eigene Wohnung genommen und auch ihrem Kreditinstitut die neue Anschrift mitgeteilt. Nachdem sie dorthin rund ein Jahr lang ihre Bankpost erhalten hatte, mußte sie plötzlich feststellen, daß das Kreditinstitut ihre Adresse - ohne sie vorher zu befragen - einfach auf die ihres getrennt lebenden Ehemannes umgestellt und dorthin auch ihre Kontoauszüge geschickt hatte.

Die Betroffene beschwerte sich bei mir über die eigenmächtige Anschriftenänderung sowie darüber, daß durch die falsche Zustellung dem Ehemann Informationen über ihren Kontostand zugänglich gemacht worden seien.

Meine Nachfrage ergab, daß die **Adreßänderung** aufgrund einer Mitteilung der Nach- und Rücksendestelle beim Postamt Bremen 1 erfolgt war. Anscheinend hatte ein Postzusteller den Briefkasten der Beschwerdeführerin nicht gefunden. Nach Auskunft der Nachsendestelle handelt es sich um einen Kundenservice, der gerade im Bereich des Massengeschäftes keine vertieften Nachforschungen ermöglicht. Zunächst werde geprüft, ob ein Nachsendeantrag vorliegt, danach bediene man sich des Telefon- oder des städtischen Adreßbuches.

Ich habe deshalb gegenüber dem Kreditinstitut erklärt, daß ich die von der Post gefertigten **„Mitteilungen über falsche Bezieheranschriften"** für keine ausreichende Grundlage halte, um den Datensatz des Kunden zu ändern. Etwas anderes kann lediglich in den Fällen gelten, in denen der Betroffene selbst einen **Nachsendeantrag** gestellt hat. Im übrigen gehört es nach den Geschäftsbedingungen der Kreditwirtschaft in der Regel zu den Obliegenheiten des Kunden, neue Anschriften mitzuteilen. Jedenfalls sind das Telefonbuch und das kommunale Adreßbuch, die jeweils lediglich in Zeitabständen von mindestens einem Jahr herausgegeben werden, keine ausreichend sichere Datenquelle. Ich habe der Bank andere Möglichkeiten aufgezeigt, um an korrekte Kundenadressen zu gelangen.

Es bedurfte mehrerer Schreiben, bis sich bei dem Kreditinstitut die Einsicht durchgesetzt hat, daß das beschriebene Verfahren - wie im Beschwerdefall deutlich geworden - zur **Speicherung falscher Daten** und dann zu Beeinträchtigungen des Persönlichkeitsrechts führen und daher nicht weiter praktiziert werden kann. Auch das Gegenargument der Bank, falsch adressierte Briefe könnten ja nur unter Verstoß gegen Strafbestimmungen zum Schutze des Briefgeheimnisses geöffnet

werden, konnte ich nicht gelten lassen, da auch eine versehentliche Öffnung durch den unberechtigten Empfänger erfahrungsgemäß leicht möglich ist.

19.2.4 Der „kurze Dienstweg": Nachbarstreit mit Insider-Informationen

In einem anderen Fall hatte der Petent für den Bau eines Hauses vor Jahren ein Hypothekendarlehen beantragt und dieses nach Einreichung der üblichen Unterlagen in der Zweigstelle eines Bremer Kreditinstituts erhalten. Er war nicht wenig erstaunt, als Informationen aus dem **Kreditverfahren** und Fotokopien dieser Unterlagen in einem **nachbarrechtlichen Streitverfahren** vor dem Amtsgericht Bremen von dem Gegenanwalt in den Prozeß eingeführt wurden. Der Prozeßgegner, sein Nachbar, war Leiter einer anderen Filiale desselben Kreditinstituts und hatte in dieser Eigenschaft bei der für den Eingeber zuständigen Zweigstelle nachgefragt und sich u. a. dessen notariellen Kaufvertrag übermitteln lassen.

Da die Vorschriften des Bundesdatenschutzgesetzes (BDSG) und damit auch meine Aufsichtsbefugnisse nur greifen, soweit Daten in oder aus **Dateien** verarbeitet werden, war Voraussetzung für mein weiteres Vorgehen, daß der Filialleiter sich die Informationen nicht (nur) aus der Kreditakte, sondern (zumindest auch) aus den im EDV-System des Kreditinstituts gespeicherten Daten beschafft hatte. Dies ließ sich nicht feststellen.

Immerhin versicherte die Bank, daß Unterlagen nur angefordert werden dürften, soweit sie für die **geschäftliche** Bearbeitung benötigt würden. Ein besonderer Interessennachweis durch die anfragende Stelle sei jedoch nicht notwendig und auch nicht praktikabel. Die abgebende Filiale sei von einem normalen Vorgang ausgegangen. Es handele sich um einen Einzelfall, „der unter vielen tausend Bearbeitungsfällen vorgekommen ist". Ein Systemfehler, der zur Änderung von Arbeitsabläufen zwinge, liege nicht vor.

Da gem. § 27 Abs. 2 BDSG die Vorschriften des BDSG nicht für die Verarbeitung und Nutzung personenbezogener Daten in **Akten** gelten, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer Datei entnommen worden sind, ergaben sich für mich keine weiteren Handlungsmöglichkeiten (zur notwendigen Aufhebung dieser Einschränkung des Anwendungsbereichs des BDSG vgl. o. Ziff. 5.1.1).

19.2.5 Marktforschung: Kundenlisten in falschen Händen

19.2.5.1 Der Sachverhalt

Bei der Kabelzeitung Bremen waren im Sommer 1995 Teile einer Liste aufgetaucht, die auf 244 Seiten rund 2.500 Datensätze über **Kunden** und **Kontaktpersonen** eines Bremer Kreditinstituts enthielt. Der Datensatz zu jeder Person umfaßte neben Name und Anschrift bzw. Firmenanschrift weitere Schlüsselnummern, u.a. auch die bankinterne Kundennummer.

Wie sich aufgrund meiner Nachforschungen herausstellte, war die Liste von der Bank erstellt und einem **Marktforschungsinstitut** in Hamburg zur Verfügung gestellt worden. Das Institut sollte eine gezielte Verbraucherbefragung im Kunden- und Interessentenkreis des Kreditinstituts durchführen, um auf der Grundlage der Umfrageergebnisse über eine Anzeigen- und Werbekampagne zu entscheiden. Vorgesehen war, aus allen Namen rund 100 Personen auszuwählen, bei denen Interviews durchgeführt werden sollten. Das Hamburger Institut schaltete hierfür ein befreundetes Unternehmen in Bremen ein und übermittelte dorthin auch die komplette Liste. In Bremen wurden verschiedene Teile der Liste kopiert und Interviewern an die Hand gegeben. Auf welche Art und Weise die Unterlagen an die **Kabelzeitung** gelangt war, ließ sich allerdings nicht mehr mit Sicherheit feststellen.

19.2.5.2 Kritische Bewertung

Meine Überprüfung bei der betroffenen Bank ergab, daß es weder schriftliche Unterlagen über vertragliche Abmachungen mit dem Hamburger Institut gab, noch in sonstiger Form datenschutzrechtliche Vorgaben für die Verarbeitung gemacht wurden. Es fehlten auch Regelungen über die Datenweitergabe und die Einschaltung von Unterauftragnehmern.

In diesem Bericht kann ich die rechtsdogmatischen Differenzierungen meiner ausführlichen Stellungnahme nicht im einzelnen wiedergeben. Im Ergebnis habe ich jedenfalls bereits die erste **Übermittlung der Datenliste** durch das Kreditinstitut

an das Meinungsforschungsinstitut für **datenschutzrechtlich unzulässig** bewertet. Weder hielt sie sich innerhalb der Zweckbestimmung des Bankvertrages mit dem jeweiligen Kunden noch konnte die Zulässigkeit aus anderen Normen des BDSG abgeleitet werden. Auch die Allgemeinen Geschäftsbedingungen der Kreditwirtschaft selbst waren nicht eingehalten; danach dürfen Informationen über Kunden von einer Bank nur weitergegeben werden, wenn gesetzliche Bestimmungen dies gebieten, der Kunde eingewilligt hat oder die Bank zur Erteilung einer Bankauskunft befugt ist.

Jedenfalls war der **Umfang** des übermittelten Datensatzes zur Durchführung der Befragungsaktion nicht erforderlich. Die Offenlegung der **Kundennummer** war nicht nur für diesen Zweck überflüssig, sondern stellte für die Kontoinhaber ein zusätzliches Gefährdungspotential dar, weil unter dieser Nummer alle Konto- und weiteren Kundeninformationen abgespeichert und damit recherchierbar sind.

Datenschutzwidrig war auch die Handhabung, eine Liste von rund 2.500 Personendatensätzen weiterzugeben, obwohl lediglich rund 100 Personen in die Befragungsaktion einbezogen werden sollten. Auch eine auf die einzelnen Interviewer bezogene Selektion der Datensätze fand nicht statt. Unabhängig von der unzulässigen Datenübermittlung wurden auch im übrigen keine technischen und organisatorischen Maßnahmen zur Datensicherung getroffen.

Schließlich habe ich auf die **Benachrichtigungspflicht** über die erstmalige Speicherung gem. § 33 BDSG hingewiesen.

19.2.5.3 Beanstandung und Reaktion

Ich habe gem. § 29 Abs. 1 BrDSG eine **Beanstandung** gegenüber dem Kreditinstitut ausgesprochen und darauf hingewiesen, daß in Zukunft darauf zu achten ist, daß **Bankgeheimnis** und die Übermittlungsregelungen des Bundesdatenschutzgesetzes zu wahren sind und Daten von **Bankkunden** für Zwecke der Markt- und Meinungsforschung nur mit ausdrücklicher Einwilligung der Betroffenen übermittelt werden dürfen.

Weiter habe ich **empfohlen,**

- die verschiedenen Organisationseinheiten des Kreditinstituts etwa durch Hausverfügungen auf diese Rechtslage hinzuweisen,
- bei Verfahren, die vom betrieblichen Datenschutzbeauftragten nicht freigegeben worden sind, vor ihrer Anwendung die datenschutzrechtliche Zulässigkeit gesondert zu prüfen und dies zu dokumentieren,
- klare schriftliche Vereinbarungen mit Firmen, die Kundendaten im Auftrag verarbeiten, zu treffen und deren Einhaltung zu kontrollieren.

Das Kreditinstitut hat im Detail eine abweichende Rechtsansicht geäußert, im Ergebnis aber bedauert, daß die Kundenliste in falsche Hände gelangt sei. Eingeräumt wurde, daß eine sensiblere datenschutzrechtliche Behandlung der Angelegenheit wünschenswert gewesen wäre. Für die Zukunft wolle man durch eine entsprechende Information des internen Datenschutzbeauftragten an alle in Frage kommenden Organisationseinheiten sicherstellen, daß Datenübermittlungen an Dritte oder Auftragnehmer nur unter Beachtung der datenschutzrechtlichen Anforderungen und aufgrund eines schriftlichen detaillierten Auftrages erfolgten. Wie von mir vorgeschlagen soll das Ergebnis der Zulässigkeitsprüfung auch dokumentiert werden.

19.3 Wirtschaftsauskunftei: Ergebnis einer Prüfung

Im Berichtsjahr schloß ich die 1994 begonnene Prüfung einer Bremer Handels- und Wirtschaftsauskunftei ab. Diese **Auskunftei** ist gleichzeitig auch als **Inkassounternehmen** tätig. Bereits früher hatte ich dort mit kritischem Ergebnis geprüft. Auch bei der jetzigen Kontrolle ergaben sich wieder zu beanstandende Tatbestände.

19.3.1 Benachrichtigung

Die für die **Benachrichtigung** verwendeten Schreiben entsprachen nicht den Anforderungen des § 33 Abs. 1 BDSG. So ist z. B. den im **Auskunfteibereich** versandten Schreiben nicht vollständig zu entnehmen, welcher **Art** die über den Betroffenen **übermittelten** Daten sind. Gleiches gilt für den Inkasso-Bereich in bezug auf die Art der über den Schuldner **gespeicherten** Angaben. Ich habe daher die Auskunftei aufgefordert, ihre **Benachrichtigungsschreiben** an die Vorgaben des § 33 Abs. 1 BDSG anzupassen.

Mit der inhaltlichen Gestaltung der Benachrichtigungsschreiben von Wirtschafts- und Handelsauskunfteien befaßte sich auf meinen Vorschlag hin auch die von den obersten Datenschutz-Aufsichtsbehörden für diese Branche eingerichtete spezielle Arbeitsgruppe. Die Erörterung des Themas in diesem Gremium führte dazu, daß der Verband der Handelsauskunfteien, in dem alle großen deutschen Unternehmen dieses Wirtschaftszweigs vertreten sind, aufgefordert wurde, das Muster eines BDSG-konformen Schreibens vorzulegen, das von allen dem Verband angehörenden Firmen möglichst einheitlich verwendet werden kann. Der Verband sagte zu, der Aufforderung bis zum Jahresende 1995 nachzukommen.

Diese Frist ist in der Zwischenzeit verstrichen. Bislang hat weder der Verband seine Zusage eingehalten noch die von mir überprüfte Auskunftei ihre Benachrichtigungsschreiben geändert. Daher prüfe ich jetzt die Einleitung eines Ordnungswidrigkeitenverfahrens nach § 44 Abs. 1 Nr. 3 BDSG. Nach dieser Bestimmung handelt ordnungswidrig, wer vorsätzlich oder fahrlässig den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt.

19.3.2 Nachtragsmeldungen

Kritisiert habe ich auch erneut das sog. **Nachtragsverfahren** der Auskunftei (vgl. 17. JB, Ziff. 17. 2. 3). In diesem Verfahren werden den Vertragspartnern der Auskunftei **ohne erneute Anfrage** zu einem vorher beauskunfteten Fall nachträglich bekannt werdende Informationen übermittelt. Neue Daten über Firmen werden bis zu einem Zeitraum von zwölf Monaten, neue Angaben über Privatpersonen bis zu einem Zeitraum von sechs Monaten nach der erstmaligen Übermittlung mitgeteilt.

Nach § 29 Abs. 2 Nr. 1a BDSG ist Voraussetzung für eine zulässige Auskunftserteilung ein vom anfragenden Vertragspartner darzulegendes **„berechtigtes Interesse".** Dies besteht nach meiner Auffassung grundsätzlich nur für die **erstmalige** Beantwortung der zugrundeliegenden Anfrage. Nachmeldungen können nur in Einzelfällen mit besonderen Umständen in Betracht kommen. Die generelle Praxis der unaufgeforderten Weitergabe von Nachtragsdaten im dargelegten zeitlichen und sachlichen Rahmen ist jedoch unzulässig.

Die Auskunftei will diese Praxis in ihrem Bundes-Verband erörtern; das Ergebnis steht derzeit noch aus.

19.3.3 Betrieblicher Datenschutzbeauftragter und Auftragsverarbeitung

Erhebliche Mängel gab es auch in bezug auf die Aufgabenerfüllung durch den **betrieblichen Datenschutzbeauftragten.** Zu monieren waren einerseits teilweise fehlende Fachkenntnisse, andererseits das zu geringe Zeitbudget für die Ausübung seiner Tätigkeit. Nach § 38 Abs. 5 BDSG kann die Aufsichtsbehörde die Abberufung des betrieblichen Datenschutzbeauftragten verlangen, wenn dieser die für die Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt. Unter Hinweis auf diese Bestimmung forderte ich die Auskunftei auf, die deutlich gewordenen Defizite zu beseitigen.

Bei der **Auftragsdatenverarbeitung** durch den Verband, dem die von mir überprüfte Auskunftei angehört, war u.a. der Nutzungsvertrag noch nicht an § 11 des seit 1991 (!) geltenden Bundesdatenschutzgesetzes angepaßt. Ich habe das Unternehmen zu den erforderlichen Nachbesserungen aufgefordert.

Der bei dieser Prüfung ermittelte Gesamtzustand der Einhaltung des Datenschutzrechts ist auch und gerade angesichts der Sensibilität der vielfach ja ohne Kenntnis der Betroffenen von Auskunfteien erhobenen und verarbeiteten Informationen eigentlich nicht hinnehmbar. Meine **aufsichtsrechtlichen Möglichkeiten,** Unternehmen zu gesetzeskonformem Handeln zu veranlassen oder gar zu zwingen, sind aber nach dem BDSG zu schwach ausgestaltet (vgl. o. Ziff. 1.1.2.3 und 17. JB, Ziff. 17.1.2.2).

19.4 Das Datenschutzregister nach § 32 BDSG - Statistik der meldepflichtigen Stellen im Land Bremen

Die Zahl der Stellen, die zum Register nach § 32 BDSG gemeldet sind, hat sich im Berichtszeitraum erhöht. Insgesamt sind derzeit im Register 110 Unternehmen verzeichnet, von denen 90 in Bremen und 20 in Bremerhaven ihren Sitz haben. Veränderungen ergaben sich insbesondere bei der Zahl der Stellen, die personenbezogene Daten im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen. Die erhöhte Zahl der Registereintragungen ist insbesondere darauf

zurückzuführen, daß ich auch weiterhin zahlreiche Unternehmen, die der Meldepflicht nach § 32 BDSG unterliegen könnten, anschreibe und um Prüfung der Meldepflicht und ggf. Anmeldung zum Register bitte.

Die Zahl der Mailbox-Dienste hat sich um fünf erhöht. Registriert werden von mir die Mailbox-Betreiber, die ihre Tätigkeit geschäftsmäßig als Dienstleistung anbieten und für sich nicht das Presseprivileg des § 41 BDSG (Verarbeitung oder Nutzung personenbezogener Daten für journalistisch-redaktionelle Zwecke) in Anspruch nehmen können. Dies sind insbesondere Personen und Stellen, die die Nutzung ihrer Mailbox anderen juristischen oder natürlichen Personen im Rahmen einer Geschäftsbeziehung unter Verwendung von Übertragungswegen, Fest- und Wählverbindungen der Telekom ermöglichen. Einzelheiten des Registers zeigt die folgende Tabelle:

Tabelle zum Register nach § 32 BDSG (Stand: 15.01.1996)

Art der Tätigkeit	insgesamt	Bremen	Bremerhaven
1. Speicherung personenbezogener Daten zum Zwecke der Übermittlung (insgesamt)	**7**	**4**	**3**
— Auskunfteien	5	4	1
— Detekteien	1		1
— Adreßverlage/Adreßhändler	1		1
2. Speicherung personenbezogener Daten zum Zwecke der anonymisierten Übermittlung (insges.)		**2**	
— Markt-u. Meinungsforschung	2	2	
3. Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (insgesamt)	**101**	**84**	**17**
— Datenerfassung	9	9	
— Dienstleistung/RZ	77	63	14
— Mikroverfilmer	4	4	
— Mailboxdienste	6	3	3
— Datenlöschung/Datenträgervernichtung	5	5	
Gesamt	**110**	**90**	**20**

20. Die Entschließungen der Datenschutzkonferenzen im Jahr 1995

20.1 Entwurf eines Gesetzes über das Bundeskriminalamt (BKA-Gesetz) - Bundesrats-Drucksache 94/95

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1995

Zu den Beratungen des Entwurfs für ein Gesetz über das Bundeskriminalamt erklären die Datenschutzbeauftragten des Bundes und der Länder:

Auch aus Sicht des Datenschutzes ist es zu begrüßen, daß die seit langem überfälligen bereichsspezifischen Regelungen zur bundesweiten polizeilichen Datenverarbeitung insbesondere im polizeilichen Informationssystem (INPOL) nunmehr in das Gesetzgebungsverfahren eingebracht werden. Der Gesetzentwurf enthält im Vergleich zu den Vorentwürfen eine Reihe von Vorschriften, die datenschutzrechtlich positiv zu werten sind. Hierzu gehören:

— der Verzicht auf die im Vorentwurf vorgesehenen Befugnisse zur sog. „Feststellung des Anfangsverdachts";

— das Erfordernis der Einwilligung für die Speicherung von Daten über Zeugen und mögliche Opfer;

— Übermittlungsverbote bei überwiegenden schutzwürdigen Interessen der Betroffenen oder bei entgegenstehenden gesetzlichen Verwendungsregelungen;

— die Beachtung landesgesetzlicher Löschungsfristen.

Andererseits begegnet der Gesetzentwurf jedoch nach wie vor gewichtigen Bedenken, da er tiefe Eingriffe in die Rechte von Betroffenen ermöglicht, deren Voraussetzungen und Reichweite unklar oder nicht durch überwiegende Interessen der Allgemeinheit gerechtfertigt sind. Dies gilt insbesondere für

— die Verwendung des Begriffs der Straftaten von erheblicher Bedeutung ohne Definition, um welche Tatbestände es sich handelt, weil damit nicht mehr voraussehbar ist, wann die an diesen Begriff anknüpfenden Eingriffsbefugnisse zur Datenverarbeitung eröffnet sind;

— die Befugnisse der Zentralstelle zu selbständigen Datenerhebungen und Übermittlungen bis hin zum automatisierten Datenverbund mit ausländischen und zwischenstaatlichen Stellen ohne Einvernehmen mit den jeweils verantwortlichen Länderpolizeien;

— die unklare Abgrenzung der Datenverarbeitungsbefugnisse im Hinblick auf die unterschiedlichen Befugnisse zur Strafverfolgung, Gefahrenabwehr, Verhütung von Straftaten und Vorsorge für künftige Strafverfolgung sowie die fehlende klare Zweckbindungs- und Zweckänderungsregelung;

— die Befugnis zur verdeckten Datenerhebung aus Wohnungen ohne eindeutige Begrenzung auf den Schutz gefährdeter Ermittler.

Die Datenschutzbeauftragten fordern den Gesetzgeber auf, die Schwachstellen des Entwurfs auszuräumen. Insbesondere fordern sie klare verfassungskonforme Regelungen zur Auskunftserteilung an Betroffene und der Prüfrechte für INPOL-Daten dahingehend, daß die Datenschutzkontrollrechte bei der datenschutzrechtlichen Verantwortung der Stellen anknüpfen, die die Speicherung im INPOL-System selbst vornehmen oder veranlassen.

20.2 Maßhalten beim vorbeugenden personellen Sabotageschutz

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1995

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, bei Sicherheitsüberprüfungen zum personellen Sabotageschutz Augenmaß zu bewahren. Bei diesen Sicherheitsüberprüfungen werden sensible Daten, z. B. über politische Anschauungen oder Alkoholkonsum, vorbeugend erhoben, also ohne daß der Betroffene dazu Anlaß geboten hätte. Polizei und Verfassungsschutz sind routinemäßig beteiligt. Schon wenn der Betroffene im Verlauf der Überprüfung auch nur in den Verdacht der Unzuverlässigkeit gerät, kann dies bereits erheblichen Einfluß zumindest auf das berufliche Fortkommen nehmen.

Gegenwärtig sind solche Überprüfungen spezialgesetzlich für den Atombereich und für Flughäfen vorgesehen. Das Bundesministerium des Innern will jetzt klären, inwieweit Beschäftigte in anderen Einrichtungen überprüft werden sollen.

Unstreitig können solche Überprüfungen unbescholtener Bürger nur zum Schutz von „lebens- und verteidigungswichtigen Einrichtungen" angemessen sein und nur Personen betreffen, die dort an „sicherheitsempfindlichen Stellen" tätig sind. Als „lebenswichtig" sehen die Innenminister und -senatoren aber bereits Stellen an, „die für das Funktionieren des Gemeinwesens unverzichtbar sind". Damit könnten Beschäftigte in weiten Bereichen des öffentlichen Dienstes und der Wirtschaft mit Sicherheitsüberprüfungen überzogen werden.

Die Datenschutzbeauftragten meinen, daß das Persönlichkeitsrecht hier größere Zurückhaltung gebietet. Die Sicherheitsüberprüfungen müssen auf Bereiche beschränkt bleiben, in denen einer erheblichen Bedrohung für das Leben zahlreicher Menschen vorgebeugt werden muß.

Soweit in solchen Bereichen Sicherheitsüberprüfungen durchgeführt werden sollen, bedarf es einer ebenso klaren gesetzlichen Grundlage, wie bisher im Atomgesetz und im Luftverkehrsgesetz. Die zu schützenden Arten lebens- und verteidigungswichtiger Einrichtungen müssen durch Rechtsvorschrift abschließend festgelegt sein. Dabei sind für die jeweiligen Bereiche angemessene Regelungen zu treffen, die mit Rücksicht auf die Interessen Betroffener folgende allgemeine Grundsätze beachten:

- möglichst klare Vorgaben zur „Sicherheitsempfindlichkeit" in der Vorschrift und exakte Festlegung dieser Stellen durch die zuständige Behörde nach Anhörung der Personalvertretung der einzelnen Einrichtung,
- Zustimmung des Betroffenen als Verfahrensvoraussetzung,
- abschließender Katalog der regelmäßig durchzuführenden Maßnahmen, dabei Beschränkung auf vorhandene Erkenntnisse, keine Ausforschungsermittlungen,
- strenge Zweckbindung und angemessene organisatorische Vorkehrungen zu deren Gewährleistung, insbesondere Trennung von Personalakte,
- eigene Verfahrensrechte des Betroffenen, insbesondere rechtliches Gehör vor ablehnender Entscheidung und aktenkundige Gegendarstellung,
- angemessener Auskunftsanspruch, einschließlich Akteneinsicht,
- effektive Datenschutzkontrolle, auch zur Datenverarbeitung in Akten bei nicht-öffentlichen Stellen.

Im Regelfall muß zusätzlich gelten:

- Überprüfung durch die zuständige Aufsichtsbehörde selbst, nicht durch Verfassungsschutzbehörden,
- keine Einbeziehung weiterer Personen (wie Ehegatten usw.).

Ausnahmetatbestände wären - auch zum Verfahren - präzise zu fassen.

Die Praxis der Sicherheitsüberprüfungen zum personellen Sabotageschutz steht in Bund und Ländern vor einer wichtigen Weichenstellung. Sie muß klar und angemessen sein.

20.3 Datenschutz bei elektronischen Mitteilungssystemen

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1995

Es ist damit zu rechnen, daß in Zukunft mit Hilfe elektronischer Mitteilungssysteme rechtsverbindliche bedeutsame Informationen und insbesondere personenbezogene Daten über Netze ausgetauscht werden.

Die zunehmende Nutzung von elektronischen Mitteilungssystemen (electronic mail, Dokumentenaustausch über Datenfernübertragung, Message Handling Systems MHS/X.400) hat zur Folge, daß Bedrohungen wie Verlust von Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit verschärft werden, weil Unbefugte Zugriffe auf Daten und Programme erhalten können und die Übertragungswege vom Kommunikationspartner nicht sicher zu kontrollieren sind. Deshalb ist beim Einsatz solcher Systeme das Risikobewußtsein bei den Verantwortlichen sowie den Anwendern zu schärfen. In diesem Zusammenhang gewinnt der Schutz der elektronisch gespeicherten, verarbeiteten und übertragenen Information durch eine Vielzahl umfassender aufeinander abgestimmter Sicherheitsmaßnahmen an Bedeutung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, daß den folgenden Sicherheitsaspekten beim Einsatz von elektronischen Mitteilungssystemen Rechnung getragen wird:

1. Authentizität von Benutzern, Nachrichten und Systemmeldungen

   Für den Empfänger einer Nachricht muß jederzeit die Möglichkeit bestehen, anhand bestimmter Kriterien die Authentizität des Absenders, der Nachricht sowie der an ihn gerichteten Systemmeldungen (z. B. Empfangs- und Weiterleitungsbestätigungen, Sendeanforderungen, Teilnehmerkennungen, Teilnehmereinstufungen) zu überprüfen.

2. Vertraulichkeit von übertragene Daten

   Für alle Arten von Daten in elektronischen Mitteilungssystemen - Nachrichten sowie Verkehrs- und Verbindungsdaten - muß die Vertraulichkeit gewahrt bleiben. Sie ist durch geeignete Maßnahmen, z. B. kryptografische Verfahren, sicherzustellen.

3. Integrität von Nachrichten und Meldungen

   Es ist zu gewährleisten, daß bei Speicherung und Weiterleitung von Daten keine unbefugte, unerkannte Veränderung erfolgen kann.

4. Fälschungssichere Kommunikationsnachweise

   Die für die Anerkennung einer elektronischen Kommunikation erforderlichen fälschungssicheren Sende-, Empfangs- und Übertragungsnachweise müssen dem Anwender auf Wunsch zur Verfügung stehen.

5. Ausschluß von Kommunikationsprofilen

   Die Erstellung von Kommunikationsprofilen muß verhindert werden. Gespeicherte Protokollierungsdaten dürfen nur zu Zwecken des Datenschutzes und der Datensicherung (§§ 14 Abs. 4, 31 BDSG bzw. landesgesetzliche Regelungen) verwendet werden.

Empfehlungen zum Einsatz von elektronischen Mitteilungssystemen:

Zum sicheren Einsatz von elektronischen Mitteilungssystemen sind als Grundschutzmaßnahmen folgende Empfehlungen zu beachten.

1. Grundsätzlich sind nur solche Produkte einzusetzen, die die Sicherheitsfunktionen der X.400-Empfehlung aus dem Jahre 1988 erfüllen. Vorhandene Systeme - insbesondere solche, die noch auf Empfehlungen von 1984 basieren -, sollen künftig durch geeignete Zusatzprodukte hinsichtlich ihrer Sicherheit verbessert oder durch neuere Softwareversionen ersetzt werden.
2. Bei Übertragung von personenbezogenen Daten ist eine Verschlüsselung vorzusehen. Die Verschlüsselung der Daten muß mit einem hinreichend sicheren Verschlüsselungsverfahren erfolgen. Neben der Auswahl eines effektiven Verschlüsselungsalgorithmus (z. B. DES, IDEA) muß dabei insbesondere eine ordnungsgemäße Schlüsselerzeugung, -verwaltung und -verteilung gewährleistet sein. Verschlüsselungskomponenten sind durch technische, bauliche und organisatorische Maßnahmen vor dem Zugriff Unbefugter zu schützen.
3. Zur Absicherung der Integrität der Daten sollte auf Verfahren der „elektronischen Unterschrift" zurückgegriffen werden.
4. Nach Möglichkeit ist die Funktion des Systemverwalters von der des Netzwerkverwalters - insbesondere der Verwaltung des elektronischen Mitteilungssystems - aus Sicherheitsgründen zu trennen.
5. Es ist grundsätzlich separat administrierbare Hard- oder Software - z. B. in Form eines Kommunikationsservers - für das elektronische Mitteilungssystem vorzusehen.
6. Bei Verwendungen von öffentlichen Übertragungswegen, sind die vorhandenen Sicherheitsmechanismen dieser Netze z. B. geschlossene Benutzergruppen, Rufnummernidentifikation, Teilnehmerzeichengabe und automatische Rückruffunktion zur Abwehr des Zugriffs durch externe zu nutzen.
7. Zur Beweissicherung einer stattgefundenen Kommunikation sollte die eingesetzte Software folgende Funktionen beinhalten:

   — Zustellung/Empfangsnachweise

   — Sende/Empfangsübergabenachweise

20.4 Automatische Erhebung von Straßennutzungsgebühren

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1995

Gegenwärtig werden Systeme zur automatischen Erhebung von Straßenbenutzungsgebühren in mehreren Versuchsfeldern erprobt. Sie können im Rahmen der weiteren Entwicklung zu zentralen Komponenten umfassender Verkehrstelematiksysteme (z. B. Verkehrsinformation und -leitung) werden.

Mit der Einführung derartiger Verkehrstelematiksysteme besteht die Gefahr, daß personenbezogene Daten über den Aufenthaltsort von Millionen Verkehrsteilnehmern erhoben und verarbeitet werden. Exakte Bewegungsprofile können dadurch erstellt werden. Damit wären technische Voraussetzungen geschaffen, daß Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Derartige Datensammlungen wären aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil das Grundrecht auf freie Entfaltung der Persönlichkeit auch das Recht umfaßt, sich möglichst frei und unbeobachtet zu bewegen. Vor diesem Hintergrund ist es besonders wichtig, elektronische Mautsysteme datenschutzgerecht auszugestalten. Bei den anstehenden Entscheidungen sind andere Verfahren wie z. B. die Vignette einzubeziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, daß der Grundsatz der datenschutzgerechten Ausgestaltung von Systemen zur automatischen Erhebung von Straßenbenutzungsgebühren von allen Beteiligten am Feldversuch auf der BAB A 555 akzeptiert wird. Zur Umsetzung dieses Grundsatzes fordern die Datenschutzbeauftragten:

- Der Grundsatz der „datenfreien Fahrt" muß auch künftig gewährleistet sein. Über Verkehrsteilnehmer, die ordnungsgemäß bezahlen, dürfen keine Daten erhoben oder verarbeitet werden, die die Herstellung eines Personenbezugs ermöglichen. Es sind ausschließlich solche Zahlungsverfahren anzuwenden, bei denen die Abrechnungsdaten nur dezentral beim Verkehrsteilnehmer gespeichert werden. Die Verkehrsteilnehmer dürfen jedoch nicht gezwungen werden, einen lückenlosen Nachweis über ihre Bewegungen zu führen.
- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Möglichkeit einer flächendeckenden Kontrolle ist von vornherein technisch und rechtlich auszuschließen. Die Gebührenkontrolle ist so zu gestalten, daß die Identität des Verkehrsteilnehmers nur dann aufgedeckt wird, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Gebühren nicht entrichtet worden sind.
- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Verkehrsteilnehmer durchschaubar sein. Der Verkehrsteilnehmer muß jederzeit über sein Guthaben, die Abbuchung und den eventuellen Kontrollvorgang informiert sein.
- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, daß sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.

Die hierbei anzuwendenden Verfahren wären gesetzlich abschließend vorzugeben. Dabei ist sicherzustellen, daß anfallende personenbezogene Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen. Ferner ist zu gewährleisten, daß Betreiber derartiger Systeme - unabhängig von ihrer Rechtsform - einer Datenschutzkontrolle nach einheitlichen Kriterien unterliegen. Die Bundesregierung wird aufgefordert, bei der anstehenden internationalen Normierung elektronischer Mautsysteme die datenschutzrechtlichen Anforderungen durchzusetzen.

20.5 Anforderungen an den Persönlichkeitsschutz im Medienbereich

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1995

Die unabhängige und unzensierte Berichterstattung durch Presse, Rundfunk und Film (Art. 5 Abs. 1 Satz 2 GG) dient der freien individuellen und öffentlichen Meinungsbildung. Das Bundesverfassungsgericht hat die freie Meinungsbildung als Voraussetzung sowohl der Persönlichkeitsentfaltung als auch der demokratischen Ordnung bezeichnet. Insofern besteht ein enger Zusammenhang zwischen der Selbstbestimmung des Einzelnen und der Medienfreiheit.

Die rasante Entwicklung der Medientechnik, die Zunahme interaktiver Teledienste und die verstärkte kommerzielle Nutzung von Pressedatenbanken eröffnen einerseits neue Informationsmöglichkeiten für den Bürger, verschärfen aber die Gefährdungen des Rechts auf informationelle Selbstbestimmung. Diesen Gefährdungen muß der Datenschutz auf rechtlicher und technisch-organisatorischer Ebene angemessen begegnen.

Electronic Publishing und Medienarchive

Neue Formen der Verbreitung von Informationen über Netze und auf elektronischen Datenträgern führen in bisher unbekanntem Maß zu großen Informationsbeständen, in denen potentiell jedermann gezielt auf personenbezogene Daten zugreifen kann. Zudem öffnen Medienarchive, die bislang ausschließlich für journalistische Zwecke genutzt wurden, riesige Datensammlungen für medienfremde Nutzer. In Persönlichkeitsrechte wird dann besonders tief eingegriffen, wenn auch lange zurückliegende Publikationen praktisch von jedermann recherchiert werden können. Damit droht das in verschiedenen Rechtsbereichen vorgesehene „Recht auf Vergessen" wirkungslos zu werden, das z. B. durch die Löschungsvorschriften für das Bundeszentralregister gewährleistet werden soll.

Angesichts dieser Entwicklungen muß die Reichweite der datenschutzrechtlichen Sonderstellung der Medien („Medienprivileg") neu bestimmt werden. Es ist zumindest gesetzlich klarzustellen, daß die geschäftsmäßige Verwendung personenbezogener Daten außerhalb des eigenen Medienbereichs, insbesondere durch kommerzielle Pressedatenbanken, nicht unter das „Medienprivileg" fällt.

Interaktive Dienste und Mediennutzungsprofile

Auch beim Ausbau neuer digitaler Kommunikationsformen (interaktive Dienste wie z. B. Video on Demand) müssen die Persönlichkeitsrechte der Nutzer gewahrt werden. Dabei ist stärker als bisher von vornherein Wert darauf zu legen, daß datenschutzfreundliche Techniken entwickelt werden und zum Einsatz kommen, bei denen personenbezogene Verbindungs- und Nutzungsdaten erst gar nicht entstehen. Von besonderer Bedeutung sind hier anonyme Zahlverfahren, z. B. Prepaid-Karten, auf denen Informationen über die Nutzung ausschießlich dezentral gespeichert werden.

Entsprechend den Bestimmungen im Bildschirmtextstaatsvertrag und in den neueren Mediengesetzen ist sicherzustellen, daß sich die Erhebung und die Aufzeichnung von Verbindungs- und Abrechnungsdaten auf das erforderliche Maß beschränken. Dieser strikte Verarbeitungsrahmen darf auch nicht dadurch ausgeweitet werden, daß die Nutzung eines Dienstes von der Einwilligung in eine zweckfremde Verwendung der Daten abhängig gemacht wird. Die Länder sollten entsprechende einheitliche Regelungen für alle interaktiven Dienste treffen.

Da es sich bei den angesprochenen Diensten um Bestandteile einer entstehenden globalen Informationsinfrastruktur handelt, wird die Bundesregierung aufgefordert, sich auf internationaler Ebene für entsprechende Regelungen einzusetzen.

Rechte der Betroffenen gegenüber den Medien

Während die von der Berichterstattung Betroffenen - neben dem für alle Bereiche geltenden Gegendarstellungsrecht - gegenüber den öffentlich-rechtlichen und privaten Rundfunkveranstaltern inzwischen weitere elementare Datenschutzrechte besitzen, gibt es gegenüber der Presse keine vergleichbaren Regelungen.

So kann derjenige, der durch die Berichterstattung der Rundfunkveranstalter in seinem Persönlichkeitsrecht beeinträchtigt wird, in den meisten Fällen nach der Publikation Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Gegenüber der Presse hat er kein entsprechendes Auskunftsrecht. Die meisten Rundfunkveranstalter sind - anders als die Presse - zudem verpflichtet, etwaige Gegendarstellungen zu den gespeicherten Daten zu nehmen, auf die sie sich beziehen (Mitspeicherungspflicht). Ein sachlicher Grund für diese Unterscheidungen ist nicht erkennbar.

Das Presserecht sollte insofern der Rechtslage nach dem Rundfunkrecht (z. B. § 41 Abs. 3 BDSG und Art. 17 Abs. 2 ZDF-Staatsvertrag) angeglichen werden.

Gegenüber Pressedatenbanken, die nicht nur dem eigenen internen Gebrauch dienen, sollte der Betroffene darüber hinaus ein Auskunftsrecht bezüglich des zu seiner Person gespeicherten veröffentlichen Materials haben.

Öffentlichkeitsarbeit der Behörden

Personenbezogene Veröffentlichungen von Behörden können das Recht auf informationelle Selbstbestimmung erheblich beeinträchtigen. Das gilt für die Personen, auf die die Aktivitäten der Behörde unmittelbar gerichtet sind, wie auch für andere Verfahrensbeteiligte (wie z. B. Einwender, Opfer von Straftaten, Zeugen) und im besonderen Maße für unbeteiligte Personen aus dem sozialen Umfeld des Betroffenen. Deshalb ist bei der Weitergabe von Daten aus Strafermittlungsverfahren an die Medien besonders zurückhaltend zu verfahren.

Für den Umfang des Anspruchs der Medien auf Weitergabe personenbezogener Daten in Form von Presseerklärungen und Auskünften gibt es keine konkreten gesetzlichen Festlegungen. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für geboten, daß der Gesetzgeber Kriterien für die Abwägung zwischen dem Persönlichkeitsrecht des Betroffenen und der Freiheit der Berichterstattung durch Rundfunk und Presse deutlicher als bisher festlegt. Dafür kommen die Vorschriften des Landespresserechts, in besonders sensiblen Bereichen aber auch spezialgesetzliche Regelungen wie etwa die Strafprozeßordnung in Betracht.

Gerichtsfernsehen

Die Datenschutzbeauftragten des Bundes und der Länder treten den in jüngster Zeit zunehmend erhobenen Forderungen nach einer Aufhebung des Verbots der Hörfunk- und Fernsehberichterstattung aus Gerichtsverhandlungen entgegen. Insbesondere bei Strafprozessen vor laufenden Mikrofonen und Kameras würde es unweigerlich zu einer gravierenden Beeinträchtigung des Persönlichkeitsrechts der Angeklagten, der Opfer, der Zeugen und ihrer Angehörigen kommen. Selbst mit Einwilligung aller Prozeßbeteiligten darf die Hörfunk- und Fernsehberichterstattung nicht zugelassen werden.

Die Gerichtsverhandlung darf nicht zu einem masssenmedial vermittelten „modernen Pranger" werden.

20.6 Sozialgesetzbuch VII - Verfassungsgemäßer Datenschutz für Unfallversicherte erforderlich

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1995

Durch die Träger der gesetzlichen Unfallversicherung werden oft Daten der Versicherten hinter deren Rücken oder zumindest ohne deren konkrete Kenntnis erhoben und weitergegeben. Der vorliegende Referentenentwurf des Bundesministeriums für Arbeit und Sozialordnung zum Unfallversicherungs-Einordnungsgesetz - SGB-VII sieht dazu keine Änderungen vor.

Aus dem Recht auf informationelle Selbstbestimmung der Versicherten, insbesondere auf Transparenz der einzelnen Verfahrensschritte, ergeben sich mehrere grundlegende Forderungen, die bei einer Überarbeitung des Referentenentwurfes berücksichtigt werden müssen:

1. **Auskunftspflicht behandelnder Ärzte gegenüber Unfallversicherungsträgern**

   Für behandelnde Ärzte sollte eine gesetzliche Auskunftspflicht gegenüber Unfallversicherungsträgern nur festgelegt werden, soweit dies erforderlich ist für eine sachgerechte und schnelle Heilung (§§ 557 Abs. 2 RVO - § 34 Referentenentwurf SGB VII). Die gesetzliche Auskunftspflicht ist daher auf Angaben über die Behandlung und den Zustand des Verletzten zu beschränken. Danach dürfen Vorerkrankungen, die aus Sicht des Arztes mit dem aktuellen Status in keinem Zusammenhang stehen oder keine Bedeutung im Zusammenhang mit dem Arbeitsunfall oder der Berufskrankheit haben, nicht übermittelt werden (Beispiel: Handverletzung und Salmonellenvergiftung).

2. **Datenerhebung, -verarbeitung und -nutzung durch Durchgangsärzte und Berufskrankheitenärzte**

   Soweit von den Unfallversicherungsträgern bestellte Durchgangsärzte personenbezogene Daten über den Unfallverletzten erheben und Unfallversicherungsträgern und anderen Stellen mitteilen, muß dies auf eine normenklare gesetzliche Grundlage gestellt werden; die bisherige Regelung in dem zwischen den Verbänden der Kassenärzte und der Unfallversicherungsträger geschlossenen „Ärzteabkommen" reicht für die damit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen nicht aus. Entsprechendes gilt für die geplante Einführung eines Berufskrankheitenarztes.

3. **Mitteilung personenbezogener Patientendaten durch Unfallversicherungsträger an ärztliche Gutachter**

   Im Hinblick auf das Recht der Betroffenen, der Bestellung eines bestimmten Gutachters im Einzelfall aus wichtigem Grund - z. B. wegen möglicher Befangenheit - zu widersprechen, haben die Betroffenen ein besonderes berechtigtes Interesse an der Transparenz dieser Datenübermittlungen.

   Gesetzlich festzulegen ist daher, daß dem Betroffenen vor Übermittlung seiner Daten an einen Gutachter der Zweck des Gutachtens und die Person des Gutachters unter Hinweis auf sein Widerspruchsrecht nach § 76 Abs. 2 SGB X mitzuteilen sind.

4. **Eingriffe der Unfallversicherungsträger und ihrer Verbände in das Recht auf informationelle Selbstbestimmung**

   Aufgaben der Unfallversicherungsträger und ihrer Verbände und ihre Befugnisse zur Datenerhebung, -verarbeitung und nutzung - einschließlich der Auf-

bewahrungsfristen - sind differenziert in der verfassungsrechtlich gebotenen Klarheit gesetzlich zu regeln. Der vorliegende Referentenentwurf erscheint in diesem Punkt weitgehend unzureichend. So werden undifferenziert Unfallversicherungsträger und ihre Verbände behandelt, die Fachaufgaben dieser Stellen nicht oder nicht hinreichend deutlich genannt und andererseits Selbstverständlichkeiten wie das Führen von Dateien über erforderliche Daten aufgeführt. Außerdem beschränkt sich die Regelung auf die Datenverarbeitung in Dateien und übergeht die gerade im Bereich der Berufsgenossenschaften mit Gutachten und ähnlichen Unterlagen stark ausgeprägte Datenverarbeitung in Akten.

Die Zuweisung von Aufgaben und Befugnissen an Verbände der gesetzlichen Unfallversicherung muß zudem wie bei allen anderen Verbänden von Leistungsträgern durch die Einrichtung einer staatlichen Aufsicht ergänzt werden.

Soweit Vorschriften der Unfallversicherungsträger und ihrer Verbände (z. B. Unfallverhütungsvorschriften) durch Regelungen über die Erhebung, Verarbeitung und Nutzung sensibler medizinischer Daten in das Recht auf informationelle Selbstbestimmung eingreifen, sind diese Eingriffe gesetzlich zu regeln.

5. Anzeige eines Berufsunfalls und einer Berufskrankheit

Bei Datenschutzkontrollen der bisherigen Anzeigen von Berufsunfällen und -krankheiten hat sich gezeigt, daß der Umfang der an die verschiedenen Stellen übermittelten Daten zum Teil dem Grundsatz der Verhältnismäßigkeit, insbesondere der Erforderlichkeit nicht Rechnung trägt. Der Inhalt dieser Anzeigen muß an diesen Grundsätzen gemessen neu festgelegt werden.

6. Zentraldateien mehrerer Unfallversicherungsträger oder ihrer Verbände

Zweck und Inhalt zentral geführter Dateien sind in angemessenem Umfang gesetzlich präzise zu regeln. Dasselbe gilt für die Datenverarbeitung und -nutzung sowie die Festlegung der jeweils speichernden Stelle.

Die rechtzeitige Beteiligung des jeweils zuständigen Bundes- oder Landesbeauftragten für den Datenschutz vor Einrichtung einer Zentraldatei ist vorzusehen.

7. Anforderung medizinischer Unterlagen bei anderen Sozialleistungsträgern

Der in § 76 Abs. 2 SGB X vorgesehene Hinweis auf das Widerspruchsrecht gegen die Übermittlung medizinischer Daten geht stets dann ins Leere, wenn bei der speichernden bzw. übermittelnden Stelle kein Verwaltungsverfahren läuft.

Es ist daher festzulegen, daß ein Unfallversicherungsträger vor der Anforderung von Sozialdaten im Sinne des § 76 SGB X bei anderen Sozialleistungsträgern den Versicherten auf dessen Widerspruchsrecht nach § 76 Abs. 2 SGB X gegenüber der übermittelnden Stelle hinzuweisen hat.

8. Akteneinsichtsrecht der Versicherten

Hinsichtlich des gesetzlichen Akteneinsichtsrechts nach § 25 SGB X treten in der Praxis seitens der Unfallversicherungsträger Unsicherheiten auf, ob zum Schutz von Betriebs- und Geschäftsgeheimnissen oder Urheberrechten das Einsichtsrecht beschränkt werden muß. Hierzu ist eine gesetzliche Klarstellung geboten, daß diese Rechte dem Akteneinsichtsrecht nicht entgegenstehen.

20.7 Eingeschränkter Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1995

Die gesetzlichen Krankenkassen schließen sich zunehmend zu landesweiten oder überregionalen gesetzlichen Krankenkassen zusammen. Es stellt sich daher verstärkt die Frage, welche bzw. wie viele Geschäftsstellen solcher Krankenkassen umfassend auf alle gespeicherten Daten eines Versicherten zugreifen können.

Die Datenschutzbeauftragten halten nur folgendes für vertretbar:

1. Geschäftsstellen einer Krankenkasse können ohne schriftliches Einverständnis des Versicherten nur auf einen „Stammdatensatz" zugreifen. Dieser „Stammdatensatz" darf nur den Namen, das Geburtsdatum, die Anschrift, die Krankenversichertennummer und die betreuende Geschäftsstelle des Versicherten umfassen.

2. Lediglich eine Geschäftsstelle kann umfassend auf den Datensatz eines Versicherten zugreifen, sofern der Versicherte nicht ausdrücklich und eindeutig schriftlich in derartige Zugriffsmöglichkeiten durch weitere Geschäftsstellen eingewilligt hat.

3. Vor der Einwilligung ist der Betroffene umfassend aufzuklären. Die Daten dürfen nur zweckgebunden verwendet werden.

20.8 Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1995

Bisher ist der Gesetzgeber im Bereich der Justiz den verfassungsrechtlichen Forderungen nach ausreichenden normenklaren Regelungen über die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien nicht nachgekommen. So enthalten z. B. die bislang bekannt gewordenen Entwürfe zu einem Strafverfahrensänderungsgesetz nur unzureichende Generalklauseln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder[1] erklärt deshalb:

1. Aufbewahrung, Aussonderung und Vernichtung der Akten und die Speicherung personenbezogener Daten in Dateien im Bereich der Justiz müssen nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich geregelt werden, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung und am Zweck der Speicherung zu orientieren hat.

   Hierbei hat der Gesetzgeber die grundlegenden Entscheidungen zur Aufbewahrungsdauer selbst zu treffen. Aufgrund einer hinreichend konkreten Verordnungsermächtigung können die Einzelheiten durch Rechtsverordnung bestimmt werden.

2. Die derzeit bestehenden Aufbewahrungsfristen sind konsequent zu vereinfachen und zu verkürzen. Soweit geboten sind Verkürzungen vorzunehmen.

3. Die derzeit geltende generelle 30jährige Aufbewahrungsfrist für Strafurteile und Strafbefehle mit der Folge der umfassenden Verfügbarkeit der darin enthaltenen Informationen ist nicht angemessen. Bei der Bemessung der Aufbewahrungsfrist von Strafurteilen und Strafbefehlen sowie für die Bestimmung des Zeitpunkts der Einschränkung der Verfügbarkeit ist vielmehr nach Art und Maß der verhängten Sanktionen zu differenzieren.

   Bei der Festlegung des Beginns der Aufbewahrungsfrist sollte - abweichend von der bisherigen Praxis, nach der es auf die Weglegung der Akte ankommt - regelmäßig auf den Zeitpunkt des Eintritts der Rechtskraft der ergangenen gerichtlichen Entscheidung abgestellt werden.

   Ergeht keine rechtskraftfähige Entscheidung, so sollte die Aufbewahrungsfrist mit dem Erlaß der Abschlußverfügung beginnen.

4. Wird der Akteninhalt auf Bild- oder Datenträgern, die an die Stelle der Urschrift treten, aufbewahrt, so sind gleichwohl unterschiedliche Löschungsfristen für einzelne Aktenteile zu beachten. Aus datenschutzrechtlicher Sicht sind Datenträger zu wählen, die eine differenzierte Löschung gewährleisten. Ist bei Altbeständen eine teilweise Aussonderung technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand zu bewerkstelligen, so hat eine Sperrung der an sich auszusondernden Teile zu erfolgen.

5. Sind in einer Akte Daten mehrerer beteiligter Personen gespeichert, so ist eine Sperre hinsichtlich solcher Aktenteile, die einzelne beteiligte Personen betreffen, vorzusehen, wenn diese Aktenteile eigentlich ausgesondert werden müßten, aus praktischen Gründen aber keine Vernichtung erfolgen kann.

[1] Bei Stimmenthaltung von Hamburg

6. Bei Freisprüchen und Einstellungen des Verfahrens wegen Wegfalls des Tatverdachts ist dafür Sorge zu tragen, daß ein Zugriff auf die automatisiert gespeicherten Daten nur noch zu Zwecken der Aktenverwaltung erfolgen kann.

7. Für die Daten von Nebenbeteiligten (z. B. Anzeigeerstatter, Geschädigte) ist eine vorzeitige Löschung vorzusehen. Hinsichtlich der Hauptbeteiligten sollte eine Teillöschung der Personen- und Verfahrensdaten stattfinden, sobald die vollständigen Daten zur Durchführung des Verfahrens nicht mehr erforderlich sind.

8. Soweit Daten verschiedener Gerichtszweige oder verschiedener speichernder Stellen in gemeinsamen Systemen verarbeitet werden, ist durch rechtliche, technische und organisatorische Maßnahmen sicherzustellen, daß die Zweckbindung der gespeicherten Daten beachtet wird.

20.9 Datenschutz bei Wahlen

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1995

Bei der Durchführung von Wahlen haben sich Probleme bei der Verarbeitung personenbezogener Daten ergeben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu die folgende Entschließung[1] gefaßt:

1. Durchführung von Wahlstatistiken

Diejenigen Wahlberechtigten, in deren Wahlbezirk eine repräsentative Wahlstatistik durchgeführt werden soll, sind bereits mit der Wahlbenachrichtigung hierüber zu informieren. In allgemeiner Form ist auch im Wahllokal ein gut sichtbarer Hinweis auf die Einbeziehung in die Wahlstatistik anzubringen.

Die Statistik sollte nur in solchen Wahlbezirken durchgeführt werden, in denen jede Geschlechts- und Altersgruppe wenigstens so viele Wahlberechtigte aufweist, daß das Wahlgeheimnis mit Sicherheit gewahrt bleibt. Das Kriterium ist vom Landeswahlleiter vor der Festlegung der Auswahlbezirke zu prüfen. Gegebenenfalls sind ungeeignete Wahlbezirke auszutauschen.

Die Auszählung der Wahlberechtigten und der Wahlbeteiligung auf der Grundlage der Wählerverzeichnisse sollte durch den Wahlvorstand erfolgen, während die statistische Auszählung der Stimmzettel durch die jeweils für die Durchführung der Statistik zuständige Stelle vorzunehmen ist.

Untersuchungen, bei denen Angaben über die Wahlbeteiligung oder die Stimmabgabe aus verschiedenen Wahlen einzelfall- und personenbezogen zusammengeführt werden, gefährden das Wahlgeheimnis und sind daher unzulässig.

2. Auslegung von Wählerverzeichnissen

Durch die Einsicht in das Wählerverzeichnis besteht nach der jetzigen Rechtslage die Gefahr, daß Daten sowohl von Bürgern, über die in Melderegistern eine Auskunftssperre eingetragen ist, als auch von Bürgern, die in einer speziellen sozialen Situation leben (z. B. Justizvollzugsanstalten, Frauenhäuser, psychiatrische Kliniken, Obdachlose), offenbart werden.

Um einerseits die Kontrollmöglichkeit durch die Öffentlichkeit im Vorfeld einer Wahl weiterhin zu gewährleisten, andererseits die datenschutzrechtlichen Belange der genannten Betroffenen zu wahren und dem Mißbrauch einer Adreßrecherche vorzubeugen, fordern die Datenschutzbeauftragten des Bundes und der Länder, daß bei allen Wahlen

— entweder in den öffentlich ausliegenden Wählerverzeichnissen nur Name, Vorname und Geburtsdatum der Wahlberechtigten aufgeführt werden

— oder aber bei Wiedergabe der Adressen im Wählerverzeichnis nur Auskünfte zu bestimmten Personen an den Auskunftssuchenden erteilt werden, wenn er vorher die Adresse dieser Person angegeben hat.

Im übrigen sind Daten von Bürgern, für die in Melderegistern eine Auskunftssperre eingetragen ist, im Wählerverzeichnis nicht zu veröffentlichen.

[1] Bei Gegenstimme von Baden-Württemberg zu Nr. 4.

3. Gewinnung von Wahlhelfern

Bei der Gewinnung von Wahlhelfern sind folgende Grundsätze zu beachten:

Es dürfen nur die zur Bestellung erforderlichen Daten, wie Name, Vorname und Wohnanschrift, erhoben werden. Die Betroffenen sind über den Zweck der Datenerhebung und die weitere Datenverarbeitung umfassend zu unterrichten.

Über die Abwicklung der jeweiligen Wahl hinaus dürfen die Daten der Wahlhelfer, soweit sie nicht ausdrücklich widersprochen haben, in einer Wahlhelferdatei nur gespeichert werden, wenn sie dieser Speicherung nicht widersprochen haben. Die Wahlhelfer sind auf ihr Widerspruchsrecht hinzuweisen.

Beschäftigtendaten dürfen nur auf freiwilliger Basis übermittelt werden, sofern nicht eine besondere Rechtsvorschrift die Übermittlung zuläßt. Im Falle der Freiwilligkeit muß es den Beschäftigten möglich sein, selbst die Meldung unmittelbar gegenüber der Wahlbehörde abzugeben. Nach Gründen, die einer Übernahme des Ehrenamtes entgegenstehen, darf erst im förmlichen Verfahren durch die Wahlbehörde gefragt werden.

4. Erteilung von Wahlscheinen

Die in den Wahlordnungen des Bundes und der Länder enthaltene Regelung, nach der die Antragstellung für die Erteilung eines Wahlscheines auf einem Vordruck zu begründen ist und der Grund gegenüber der Gemeinde glaubhaft gemacht werden muß, ist aus datenschutzrechtlicher Sicht unverhältnismäßig. Da sich aus der geforderten Differenzierung der Begründung keine unterschiedlichen Rechtsfolgen ableiten, ist diese entbehrlich. Es genügt in der Antragstellung eine Erklärung des Wahlberechtigten, daß er am Tag der Wahl aus wichtigem Grund das für ihn zuständige Wahllokal nicht aufsuchen kann.

20.10 Entwurf einer Telekommunikations- und Informationsdienstunternehmen-Datenschutzverordnung (TIDSV) des Bundesministeriums für Post und Telekommunikation (Stand: 6. Juni 1995)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Das Bundesministerium für Post und Telekommunikation hat den Entwurf einer Telekommunikations- und Informationsdienstunternehmen-Datenschutzverordnung (TIDSV) vorgelegt, der auf der Grundlage des bereits seit Anfang dieses Jahres geltenden Gesetzes über die Regulierung der Telekommunikation und des Postwesens (PTRegG) den Schutz personenbezogener Daten der am Fernmeldeverkehr beteiligten Bürger regeln soll. Die Verordnung muß entsprechend der gesetzlichen Vorgabe dem Grundsatz der Verhältnismäßigkeit genügen, insbesondere hat sie die Erhebung, Verarbeitung und Nutzung der Daten auf das Erforderliche zu beschränken und ihre Zweckbindung zu gewährleisten. Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, daß der vorliegende Entwurf diesen aus der Verfassung abgeleiteten gesetzlichen Vorgaben teilweise nicht genügt.

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung vom 8. März 1991 auf die Bedeutung des Grundrechts auf unbeobachtete Kommunikation hingewiesen und gefordert, daß das Telekommunikationsdatenschutzrecht dieses Grundrecht zu sichern hat. Im Zeitalter der elektronischen Information und Kommunikation ist es geboten, die Betreiber zur Bereitstellung anonymer Nutzungsmöglichkeiten zu verpflichten und den Bürger in die Lage zu versetzen, selbst zu entscheiden, ob er seine personenbezogenen Daten preisgeben und sich den damit verbundenen Risiken aussetzen will.

Im einzelnen halten die Datenschutzbeauftragten den vorliegenden Entwurf in folgenden Punkten für verbesserungsbedürftig, auch um eine Absenkung des Datenschutzniveaus gegenüber der gegenwärtigen Rechtslage zu verhindern:

- Die Verarbeitung von Kundendaten muß auch in Zukunft ausdrücklich auf Telekommunikationszwecke und Zwecke der Informationsdienstleistung beschränkt werden; jede Aufweichung des Zweckbindungsgrundsatzes ist abzulehnen.
- Auch im Bereich des Sprachtelefondienstes soll nach dem Entwurf die Speicherung der vollständigen Rufnummer des angerufenen Teilnehmers bis zu 80 Tagen nach Rechnungsversand zur Regel werden. Bislang war dies nur vorgesehen, wenn der Anrufer einen Einzelverbindungsnachweis beantragt hat; dabei sollte es auch in Zukunft bleiben.

— Eine Auswertung der Verbindungsdaten nach Zielrufnummern auch außerhalb des Sprachtelefondienstes ohne Einwilligung des Kunden ist nach § 10 Abs. 2 Nr. 2 PTRegG unzulässig. Hiernach „dürfen Daten des Anrufenden nur mit dessen Einwilligung verwendet und müssen Daten des Angerufenen unverzüglich anonymisiert werden".

— Die Übermittlung von Verbindungsdaten an Diensteanbieter darf auch für Zwecke des Entgelteinzuges weiterhin nur mit Einwilligung des Kunden zugelassen werden, wenn der Datenempfänger sich vertraglich zur Einhaltung des Fernmeldegeheimnisses verpflichtet hat.

— Ein Einzelverbindungsnachweis sollte auch in Zukunft nur erteilt werden, wenn der Antragsteller das Einverständnis der zum Haushalt gehörenden Mitbenutzer des Anschlusses nachweisen kann.

— Die Anonymität von Anrufern bei Beratungseinrichtungen muß auch dann gewährleistet sein, wenn sie über ein Mobilfunknetz anrufen. Es ist nicht nachzuvollziehen, daß gerade an den dynamischsten und modernsten Teilbereich der Telekommunikation geringere Datenschutzanforderungen gestellt werden sollen als an das traditionelle Festnetz. Ohnehin ist eine Entwicklung absehbar, die Mobilfunk- und Festnetze zusammenwachsen läßt.

— Der Anrufer muß im Sprachtelefondienst die kostenfreie Möglichkeit haben, die Übermittlung seiner Rufnummer an den angerufenen Anschluß dauernd oder fallweise auszuschließen.

— Beim angerufenen Anschluß im Sprachtelefondienst muß auch in Zukunft die Abschaltung der Rufnummeranzeige allgemein und im Einzelfall möglich sein, damit Personen, die sich in räumlicher Nähe zum Angerufenen aufhalten, nicht zwangsläufig Kenntnis vom jeweiligen Anrufer erhalten.

— Die regelmäßige Herausfilterung der Daten solcher Verbindungen, für die tatsächliche Anhaltspunkte den Verdacht eines strafbaren Mißbrauchs von Fernmeldeanlagen oder der mißbräuchlichen Inanspruchnahme von Telekommunikations- oder Informationsdienstleistungen begründen, kommt einer präventiven Rasterfahndung der dem Fernmeldegeheimnis unterliegenden Verbindungsdaten gleich, in die bereits im Vorfeld eines konkreten Verdachts sämtliche Teilnehmer einbezogen werden. Die entsprechende Regelung sollte dieses Verfahren lediglich auf den Einzelfall beschränken.

— Hinsichtlich der Erhebung, Verarbeitung und Nutzung von Nachrichteninhalten sind die strengen Vorgaben von § 10 Abs. 2 Sätze 2 - 5 PTRegG einzuhalten. Insoweit fehlt in dem vorliegenden Entwurf eine Einschränkung auf den Einzelfall und die Verankerung der nach § 10 PTRegG vorgesehenen Informations- und Unterrichtungspflichten.

— Die geplante Umwandlung der bisherigen Telefonauskunft ist datenschutzrechtlich nur vertretbar, wenn der Kunde über die Verwendungsmöglichkeit in der Telefonauskunft und sein Widerspruchsrecht hinreichend informiert wird. So muß er insbesondere wissen, daß nicht nur seine Rufnummern, sondern sämtliche Angaben, die er für die Teilnehmerverzeichnisse freigegeben hat, auch beauskunftet und verwendet werden können, sofern er dem nicht widersprochen hat.

— Die vorgesehenen Regelungen über öffentliche Kundenverzeichnisse und die Telefonauskunft tragen den besonderen Risiken der Verbreitung von Kundendaten in elektronischer Form, etwa auf CD-ROM oder durch Abruf aus On-line-Diensten (Adreß-Selektion, bundesweite Recherche, umgekehrte Rufnummernsuche) nicht Rechnung. Der Kunde muß ein differenziertes Widerspruchsrecht erhalten, das ihm ermöglicht, seine Daten zwar in das herkömmliche Telefonbuch aufnehmen oder von der Telefonauskunft mitteilen zu lassen, eine Aufnahme in elektronische Verzeichnisse mit qualititv weitergehenden Verarbeitungsmöglichkeiten jedoch zu unterbinden.

— Der Verordnungsentwurf läßt abweichend von der gegenwärtigen Praxis bei der Deutschen Telekom AG die Erstellung von Einzelverbindungsnachweisen mit vollständigen Zielrufnummern ohne Einflußmöglichkeit der angerufenen Kunden zu. Die Anonymität des Angerufenen wird aber auch durch die Verkürzung der Zielrufnummer um die letzten drei Ziffern nicht hinreichend gewährleistet. Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung vom 9./10. März 1994 darauf hingewiesen, daß dem Schutz des informationellen Selbstbestimmungsrechts und des Fernmeldegeheimnisses des Angerufenen am besten dadurch entsprochen würde, wenn

jeder inländische Anschlußinhaber selbst entscheiden könnte, ob und gegebenenfalls wie seine Rufnummer auf Einzelverbindungsnachweisen erscheinen soll. Obwohl ein entsprechendes Verfahren in den Niederlanden bereits erfolgreich praktiziert wird, hat der Bundesminister für Post und Telekommunikation diesen Vorschlag bisher nicht aufgegriffen.

— Die Vorschriften für Bildschirmtextdienste sollten, auch im Sinne der Rechtssicherheit, möglichst weitgehend mit denen des Bildschirmtext-Staatsvertrages harmonisiert werden. Insbesondere sollte die Speicherung von Abrechnungsdaten so beschränkt werden, daß Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von den einzelnen Kunden in Anspruch genommener Angebote nicht erkennbar sind, es sei denn, der Kunde beantragt mit Einverständnis der Mitbenutzer einen Einzelverbindungsnachweis. Ferner ist vorzusehen, daß Abrechnungsdaten nicht erst sechs Monate nach Bekanntgabe der Entgeltrechnung gelöscht werden, sondern unverzüglich, wenn sie für Abrechnungszwecke nicht mehr erforderlich sind.

20.11 Datenschutz bei elektronischen Geldbörsen und anderen kartengestützten Zahlungssystemen

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. Oktober 1995

Die Datenschutzbeauftragten des Bundes und der Länder halten es für dringend erforderlich, daß bei kartengestützten Zahlungssystemen, die zunehmend in Konkurrenz zum Bargeld treten, datenschutzfreundliche Verfahren eingesetzt werden. Dabei bietet es sich an, vor allem Guthabenkarten zu verwenden. Es sollten nur solche Clearingverfahren eingesetzt werden, die weder eine individuelle Kartennummer benutzen noch einen anderen Bezug zum Karteninhaber herstellen.

Sowohl im öffentlichen Personennahverkehr als auch bei der Deutschen Bahn AG können Fahrscheine bargeldlos erworben werden. Auch Autofahrer können auf Bargeld verzichten: Beim Parken, beim Tanken, künftig auch bei der Benutzung von Autobahnen wird verstärkt auf elektronisches Bezahlen zurückgegriffen. Immer mehr Telefone und Warenautomaten werden auf bargeldlose Zahlungsverfahren umgestellt, so daß viele Artikel des täglichen Bedarfs elektronisch bezahlt werden können. Von Kreditinstituten wird die Kombination verschiedener Anwendungen auf einer Karte angestrebt, z.B. mit einer Kombination der Bezahlung für den öffentlichen Nahverkehr, Parkgebühren und Benutzungsentgelte für öffentliche Einrichtungen.

Zum elektronischen Bezahlen werden entweder Kreditkarten, Debitkarten oder Guthabenkarten eingesetzt. Bei Kredit- und Debitkarten werden sämtliche Zahlungsbeträge verbucht, dem Käufer in Rechnung gestellt, auf den Kontoauszügen ausgedruckt und für mindestens 6 Jahre gespeichert. Dagegen wird bei Guthabenkarten im voraus ein Guthaben eingezahlt und bei jeder einzelnen Zahlung das Guthaben entsprechend herabgesetzt; die Zahlungsbeträge müssen keinem Käufer zugeordnet werden.

Beim elektronischen Bezahlen entstehen sehr unterschiedliche Datenschutzrisiken. Bei Kredit- und Debitkarten besteht die Gefahr, daß die aus Abrechnungsgründen gespeicherten personenbezogenen Daten ausgewertet und zweckentfremdet genutzt werden: Informationen über den Kauf von Fahrscheinen oder über die Nutzung von Autobahnen können zu Bewegungsprofilen verdichtet werden. Das Konsumverhalten des Einzelnen wird bis ins Detail nachvollziehbar, falls auch Kleineinkäufe am Kiosk nachträglich abgerechnet werden. Durch den Datenverkauf für Werbung und Marketing können sich weitere Risiken ergeben. Demgegenüber kann bei der Verwendung von Guthabenkarten auf das Speichern personen- oder kartenbezogener Daten aus erfolgten Zahlungen verzichtet werden.

Vor allem im Kleingeldbereich ist die Nutzung von Debit- und Kreditkarten entbehrlich, da fälschungssichere Guthabenkarten auf der Basis von Chipkarten mit integriertem Verschlüsselungsbaustein zur Verfügung stehen. Falls größere Geldbeträge nachträglich per Kredit- oder Debitkarte bezahlt werden, ist darauf zu achten, daß die Abrechnung zunächst über Konten erfolgt, deren Inhaber dem Zahlungsempfänger nicht namhaft gemacht wird. Erst bei Zahlungsunregelmäßigkeiten ist es notwendig, den Bezug zum Kontoinhaber herzustellen.

Angesichts der Risiken, aber auch der von Chipkarten ausgehenden Chancen, fordern die Datenschutzbeauftragten die Kartenherausgeber und die Kreditwirtschaft dazu auf, kartengestützte Zahlungssysteme zu entwickeln, die möglichst

ohne personenbezogene Daten auskommen, und deren Anwendung so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt. Der Gesetzgeber muß sicherstellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher anonym zu bleiben.

20.12 Planungen für ein Korruptionsbekämpfungsgesetz

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995

Derzeit gibt es Vorschläge, die Bekämpfung der Korruption durch Verschärfungen des Strafrechts und des Strafprozeßrechts mit weiteren Eingriffen in das Grundrecht auf informationelle Selbstbestimmung zu organisieren. Ein Beispiel dafür ist der Beschluß des Bundesrates vom 3. November 1995 zur Einbringung eines Korruptionsbekämpfungsgesetzes.

Nach dem vom Bundesrat beschlossenen Gesetzentwurf sollen Bestechlichkeit und Bestechung in den Kreis derjenigen Tatbestände aufgenommen werden, bei deren Verdacht die Überwachung des Fernmeldeverkehrs und der Einsatz technischer Mittel ohne Wissen des Betroffenen (§§ 100a, 100c StPO) angeordnet werden dürfen.

Die Datenschutzbeauftragten weisen demgegenüber darauf hin, daß es vorrangig um Prävention, nicht um Repression geht. Die Datenschutzbeauftragten treten für eine entschlossene und wirksame Bekämpfung der Korruption mit rechtsstaatlichen Mitteln unter strikter Beachtung der Freiheitsrechte ein.

Sie wenden sich zugleich gegen eine Rechtspolitik, welche - noch bevor sie sich darüber im klaren ist, was die bisherigen Verschärfungen und Eingriffe an Vorteilen und an Nachteilen gebracht haben - auf weitere Verschärfungen und Eingriffe setzt.

Gerade gegenüber der Korruption gibt es Möglichkeiten, welche Effektivität versprechen und gleichwohl die Privatsphäre der unbeteiligten und unschuldigen Bürgerinnen und Bürger nicht antasten:

- Rotation derjenigen Mitarbeiterinnen und Mitarbeiter einer Behörde, deren Position und Aufgaben erfahrungsgemäß für Bestechungsversuche in Betracht kommen;
- Vier- und Sechsaugenprinzip bei bestimmten Entscheidungen;
- Trennung von Planung, Überwachung und Ausführung, von Ausschreibung und Vergabe;
- Prüfverfahren und Innenrevision;
- Codes of Conduct (formalisierte „Ethikprogramme") im Bereich der Wirtschaft;
- verbesserte Transparenz von Entscheidungsprozessen in der Verwaltung.

Die in den Gesetzentwürfen vorgesehene weitere Einschränkung von Grundrechten, die mit einer abermaligen Erweiterung der Telefonüberwachung verbunden wäre, ist nur vertretbar, wenn sie nach einer sorgfältigen Güter- und Risikoabwägung zusätzlich zu den o. g. Verfahrens- und Verhaltensmaßregeln als geeignet und unbedingt erforderlich anzusehen wäre.

Die Datenschutzbeauftragten verlangen, daß vor einer zusätzlichen Aufnahme von Straftatbeständen in den Katalog der Abhörvorschrift des § 100a StPO diese Abwägung durchgeführt wird.

Die Datenschutzbeauftragten fordern weiterhin, daß eine Erweiterung des genannten Straftatenkataloges nur befristet vorgenommen wird, damit sich vor einer Verlängerung die Notwendigkeit stellt, auf der Grundlage einer sorgfältigen Erfolgs- und Effektivitätskontrolle erneut die Erforderlichkeit und Verhältnismäßigkeit einer solchen Erweiterung des Grundrechtseingriffs zu überprüfen.

Die Datenschutzbeauftragten verlangen, daß der Gesetzgeber vor weiteren Eingriffen in Freiheitsrechte eine sorgfältige Güter- und Risikoabwägung vornimmt und dabei insbesondere verantwortlich prüft, ob sich die innenpolitischen Ziele mit Mitteln erreichen lassen, welche die informationelle Selbstbestimmung der Bürgerinnen und Bürger schonen.

Schließlich gibt die anstehende erneute Erweiterung des Katalogs von § 100a StPO Veranlassung, den Umfang der darin genannten Straftaten sobald wie möglich grundlegend zu überprüfen.

20.13 Weiterentwicklung des Datenschutzes in der Europäischen Union

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995

Die Konferenz der Datenschutzbeauftragten der Europäischen Union hat am 08.09.1995 in Kopenhagen in einer Resolution im Hinblick auf die für 1996 geplante Regierungskonferenz dafür plädiert, anläßlich der Überarbeitung der Unions- und Gemeinschaftsverträge in einen verbindlichen Grundrechtskatalog ein einklagbares europäisches Grundrecht auf Datenschutz aufzunehmen. Die Schaffung rechtsverbindlicher Datenschutzregelungen für die Organe und Einrichtungen der Union sowie die Schaffung einer unabhängigen und effektiven Datenschutzkontrollinstanz der EU werden angemahnt. Dieser Resolution schließt sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an. Sie hält angesichts der fortschreitenden Integration und des zunehmenden Einsatzes von Informations- und Kommunikationstechnologien in der EU eine Weiterentwicklung des Datenschutzes im Rahmen der EU für geboten.

Sie fordert die zuständigen Politiker und insbesondere die Bundesregierung auf, dafür einzutreten, daß im EU-Vertragsrecht ein Grundrecht auf Datenschutz aufgenommen wird, die materiellen Datenschutzregelungen in der EU verbessert werden, das Amt eines Europäischen Datenschutzbeauftragten geschaffen wird sowie eine parlamentarische und richterliche Kontrolle der Datenverarbeitung der im EU-Vertrag vorgesehen Instanzen sichergestellt wird.

Grundrecht auf Datenschutz

Bei einer Weiterentwicklung der Europäischen Union ist es unabdingbar, daß dem Grundrechtsschutz eine angemessene Bedeutung beigemessen wird. Dies sollte dadurch geschehen, daß die Verträge zur Europäischen Union mit einem Grundrechtskatalog ergänzt werden. Mit einer Entschließung vom 10.2.1994 hat das Europäische Parlament einen Entwurf zur Verfassung der Europäischen Union zur Erörterung gestellt, der u. a. folgende Aussagen enthält: „Jeder hat das Recht auf Achtung und Schutz seiner Identität. Die Achtung der Privatsphäre und des Familienlebens, des Ansehens (. . .) wird gewährleistet".

Die Konferenz der Datenschutzbeauftragten ist mit ihrer Entschließung vom 28.4.1992 dafür eingetreten, daß in das Grundgesetz nach dem Vorbild anderer europäischer Verfassungen ein Grundrecht auf Datenschutz aufgenommen wird. Sie hat hierfür einen Formulierungsvorschlag gemacht. Auf ihren Konferenzen am 16./17.2.1993 und 9./10.3.1994 bekräftigten die Datenschutzbeauftragten des Bundes und der Länder ihre Position. Diese Forderung wurde aber wegen des Nichterreichens der notwendigen qualifizierten Mehrheit durch den Gesetzgeber nicht umgesetzt.

In Wirtschaft, Verwaltung und Gesellschaft der Staaten der EU erhält der Dienstleistungs- und Informationssektor eine zunehmende Bedeutung. Dies hat zur Folge, daß mit hochentwickelten Informationstechnologien von privaten wie von öffentlichen Stellen verstärkt personenbezogene Daten verarbeitet und auch grenzüberschreitend ausgetauscht werden. Diese Entwicklung wird gefördert durch die Privatisierung und den rasanten Ausbau transeuropäischer elektronischer Telekommunikations-Netze. Dadurch gerät das Grundrecht auf informationelle Selbstbestimmung in besonderem Maße auf der überstaatlichen Ebene in Gefahr. Dieser Gefahr kann dadurch entgegengetreten werden, daß in einen in den überarbeiteten EU-Vertrag aufzunehmenden Grundrechtskatalog das Grundrecht auf Datenschutz und zu dessen Konkretisierung ein Recht auf unbeobachtete Telekommunikation aufgenommen werden. Dies hätte folgende positive Auswirkungen:

- Anhand einer ausdrücklichen gemeinsamen Rechtsnorm kann sich eine einheitliche Rechtsprechung zum Datenschutz entwickeln, an die sowohl die EU-Organe wie auch die nationalen Stellen gebunden werden.
- Ein solches Grundrecht wäre die Basis für eine Vereinheitlichung des derzeit noch sehr unterschiedlichen nationalen Datenschutzrechts auf einem hohen Niveau.
- Den Bürgerinnen und Bürgern wird deutlich erkennbar, daß ihnen in einklagbarer Form der Datenschutz in gleicher Weise garantiert wird wie die traditionellen Grundrechte.
- Das grundlegende rechtsstaatliche Prinzip des Datenschutzes wird dauerhaft, auch bei Erweiterung der EU, gesichert.

— Mit der rechtlichen Konkretisierung eines Rechts auf unbeobachtete Telekommunikation würde der zunehmenden Registrierung des Verhaltens der Bürgerinnen und Bürger in der multimedialen Informationsgesellschaft entgegengewirkt und der Schutz des Fernmeldegeheimnisses auch nach dem Abbau der staatlichen Monopole im Sprachtelefondienst sichergestellt.

Materielle Datenschutzregelungen

Mit der kürzlich verabschiedeten EU-Datenschutzrichtlinie wird ein großer Fortschritt für den Datenschutz auf europäischer Ebene erreicht. Dies darf aber nicht den Blick dafür verstellen, daß in einzelnen Bereichen spezifische, dringend nötige Datenschutzregelungen fehlen. Insbesondere sind folgende Bereiche regelungsbedürftig:

— Es bedarf eines für die EU-Institutionen verbindlichen eigenen Datenschutzrechts. Die datenschutzrechtliche Verantwortung der Mitgliedstaaten einschließlich ihrer Datenschutzkontrolle der Übermittlung von Daten an EU-Institutionen bleibt dabei unberührt.

— Die geplante ISDN-Datenschutzrichtlinie darf weder einer völlig falsch verstandenen Subsidiarität zum Opfer fallen noch in unzureichender Form verabschiedet werden.

— Die im Bereich der Statistik bestehenden datenschutzrechtlichen Defizite sind abzubauen.

— Es soll eine Technikfolgenabschätzung bei der Förderung und Einführung neuer Informationstechniken mit Personenbezug durch die EU obligatorisch eingeführt werden.

— In den Bereichen Inneres und Justiz sind aufeinander abgestimmte verbindliche Regelungen mit hohem Datenschutzstandard, die die Datenverarbeitung in Akten und die Sicherung der Datenschutzkontrolle mit umfassen, zu schaffen.

— Es bedarf der Harmonisierung des Arbeitnehmerdatenschutzes auf hohem Niveau in den Staaten der EU.

— Für das Personal der EU-Organe ist der Arbeitnehmerdatenschutz sicherzustellen, was z. B. bei der Durchführung von Sicherheitsüberprüfungen insbesondere unter Beteiligung von Behörden der Heimatstaaten von großer Bedeutung ist.

Es ist zu prüfen, inwieweit Informationszugangsrechte in weiteren Bereichen eingeführt werden sollen.

Europäischer Datenschutzbeauftragter

Die Konferenz der EU-Datenschutzkontrollinstanzen (25./26.5.1994, 8.9.1995) und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (25.8.1994) haben darauf hingewiesen, daß es an einer unabhängigen und effektiven Datenschutzkontrollinstanz fehlt, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der EU in seinen Rechten verletzt zu sein. Aufgabe eines Europäischen Datenschutzbeauftragten sollte die Behandlung aller Datenschutzbelange der EU sein. Dazu gehört nicht nur die Bearbeitung von Betroffeneneingaben, sondern auch die datenschutzrechtliche Beratung der EU-Organe und -Einrichtungen sowie deren anlaßunabhängige Kontrolle, die Begleitung informationstechnischer EU-Projekte und der entsprechenden EU-Normsetzung sowie die Zusammenarbeit mit den nationalen Kontrollinstanzen. Wegen der teilweise anders gelagerten Aufgaben sollen die Funktionen des Europäischen Datenschutzbeauftragten und des Bürgerbeauftragten nach den EG-Verträgen nicht vermengt werden. Die Bundesregierung sollte im Rahmen der Vorbereitung der Regierungskonferenz 1996 darauf hinwirken, daß ein unabhängiger Europäischer Datenschutzbeauftragter in den Verträgen über die Europäische Union institutionell abgesichert wird.

Parlamentarische und richterliche Kontrolle

Bei der Zusammenarbeit der EU-Staaten in den Bereichen Justiz und Inneres muß mit Besorgnis festgestellt werden, daß eine ausreichende parlamentarische und richterliche Kontrolle im EUV derzeit nicht gewährleistet ist. Die geplante Europol-Konvention ist hierfür ein Beispiel. Mit unbestimmten Formulierungen werden einem fast völlig freischwebenden Europäischen Polizeiamt informationelle Befugnisse eingeräumt, einem Amt, das keiner parlamentarischen Verantwortlichkeit und nur einer unzureichenden (teils nur nationalen) Rechtskontrolle

unterworfen wird. Zur Wahrung des Datenschutzes bei der Umsetzung gemeinsamer Maßnahmen in den Bereichen Justiz und Inneres muß daher - unbeschadet der Kontrolle durch die nationalen Datenschutzbehörden - auch eine im Rahmen ihrer jeweiligen Zuständigkeiten lückenlose Kontrolle durch die nationalen Parlamente und Gerichte sowie durch das Europäische Parlament und den Europäischen Gerichtshof sichergestellt werden.

20.14 Datenschutzrechtliche Anforderngen an den Einsatz von Chipkarten im Gesundheitswesen

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 09./10. März 1994 kritisch zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. In dem Beschluß wird die Nutzung von Patientenkarten von mehreren Voraussetzungen zur Sicherung des Persönlichkeitsrechts abhängig gemacht.

Seitdem werden in mehreren Ländern Modellversuche und Pilotprojekte durchgeführt. Die Bandbreite reicht

- von allgemeinen Patientenkarten, die an möglichst viele Patienten/Versicherte ausgegeben werden, eine Vielzahl von Krankheitsdaten enthalten und von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (z.B. VitalCard der AOK Leipzig, Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin)
- bis zu krankheitsspezifischen Karten für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (z. B. Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Datenschutzrechtlich stellen sich vor allem folgende Probleme:

- Die massenhafte Einführung der Karten erzeugt einen sozialen Druck auf die Betroffenen, sie mitzuführen und vorzuzeigen. Diesen Erwartungen wird sich der Betroffene vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehnt, verweigern können.
- Die Verwendung von allgemeinen Patientenkarten bringt die Gefahr einer pauschalen Offenbarung von medizinischen Daten mit sich.
- Dem Patienten wird die Last aufgebürdet, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten fordern alle für Kartenprojekte im Gesundheitswesen Verantwortlichen in Politik, Industrie, Ärzteschaft, Wissenschaft und in den Krankenversicherungen auf, das Recht auf informationelle Selbstbestimmung der betroffenen Patienten bzw. Versicherten zu gewährleisten. Die 50. Konferenz hält folgende Voraussetzungen für elementar:

1. Besondere Schutzwürdigkeit medizinischer Daten

Medizinische Daten sind besonders schutzwürdig, unabhängig davon, welche Technologien eingesetzt werden, ob die Patientendaten beim Arzt gespeichert und versandt oder über ein Netz abgerufen werden oder ob der Patient die Daten auf einer Chipkarte bei sich hat. Es handelt sich oftmals um belastende, schicksalshafte Daten. Zudem geht es nicht nur um Daten des Patienten, sondern auch um fremde Einblicke in die ärztliche Tätigkeit.

2. Wirksame Entscheidung der Betroffenen über die Verwendung einer Karte

Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,

- ob Daten auf einer Chipkarte gespeichert werden,
- welche der Gesundheitsdaten auf die Karte aufgenommen werden,
- welche Daten auf der Karte wieder gelöscht werden,
- ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und
- welche Daten im Einzelfall zugänglich gemacht werden.

Ein Widerruf der Entscheidung muß ohne Nachteile für die Betroffenen möglich sein. Die gleiche Freiheit der Entscheidung für oder gegen die Verwendung der Chipkarte muß für Ärzte und Apotheker gewährleistet sein. Eine wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Information über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus. Das Gesamtkonzept des Chipkarteneinsatzes und der damit verbundenen Datenverarbeitung muß für die Betroffenen überschaubar sein.

Auf der Karte darf nicht der Datensatz der Krankenversichertenkarte nach § 291 Abs. 2 SGB V, insbesondere nicht die Krankenversicherung und die Krankenversicherungsnr., gespeichert werden, da andernfalls - zumal bei allgemeinen Patientenkarten mit hohem Verbreitungsgrad - die Krankenversichertenkarte verdrängt und deren Nutzungsbeschränkungen umgangen werden.

3. Freiheit der Entscheidung

Die uneingeschränkte Freiheit der Entscheidung der Betroffenen für oder gegen die Verwendung einer Chipkarte muß gewährleistet sein, denn der Einsatz von Chipkarten im Gesundheitswesen führt keineswegs zwangsläufig zu größerer Autonomie der Patienten. Neue Technologien können sich auch als Verführung erweisen, deren Preis erst langfristig erkennbar wird. Die individuelle Entscheidung des Bürgers über die Verarbeitung seiner Daten war und bleibt ein zentrales Recht gegenüber Eingriffen in seine Freiheitssphäre. Mit der Chipkarte können sich jedoch Situationen ergeben, in denen wirkliche Freiheit, tatsächliche Wahlmöglichkeit der Betroffenen nicht mehr gewährleistet sind und durch technische und organisatorische, rechtliche und soziale Rahmenbedingungen wiederhergestellt werden müssen.

Dem Staat kommt hier eine veränderte Rolle zu: Freiheitsrechte nicht einzuschränken, sondern sie zu sichern, wo Entwicklungen des Marktes und der Technologien sowie Gruppeninteressen die Entscheidungsfreiheit des Bürgers bedrohen. Die Technologie selbst kann für die Sicherung der Freiheitsrechte ein wertvolles Hilfsmittel sein. Darüber hinaus kommt der Informiertheit der Betroffenen ein zentraler Stellenwert zu. Ihre Kompetenz zur Entscheidung und zum praktischen Umgang mit der Karte muß gestärkt werden, damit sie auch langfristig die größtmöglichen Chancen haben, ihre Interessen durchzusetzen.

Mit der Ausstellung der Karte dürfen nur die Vorteile verknüpft werden, die sich unmittelbar aus den Nutzungspraktiken der Karte selbst ergeben. Die freie Entscheidung der Betroffenen, eine Karte zu nutzen oder dies abzulehnen, darf nicht durch einen Nutzungszwang oder eine Bevorzugung von Karten-Nutzern (z. B. durch Bonuspunkte) bzw. durch eine Benachteiligung von Karten-Verweigerern eingeschränkt werden.

4. Keine Verschlechterung der Situation der Betroffenen

Durch die Einführung von Kommunikationssystemen mit Chipkarten dürfen die Betroffenen nicht schlechter gestellt werden als im konventionellen Verfahren. Die medizinische Versorgung, der Schutz der Gesundheitsdaten und die Mitentscheidungsrechte der Betroffenen müssen in Umfang und Qualität erhalten bleiben.

Das therapeutische Verhältnis Arzt/Patient darf sich durch den Einsatz von Chipkarten nicht verschlechtern. Freiheit und Vertrauen innerhalb des Arzt-Patienten-Verhältnisses sowie der Grundsatz der Abschottung der dem Arzt anvertrauten Informationen und der ärztlichen Erkenntnisse nach außen, gegen die Kenntnisnahme durch Dritte, müssen erhalten bleiben. Insbesondere muß der Gesetzgeber sicherstellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Eine Kommunikation unter Vorlage der Karte mit Personen oder Stellen außerhalb des Arzt-Patienten-Verhältnisses, z. B. Arbeitgebern oder Versicherungen, muß vom Gesetzgeber untersagt werden.

Das sich im Gespräch entwickelnde Vertrauensverhältnis zwischen Arzt und Patient darf nicht durch eine Chipkarten-vermittelte Kommunikation verdrängt werden. Verkürzte Darstellungen medizinischer Sachverhalte auf der Chipkarte - z. B. mit Hilfe von Schlüsselbegriffen - dürfen nicht zu einer Minderung der Qualität des therapeutischen Verhältnisses führen; das liegt auch im Interesse des Arztes. Der Patient muß auch weiterhin die Möglichkeit des individuellen Dialogs

wählen können. Dies schließt insbesondere die Freiheit des Betroffenen ein, eine Chipkarte im Einzelfall nicht vorzulegen, auf der Chipkarte nur einen begrenzten Datensatz speichern zu lassen oder zu entscheiden, welchem Arzt welche Informationen oder Informationsbereiche offenbart werden. Der Patient darf durch die Ausgestaltung und den Verwendungszusammenhang der Chipkarte nicht zur pauschalen Offenbarung seiner Daten gezwungen sein. So sind Daten auf der Chipkarte so zu ordnen, daß z. B. beim Zahnarzt die gynäkologische Behandlung geheim bleiben kann.

Es darf keine „Einwilligung" in Chipkarten und Chipkartensysteme mit verminderter Datensicherheit geben. Der Gesetzgeber muß die Patienten vor „billigen Gesundheitskarten" ohne ausreichende Sicherung vor einer Nutzung durch Dritte schützen.

5. Sicherstellung der Integrität und Authentizität der Daten

Zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten auf Chipkarten im Gesundheitswesen und zur Differenzierung der Zugriffsmöglichkeiten nach dem Grundsatz der Erforderlichkeit in unterschiedlichen Situationen sind kryptographische Verfahren sowie geeignete Betriebssysteme zur Abschottung unterschiedlicher Anwendungsbereiche nach dem Stand der Technik in Chipkarten und Schreib-/Lese-Terminals zu implementieren. Eine Protokollierung der Lösch- und Schreibvorgänge auf der Karte ist unverzichtbar.

Darüber hinaus ist für das infrastrukturelle Kartenumfeld (Herstellung, Verteilung, Personalisierung,. . ., Rücknahme) sicherzustellen, daß ausreichende technische und organisatorische Maßnahmen Berücksichtigung finden. Für die zur Erstellung und Personalisierung von Gesundheits-Chipkarten dienenden Systeme sowie die informationstechnischen Systeme und Verfahren, mit denen Daten auf der Chipkarte gelesen, eingetragen, verändert, gelöscht oder verarbeitet werden, muß der gleiche hohe Sicherheitsstandard erreicht werden.

6. Keine neuen zentralen medizinischen Datensammlungen

Der Einsatz von Chipkarten im Gesundheitswesen darf nicht zur Entstehung neuer zentraler Dateien von Patientendaten bei Kassenärztlicher Vereinigung, Krankenkassen, Kartenherstellern oder sonstigen Stellen führen. Dies gilt auch für das Hinterlegen von Sicherungskopien der auf der Karte gespeicherten medizinischen Daten. Es steht in der freien Entscheidung der Betroffenen, ob sie dem Arzt ihres Vertrauens eine umfassende Pflege aller Chipkarten-Daten - einschließlich der Sicherungskopien - übertragen oder nicht.

7. Leserecht des Karteninhabers

Der Karteninhaber muß das Recht und die Möglichkeit haben, seine auf der Chipkarte gespeicherten Daten vollständig zu lesen.

8. Suche nach datenschutzfreundlichen Alternativen

Angesichts der aufgezeigten Gefährdungen der informationellen Selbstbestimmung im Gesundheitswesen muß die Suche nach datenschutzfreundlichen Alternativen zur Chipkarte fortgesetzt werden.

Vorstehende Kriterien sind der Maßstab für die datenschutzrechtliche Bewertung von Projekten für die Einführung von Chipkarten im Gesundheitswesen.

Die Datenschutzbeauftragten von Bund und Ländern fordern die Gesetzgeber auf, die dringend notwendigen Regelungen zur Sicherung der Rechte von Patienten und Ärzten zu schaffen. Ebenso ist durch die Gesetzgeber den Besonderheiten der Datenverarbeitung auf Chipkarten durch bereichsspezifische Regelungen Rechnung zu tragen.

20.15 Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden)

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995

1. Für die Übermittlung von personenbezogenen Daten durch Justiz und Polizei an die Medien sollte eine bereichsspezifische Rechtsgrundlage geschaffen werden. Die Regelung sollte für den betroffenen Bürger den Umfang des Eingriffs in sein Recht auf informationelle Selbstbestimmung erkennbar machen.

2. Die Übermittlung personenbezogener Daten an die Medien ist nur ausnahmsweise gerechtfertigt, wenn das Verfahren gerade im Hinblick auf die Person des Betroffenen oder die besonderen Umstände der Tat für die Öffentlichkeit von überwiegendem Interesse ist.

3. Bei der Entscheidung, ob und in welchem Umfang personenbezogene Daten an die Medien übermittelt werden, sind die schutzwürdigen Belange der Betroffenen zu berücksichtigen. Dazu zählen insbesondere die privaten und beruflichen Folgen für das Opfer, den Beschuldigten/Angeklagten und deren Angehörige sowie die Schwere, die Umstände und die Folgen des Delikts.

4. Bei der Übermittlung von personenbezogenen Daten über Beschuldigte/Angeklagte sind auch der Grad des Tatverdachts und der Stand des Verfahrens zu berücksichtigen. Vor Beginn der öffentlichen Hauptverhandlung ist ein besonders strenger Maßstab an das Vorliegen eines „überwiegenden Interesses" der Öffentlichkeit anzulegen.

5. Bis zur rechtskräftigen Verurteilung ist die Unschuldsvermutung zugunsten des Beschuldigten oder Angeklagten zu beachten. Zu unterlassen sind alle Auskünfte oder Erklärungen, die geeignet sind, die Unbefangenheit der Verfahrensbeteiligten zu beeinträchtigen. Akteneinsicht durch Medienvertreter kommt nicht in Betracht.

6. Grundsätzlich sind in Auskünfte und Erklärungen über das Ermittlungs- und Strafverfahren keine Namen und sonstige personenbezogene Angaben, die Opfer von Straftaten, Zeugen, Beschuldigte und Angeklagte bestimmbar machen, aufzunehmen. Vor allem bei Hinweisen auf den Wohnort, das Alter, den Beruf und die familiären Verhältnisse oder sonstigen sozialen Bindungen (z. B. Partei- oder Vereinsmitgliedschaft) ist zu prüfen, inwieweit dadurch eine Identifizierung des Betroffenen möglich wird.

7. Personenbezogene Daten dürfen nicht übermittelt werden, wenn besondere bundesgesetzliche oder landesgesetzliche Verwendungsregelungen entgegenstehen.

8. Ist die Bekanntgabe der Person des Beschuldigten oder Angeklagten wegen des überwiegenden öffentlichen Interesses gerechtfertigt, muß auch bei der Übermittlung sonstiger personenbezogener Daten abgewogen werden, ob diese Informationen für die Berichterstattung über die Tat selbst oder die Hintergründe, die zu der Tat geführt haben, erforderlich sind, und in welchem Umfang der Betroffene dadurch in seinem Persönlichkeitsrecht beeinträchtigt wird.

9. Die Bekanntgabe von Vorstrafen ist nur ausnahmsweise zulässig. Sie setzt voraus, daß die frühere Verurteilung im Bundeszentralregister noch nicht getilgt und ihre Kenntnis für eine nachvollziehbare Berichterstattung über eine schwerwiegende Straftat - auch unter Berücksichtigung des Persönlichkeitsrechts des Betroffenen und des Resozialisierungsgedankens - erforderlich ist. Besondere Zurückhaltung ist bei Auskünften und Erklärungen über Sachverhalte geboten, die der früheren Verurteilung zugrunde liegen.

10. Wegen des überragenden Schutzes von Minderjährigen und Heranwachsenden ist bei Auskünften und Erklärungen über Verfahren gegen diesen Personenkreis besondere Zurückhaltung hinsichtlich der Bekanntgabe personenbezogener Daten zu wahren.

11. Opfer, Zeugen und Familienangehörige haben in der Regel keine Veranlassung gegeben, daß ihre persönlichen Lebensumstände in der Öffentlichkeit bekannt gemacht werden. Die Übermittlung personenbezogener Daten über diesen Personenkreis an die Medien kommt deshalb grundsätzlich nicht in Betracht.

12. Bildveröffentlichungen greifen wegen der damit verbundenen sozialen Prangerwirkung besonders tief in das Persönlichkeitsrecht des Betroffenen ein. Eine Bildherausgabe kommt daher für Zwecke der Medienberichterstattung nicht in Betracht.

20.16 Datenschutz bei der Neuordnung der Telekommunikation (Postreform III)

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995

Mit der Postreform III soll die Neugestaltung des Telekommunikationssektors in Deutschland nach den Vorgaben des Liberalisierungskonzepts der Europäischen

Union abgeschlossen werden. Entstehen wird ein riesiger Markt mit einer Vielzahl von großen und kleinen, teilweise auch grenzüberschreitend tätigen Netzbetreibern und Diensteanbietern. Die Akteure auf diesem Telekommunikationsmarkt werden zum größeren Teil als Privatunternehmen operieren, es werden aber auch öffentliche Stellen ihre Leistungen anbieten. Der gesetzgeberische Abschluß der Liberalisierung und der Privatisierung des TK-Sektors wird die rechtliche Grundlage bilden für den endgültigen Eintritt in das Zeitalter von weltweiter Vernetzung, Multimedia und interaktiven Diensten und damit für den rapiden Anstieg des Konsums von Angeboten der Telekommunikation, des interaktiven Rundfunks und der Datenverarbeitung.

Die Konsequenzen sind absehbar: Gegenüber der heutigen Situation werden unvergleichlich mehr personenbezogene Daten durch mehr Stellen registriert und ausgewertet. Betroffen sind alle, die fernsehen, telefonieren, fernkopieren, Texte und Dokumente über Datenleitung schicken oder Telebanking oder Teleshopping betreiben. Die Risiken für den Einzelnen durch die vermehrten Möglichkeiten der Verhaltens- und Umfeldkontrolle oder der Ausforschung persönlicher Lebensgewohnheiten und Eigenschaften vergrößern sich entsprechend.

Der vom Bundesministerium für Post und Telekommunikation vorgelegte Referentenentwurf für ein Telekommunikationsgesetz (TKG-E, Stand: 06.10.95) macht es erforderlich, erneut die Realisierung der grundlegenden Rahmenbedingungen für eine datenschutzgerechte Gestaltung der künftigen Telekommunikationslandschaft - soweit die Gesetzgebungskompetenz des Bundes betroffen ist - anzumahnen.

Ein wirksamer Datenschutz muß - wie bereits jetzt gesetzlich fixiert - auch künftig gleichberechtigtes Regulierungsziel neben z. B. der Sicherstellung der flächendeckenden Grundversorgung mit Telekommunikationsdienstleistungen bleiben.

Kundenwünsche nach variablerer und komfortablerer Nutzung der technischen Möglichkeiten werden zunehmen. Gerade deshalb müssen die Prinzipien der Datenvermeidung und der strikten Begrenzung der Datenverarbeitung auf das erforderliche Ausmaß ihren Vorrang bei der Ausgestaltung der kommunikationstechnischen Infrastruktur behalten. Netzbetreiber und Diensteanbieter sollten verpflichtet werden, überall dort, wo dies technisch möglich ist, auch anonyme Zugangs- und Nutzungsformen für ihre Leistungen bereitzustellen. Für eine sichere Datenübertragung sind ohne prohibitive Zusatzkosten wirksame Verschlüsselungsverfahren bereitzustellen.

Das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis müssen für alle Netzbetreiber und Diensteanbieter ungeachtet ihrer Rechtsform und ihrer Kundenstruktur (z.B. sog. Corporate Networks) einheitlich auf einem hohen Niveau gesichert werden. Der bisherige Schutzstandard darf keinesfalls unter den durch die Postreform II erreichten Stand gesenkt werden. Ein hohes Datenschutzniveau ist als Grundversorgung unabdingbar; seine Gewährleistung sollte deshalb Teil der Universaldienstleistung sein. Die in Grundrechte eingreifenden Regelungen sind im Telekommunikationsgesetz selbst und nicht in Verordnungen zu treffen. Die untergesetzlichen, den Datenschutz betreffenden Normen gehören in eine einzige, nicht verstreut in mehrere Verordnungen.

Entscheidend für die Wirksamkeit des Grundrechtsschutzes ist die strikte Einhaltung der Zweckbindung der Verbindungs- und Rechnungsdaten. Das „Feststellen mißbräuchlicher Inanspruchnahme" oder die "bedarfsgerechte Gestaltung" von TK-Leistungen dürfen nicht als Anlaß für eine umfassende Auswertung dieser Angaben oder sogar der Nachrichteninhalte herangezogen werden.

Für den Kunden bzw. Teilnehmer ist es von größter Bedeutung, die Verarbeitungsvorgänge im TK-Bereich überschauen zu können. Er muß auch künftig über die Nutzungsrisiken bestimmter Kommunikationstechniken (z. B. Mobilfunk) ebenso wie über seine Widerspruchsmöglichkeiten umfassend aufgeklärt werden. Keinesfalls darf die Einwilligung des Betroffenen mißbraucht werden um bereichsspezifische Schutznormen oder effiziente Datensicherungsvorkehrungen zu umgehen.

Um auch und gerade für das besonders schutzwürdige Fernmeldegeheimnis einen durchgängig hohen Schutzstandard zu sichern, braucht es eine unabhänbgige Kontrolle nach bundesweit einheitlichen Kriterien. Die Zuweisung dieser Überwachungsaufgabe an die im TKG-Entwurf vorgesehene Regulierungsbehörde ist wegen deren mangelhafter Unabhängigkeit und der von ihr wahrzunehmenden Regulierungsaufgaben, die mit Interessenkonflikten verbunden sein werden, nicht akzeptabel.

Deshalb sollte aufgrund seiner langjährigen fachlichen Erfahrung bei der Kontrolle der TELEKOM und seiner umfassenden Querschnittskenntnisse im TK-Bereich der Bundesbeauftragte für den Datenschutz eine zentrale Funktion für die Kontrolle im Telekommunikationsbereich erhalten. Die Aufgaben, die die Landesbeauftragten für den Datenschutz und die Aufsichtsbehörden im Rahmen ihrer Zuständigkeiten erfüllen, sind gesetzlich klar zu regeln.

Die Akzeptanz der Informationsgesellschaft der Zukunft hängt wesentlich ab von der Sicherung des Grundrechts auf unbeobachtete Kommunikation. Das Telekommunikationsgesetz wird einen entscheidenden Baustein für die rechtliche Ausgestaltung der künftigen TK-Infrastruktur bilden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher dazu auf, die von ihr vorgeschlagenen Regelungen im weiteren Gesetzgebungsverfahren zu berücksichtigen und sich für ihre Umsetzung auch auf der europäischen Ebene (z. B. der ISDN-Richtlinie) einzusetzen.

21. Index

Druck: Anker-Druck Bremen