22. Jahresbericht
des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats über das Ergebnis der Tätigkeit im Jahre 1999 den 22. Jahresbericht zum 31. März 2000 (§ 33 Abs. 1 Bremisches Datenschutzgesetz – BrDSG). Die Gliederung und die im Bericht geschilderten Arbeitsergebnisse sind ganz überwiegend in der Zeit entstanden, als Dr. Walz noch Landesbeauftragter für den Datenschutz war. Mit Ausnahme des Vorworts entspricht die Darstellung somit den Vorgaben. Der Bericht enthält, wie der Leser feststellen wird, wieder einen bunten Strauß von Vorgängen unterschiedlicher Qualität aus verschiedenen Bereichen. Da Dr. Walz Ende des Jahres 1999 ausgeschieden ist, obliegt es mir, als dem vom Senat bestellten Vertreter, den Bericht vorzulegen. Redaktionsschluß für die Beiträge war der 31. Januar 2000. Ich war bemüht, alle bis dahin eingehenden Äußerungen zu berücksichtigen.

Sven Holst
(Vom Senat bestellter Vertreter des Landesbeauftragter für den Datenschutz)

Inhaltsverzeichnis

1. Vorwort

1.1. Millennium

Auch von den Datenschutzbeauftragten wurde mit Spannung der Jahrtausendwechsel erwartet, denn die weltweit befürchteten Computerpannen hätten natürlich schnelle Entscheidungen erforderlich gemacht, bei denen auch Datenschutzfragen eine Rolle spielen konnten. Zwar waren lange vorher vieler Orts Maßnahmen ergriffen worden, um Fehler zu verhindern, aber als kurz vor dem Jahreswechsel Bescheide der Stadt München auftauchten, die bei Forderungen der Stadt für einhundert Jahre Verzugszinsen berechneten, waren die Signale doch auf Alarm gestellt. In den Betrieben wie auch im öffentlichen Dienst gab es Urlaubssperren, Notdienste und schnelle Eingreifgruppen wurden gebildet. Zum Glück blieb ein Desaster aus. Von kleinen Pannen einmal abgesehen, insbesondere bei älteren PC mit entsprechend betagter Software, sind mir keine gravierenden Pannen im Land bekannt geworden.

1.2. Neue Trends und Bedrohungen für das informationelle Selbstbestimmungsrecht

Da der Landesbeauftragte für den Datenschutz sowohl im öffentlichen wie als Datenschutzaufsichtsbehörde im privaten Bereich Aufgaben hat, muß er die Entwicklung in beiden Bereichen im Auge haben. Mittlerweile haben wir die Schwelle zum 20. Jahrhundert überschritten und eine Vielzahl neuer Tendenzen sind erkennbar, die das informationelle Selbstbestimmungsrecht in der realen wie in der virtuellen Welt entscheidend beeinträchtigen können.

Um nur ein Beispiel zu nennen; der Verbraucher wird gezielt aufs Korn genommen. Seine Verbrauchsgewohnheiten, Interessen und Wünsche wecken die Begehrlichkeiten vieler. Es ist bekannt, daß im Internet spätestens dann alle weiteren und vorherigen Bewegungen im Netz personenbezogen zugeordnet werden können, wenn entweder bei einer Bestellung Name und Lieferanschrift genannt werden oder wenn vor Inanspruchnahme einer Dienstleistung die Bezahlung über Kreditkarte geregelt wird. Darüber hinaus besteht die Gefahr weiterer Beeinträchtigungen, Presseberichten zufolge sind in den USA bis heute bereits 400.000 Fälle von "Identitätsdiebstahl" bekannt geworden.

Aber auch im Kaufhaus wird bald jeder Schritt nachvollziehbar sein. In der Entwicklung befinden sich nämlich sogenannte "Intelligente Einkaufswagen". Nicht nur, daß über ein Ortungssystem festgestellt werden kann, wann, wo und wie lange sich ein Einkaufswagen aufgehalten hat, nein der am Wagen angebrachte Chip registriert auch die in den Warenkorb eingelegte Ware. Wird ein solcher Warenkorb durch die Kasse geschoben, sitzt dort nicht mehr eine Kassiererin, die die Artikel einzeln erfassen muß, sondern per Funkkontakt tauscht der Chip die gespeicherten Daten mit dem Kassenterminal aus und wenn dann auch noch unbar, womöglich mit einer Kundenkreditkarte gezahlt wird, ist das Profil personenbezogen erstellt. Nach dem gleichen Prinzip funktioniert natürlich auch der geplante "Intelligente Mülleimer". Er erkennt nach Einwurf der Verpackung den Verbrauch von Konsumgütern und bestellt diese automatisch via Internet beim Händler nach, der z. B. einmal die Woche, die verbrauchten Lebensmittel nachliefert, um den Kühlschrank des Konsumenten wieder aufzufüllen. Oder der Verkaufsautomat, der ein Produkt erst freigibt, nachdem mit dem Handy eine bestimmte

Telefonnummer angerufen worden ist. Das Handy überträgt die Rufnummer des Käufers und die Abrechnung des Automatenkaufs erfolgt über die Telefonrechnung.

Eines machen die drei Beispiele deutlich, in immer größerem Umfange fallen personenbezogene, personenbeziehbare oder pseudonymisierte Daten an, in vielen Fällen ist dem Verbraucher nicht mehr bekannt, in welchem Umfange über seine Person Daten gespeichert und verarbeitet werden und es ist derzeit noch kein Zahlungsmittel in Sicht, das die anonymisierende Wirkung von Bargeld erreicht.

Eine weitere Tendenz ist erkennbar. Mit aller Macht soll dem Internet als Medium für kommerzielle Anwendungen zum Durchbruch verholfen werden. Das Stichwort hierfür heißt "E-Commerce". Erst vor kurzem meldete eine große deutsche Tageszeitung, ein Automobilkonzern wolle seinen rund 350.000 Beschäftigten kostenlos Personalcomputer mit Internetzugang zur Verfügung stellen. Die Mitarbeiter sollen über ein spezielles Portal Zugang zum Internet haben, das es ihnen ermöglicht, ihre Optionen, Preferenzen und Kurzbefehle individuell anzupassen. Der Präsident des Unternehmens sagte denn auch: "Wir sind entschlossen, unseren Kunden besser zu dienen, in dem wir ihre Denk- und Handlungsweisen verstehen." Andere Informationsgewinnungsmethoden sind noch subtiler. Über Gewinnspiele, Bonussysteme und Dumping-Preise wird dem Kunden versucht die Identität zu entlocken.

Laut Presseberichten lag der Verbreitungsgrad von Internetanschlüssen in Deutschland Ende 1999 zwischen rund 20 und 27 Prozent, darunter sollen 40 % Frauen vertreten sein. Der Verbreitungsgrad in Deutschland soll einer Studie zufolge bis 2003 knapp 40 % erreichen. Ob hierbei bereits die neuen Handys mit WAP-Funktion berücksichtigt sind, konnte ich nicht feststellen. Es liegt auf der Hand, daß sich Deutschland im Wandel befindet, die Industriegesellschaft wird ergänzt durch eine Informationsgesellschaft.

Die neuen Informationstechnologien und Netze beeinflussen mittlerweile fast alle Bereiche des Privatlebens und nahezu die gesamte Arbeitswelt. Für die Datenschutzaufsichtsbehörden stellen sich immense neue Aufgaben. Die Zeichen sind erkannt, neue Konzepte liegen auf dem Tisch. Sie müssen unter dem Stichwort "Der neue Datenschutz" noch ausgefüllt und den ständigen Veränderungen angepaßt werden. Dabei besteht natürlich die Gefahr, daß eine Vielzahl die neuen Medien nutzt, ohne die Gefahren für das informationelle Selbstbestimmungsrecht zu erkennen. Pessimisten behaupten, das auch beim Internet-Anschluß vorherschende Prinzip "plug and play" (frei übersetzt: anschließen und loslegen) führe dazu, daß die Nutzer sich bereits aller Daten entäußert haben, die zu einer Identifizierung erforderlich sind, bevor sie ein dem Medium adäquates Bewußtsein entwickelt haben.

Andererseits bin ich der Meinung, daß das Datenschutzbewußtsein der deutschen Bevölkerung nicht unterentwickelt ist. Die 1998 durchgeführte Repräsentativumfrage des BAT-Freizeit-Forschungsinstituts (Der gläserne Mensch: Multimedia und Datenschutz) hat ergeben, daß 42 % der Befragten die Hauptursache für Verstöße gegen den Datenschutz im eigenen sorglosen Umgang mit den Daten sehen. Eine Untersuchung in den USA (Privacy and American Business: Commerce, Communication and Privacy Online) kommt sogar zu dem Ergebnis, daß 50 % der Internetnutzer den Mißbrauch ihrer Angaben beim Versand von E-Mails befürchten. Das Datenschutzbewußtsein scheint also doch nicht so gering entwickelt zu sein, wie manche befürchten. Gleichwohl, weitere Aufklärung über die Risiken

tut Not, aber noch wichtiger ist das Erlernen von Vermeidungsstrategien. Auch hier ist der Datenschutz gefordert, dies den Bürgern näher zu bringen.

1.3. Vormarsch des technischen Datenschutzes

Waren früher die gelieferten Hard- und Softwarekomponenten starr, unflexibel und ließ sich Datenschutz oft nur durch organisatorische und personelle Maßnahmen erreichen, so ist in den letzten Jahren ein Wandel zu verzeichnen. Als wäre das Bitten der Datenschutzbehörden nach vielfältigen Gestaltungsmöglichkeiten der Technik erhört worden, kommen immer mehr neue Produkte auf den Markt, die eine zum Teil schon nicht mehr von einem Einzelnen überschaubare Vielzahl von Variations- und Einstellungsmöglichkeiten technischer Art beinhalten. Die Hersteller von Informationstechnik haben immer mehr Varianten in ihre Produkte integriert, um die vielfältige Verwendbarkeit sicherzustellen bzw. zu erhöhen. Dies kommt dem Anliegen des Datenschutzes häufig entgegen, es bedeutet aber auch, daß sich der Beratungsbedarf auf diesem Gebiet erhöht, denn von den Herstellern selbst werden die Geräte häufig mit der Einstellung "wide range" ausgeliefert und die Systembetreuer stehen dann vor der Aufgabe, die systemseitigen Einstellungen zur Verbesserung des Datenschutzes, wie in § 7 Abs. 2 BrDSG angelegt, vorzunehmen.

Dies ist allerdings im Grunde genommen eine Implementierung des Datenschutzes auf vorletzter Stufe. Der weitergehende Ansatz ist, Datenschutzelemente bereits bei der Produktionsplanung zu berücksichtigen. Da dies von den Datenschutzbeauftragten nicht unmittelbar beeinflußt werden kann, sind Überlegungen einer Produktzertifizierung und eines Datenschutzaudits angestellt worden. Es ist zu erwarten, daß eine entsprechende Regelung im BDSG aufgenommen wird (vgl. Ziff. 16.10.). Auch der Datenschutz in Bremen hat sich um eine verstärkte Beratung der technischen Datenschutzkomponenten bemüht, dies hat auch seinen Niederschlag im Jahresbericht gefunden.

1.4. Bürgerservice der Bremer Verwaltung über Internet

Die bremische Verwaltung präsentiert sich bisher unterschiedlich intensiv im Internet. Nun soll mit dem Projekt MEDIA@Komm ein weiterer Schritt getan werden. Mit dem Projekt MEDIA@Komm wird eine Plattform gebildet, über die der Bürger via Internet seine Verwaltungsangelegenheiten erledigen kann. MEDIA@Komm bindet dabei nicht nur die Verwaltungsseite ein, sondern an dem Projekt beteiligen sich auch namhafte Firmen. Als End-User sind neben den Bürgern auch Firmen und Gewerbetreibende gefragt.

MEDIA@Komm ist damit ein Projekt, das in die Zukunft gerichtet ist. Am Ende könnte stehen, daß der Bürger und Privatfirmen und über Serviceterminals (sog. Kiosk) auch der Bürger, der über keinen eigenen Internetanschluß verfügt, alle Verwaltungskontakte weitgehend 'online' abwickeln können. Am Anfang steht zwar lediglich die mediale Kontaktvermittlung zur Verwaltung. Dabei wird es aber nicht bleiben. Unabhängig vom Projekt MEDIA@Komm ist absehbar: Wenn die Verwaltung 'online' geht, werden langfristig auch die Verwaltungsabläufe dadurch beeinflußt werden. Aber nicht nur das, es ist auch zu erwarten, daß die Verwaltungsstrukturen dadurch beeinflußt werden.

Bremen hat mit dem Projekt die Chance, in der Bundesrepublik eine Vorreiterrolle zu spielen. Es steht außer Frage, daß dies eine Entwicklung mit weitreichenden Folgen ist. Auch der Datenschutz betritt mit seiner Teilnahme an dem Projekt Neuland. Es bedarf daher einer besonders gründlichen und

überlegten Beratung des Datenschutzkonzeptes. Den Vorteil, der darin liegt, bereits frühzeitig bei der Gestaltung des Verfahrens auf die Entwicklung Einfluß nehmen zu können, um einen datenschutzgerechten Ablauf bei den Verfahren zu implementieren, will ich nutzen.

1.5. Weltweite Datenschutzkultur nicht in Sicht

In den vergangenen Jahren wurde zwischen den Kontinenten weiter die Diskussion über den richtigen Weg zu einem effektiven Datenschutz geführt. Im Vordergrund stand dabei die Frage, auf welche Weise die Bürger besser in ihren Rechten auf informationelle Selbstbestimmung zu schützen sind: Durch mehr staatliche Regulierung oder durch Stärkung ihrer Rechte und der Eigenverantwortlichkeit?

Der europäischen Rechtstradition entspricht eher der Weg verstärkter Regulierung und diesen Weg geht auch die EU-Datenschutz-Richtlinie. Insbesondere in den USA hingegen, wo vor dem Hintergrund der schnellen Entwicklung der neuen Medien dem Schutz der Privatsphäre wieder mehr Bedeutung geschenkt wird, wird in der Selbstregulierung die Lösung gesehen (vgl. Safe-Harbour, Ziff. 16.11.). Sie soll durch vertragliche Bindung und Selbstverpflichtung der Datenverarbeiter, wie auch durch eine stärkere Einbeziehung der Betroffenen selbst erreicht werden.

Wie der aus den Grundrechten entwickelte Begriff des "informationellen Selbstbestimmungsrechts" schon aussagt, geht es auch in Deutschland primär um die Selbstentscheidung durch die Betroffenen. Ein Entscheidungsrecht kann nur dann tatsächlich ausgeübt werden, wenn ein Rahmen, eine allgemeine gesellschaftiche Konvention oder Gesetze eben die Ausübung eines solchen Rechtes ermöglichen. An einem solchen verbindlichen Codex - man kann auch sagen Kultur - fehlt es eben noch, wie sich am besten am Beispiel des Internet nachweisen läßt.

Da agieren alle möglichen Suchmaschinen, Datamining-Firmen und Geheimdienste und greifen jedwede Information ab. Keiner der Internet-Bürger weiß, wann was und wieviel von ihm selbst irgendwo abgesogen wird. Studien kommen denn auch zu dem Ergebnis, daß deutlich über 50 % der befragten Internetnutzer den Mißbrauch ihrer Daten im Netz oder beim Versenden von E-Mails befürchten.

Kein Wunder, wer hat es nicht schon selbst erlebt, daß er eben nur mal auf ein interessantes Banner geklickt hat, um zu sehen, was dort geboten wird und schon ist er eingeschlossen. Er kann sich zwar innerhalb der Anbieterseiten hoch und runter klicken, der Rücksprung auf die ursprüngliche Seite funktioniert einfach nicht. Man kann dann nur noch ganz aussteigen und die Anmeldeprozeduren neu durchlaufen. Oder um ein anderes Beispiel zu nennen, man besucht eine Homepage und als erstes wird man gefragt, ob ein Cookie auf dem eigenen Rechner installiert werden darf. Man klickt auf "Nein" und denkt die Sache ist damit erledigt. Aber schon ist der Cookie-Button wieder auf dem Bildschirm und nicht nur zwei-, dreimal, sondern zwanzig- bis dreizigmal in unregelmäßigen Abständen. Man kann ihn auch nicht ignorieren, denn alle anderen Funktionen auf dem Bildschirm sind nicht ansprechbar, bevor der Cookie-Button nicht seine Antwort hat. Nur ganz hart gesottene bleiben standhaft bei ihrem "Nein". Manch einer hat bestimmt längst aufgegeben und der Cookie-Installation zugestimmt. Ja, und was steht eigentlich in dem Cookie? Was genau macht er mit meinen Daten? Nur in den seltensten Fällen werden auf die Fragen Anbieterantworten bereitgehalten. Oder um noch ein Beispiel zu nennen, der Intel-Chip Pentium III, der letztes Jahr auf den Markt kam, enthält eine ein-

malige Fabrikationsnummer, die über eine Schnittstelle ausgelesen werden kann. Man fragt sich, wie kann ein Unternehmen, das auch nach Europa liefert, nur auf die Idee kommen, das Verfahren so auszugestalten. Erst auf den weltweiten Protest der Datenschutz- und Verbraucherorganisationen hin wurde das Verfahren so realisiert, daß der Käufer selbst entscheiden kann, ob er sich dieser Kennziffer bedienen will und sie einschalten will.

Das sind Beispiele für eine unterentwickelte Daten- und Verbraucherschutzkultur und solange die fehlt, kann man wohl kaum auf rechtlich vorgegebene Rahmenbedingungen verzichten. Von allein stellt sich eine solche Kultur nicht ein. Ohne verbindliche Grundprinzipien und ein Mindestmaß an zu erbringender Transparenz, an durchsetzbaren Rechten für die Betroffenen und auch an Kontrollmechanismen würde der Einzelne noch lange das Nachsehen haben.

1.6. Personelle Situation der Dienststelle

Am Anfang des Berichtsjahres schied unser Diplominformatiker, der Leiter des Referats 40 aus. Die Stelle konnte in vollem Umfang erst wieder zum 01.01.2000 kompetent besetzt werden. Dadurch entstand eine besonders lange Durststrecke, zumal eine qualifizierte technische Beratung verschiedener Verfahren heute mehr denn je gefordert ist. Dies machen auch weite Teile des Berichts deutlich. Daß dennoch viel auf diesem Gebiet geleistet werden konnte, verdanken wir dem engagierten Einsatz zweier Kolleginnen.

Am 31.12.1999 schied der Landesbeauftragte für den Datenschutz, Herr Dr. Walz, dessen Wahlperiode noch bis zum 31.05.2000 ging, vorzeitig aus. Herr Dr. Walz, der das Amt am 01.06.92 angetreten hatte, war somit rund 7 1/2 Jahre Landesbeauftragter für den Datenschutz in Bremen. Die Stelle ist noch nicht wieder besetzt, der Senat bestellte gem. § 24 Abs. 2 BrDSG nach vorheriger Anhörung des Datenschutzausschusses mich zum Vertreter. Die übrigen beim Landesbeauftragten für den Datenschutz - zum Teil langjährig - Beschäftigten blieben auch im Berichtsjahr der Dienststelle treu.

1.7. Statistik der Eingaben und Öffentlichkeitsarbeit

Auf die Darstellung einer dezidierten Statistik der schriftlichen und mündlichen Bürgereingaben verteilt auf öffentlichen und nichtöffentlichen Bereich habe ich verzichtet, weil die Zahlen im Verhältnis zum Vorjahr in etwa gleich geblieben sind. Auch im Berichtsjahr haben der Landesbeauftragte und die Mitarbeiter der Dienststelle verschiedene Fortbildungs- und Vortragsveranstaltungen durchgeführt, darunter ein Datenschutz-Wochenseminar. In der Tendenz zeigt sich allerdings, daß gezielte ein- oder zweitägige Veranstaltungen für einzelne berufliche und dienstliche Bereiche mit größerem Interesse aufgenommen werden. Meine Präsenz im Erfa-Kreis, dem Treffpunkt der betrieblichen Datenschutzbeauftragten ist obligatorisch, darüber hinaus habe ich verschiedene neu bestellte betriebliche Datenschutzbeauftragte vor der Aufnahme ihrer Arbeit beraten und ihnen Hilfestellung gegeben, wie sie ihren gesetzlichen Verpflichtungen am besten nachkommen können. Im übrigen habe ich im Berichtsjahr Broschüren und Faltblätter herausgebracht. Hierzu zählen auch eine Gesetzessammlung aller im Lande Bremen relevanten rechtlichen Datenschutzregelungen, die bei mir weiterhin angefordert werden kann, deren Titel "Datenschutz in der Freien Hansestadt Bremen" lautet, sowie eine Broschüre "Datenschutz bei WindowsNT". Eine Liste noch weiterhin bei mir verfügbarer Materialien befindet sich am Ende dieses Jahresberichts.

1.8. Kooperation mit anderen Datenschutzbehörden

§ 27 Abs. 5 BrDSG ermächtigt und verpflichtet mich zur Zusammenarbeit mit anderen Stellen, die mit der Kontrolle des Datenschutzes betraut sind. In der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die im vergangenen Jahr am 25./26. März in Schwerin und am 07./08. Oktober in Rostock unter Vorsitz des Landesbeauftragten von Mecklenburg-Vorpommern, Dr. Werner Kessel, tagte, bündelt sich die Zusammenarbeit. Die dort gefaßten Beschlüsse, die in der Regel auf Ergebnissen aus Arbeitskreisen beruhen, die von einzelnen Ländern betreut werden, sind häufig richtungsweisend für die Fortentwicklung des Datenschutzes. Im vergangenen Jahr waren Gegenstand derartiger Beschlüsse u. a. die BDSG-Novelle, die Telekommunikation und die Kryptopolitik (vgl. Ziff. 18.).

Im Bereich der Obersten Aufsichtsbehörden für den Datenschutz, denen die Kontrolle im privaten Bereich übertragen ist, wird die Koordinierung im Düsseldorfer Kreis geleistet, der sich ebenfalls zweimal im Jahr stets in Düsseldorf unter Vorsitz des dortigen Innenministeriums trifft. Wichtige Themen hier habe ich unter Ziff. 16.9. dargestellt.

1.9. Ausblick

Neben der intensiven Vorbereitung auf die neuen Aufgaben, die durch die Novellierung des Bundesdatenschutzgesetzes auf die Dienststelle zukommen (vgl. Ziff. 16.10.), werden die Beratungen des neuen Polizeigesetzes (vgl. Ziff. 6.1.), der erwarteten melderechtlichen Regelungen (vgl. Ziff. 6.3.1.) und in Folge der EU-Datenschutz-Richtlinie auch die Beratungen zur Novellierung des Bremischen Datenschutzgesetzes aufzunehmen sein. Im öffentlichen Sektor werden die technischen, aber auch rechtlichen Beratungen des Bremer Verwaltungsnetzes (BVN, vgl. Ziff. 3.2.) und von MEDIA@Komm (vgl. Ziff. 3.1.) im Vordergrund stehen. Daneben ist absehbar, daß Internetanwendungen und -nutzungen der Verwaltung (z. B. das Angebot von T-Online für freien Netzzugang der Schulen), insbesondere E-Mail (vgl. auch Ziff. 3.4.), den Datenschutz in Atem halten werden. Die meisten der bereichsspezifischen Datenschutzregelungen sind nicht mit Blick auf das Medium 'Internet" konzipiert worden. Ich gehe deshalb davon aus, daß in der kommenden Zeit ein Untersuchungsbedarf besteht, ob Anpassungen erforderlich sind. Die zunächst einmal restriktiv formulierten Ansätze im Artikel "Internet-Nutzung durch Schulen" (vgl. Ziff. 10.3.) machen dies deutlich. Auch der verstärkte Einsatz von Videotechnik im öffentlichen und privaten Bereich werden Datenschutzberatungen und -kontrollen nach sich ziehen (vgl. auch Ziff. 6.1.3. und 16.1.). Neben den im Kapitel 16. "Datenschutz in der Privatwirtschaft" angesprochenen Feldern wird ein Beratungsschwerpunkt im Bereich der Tele- und Telekommunikationsdienste liegen. In der Privatwirtschaft eingesetzte moderne Computersysteme lassen eine Vielzahl von Überwachungsmöglichkeiten zu (vgl. z. B. Ziff. 16.2.), die Konflikte zwischen Arbeitnehmern und Arbeitgebern sind vorprogrammiert. Zu erwarten ist, daß insgesamt das Thema Arbeitnehmerdatenschutz wieder einen höheren Stellenwert einnehmen wird.

Die auch im Bericht feststellbare rasche Entwicklung der IuK-Technik mit ihren Auswirkungen im öffentlichen, insbesondere aber im privaten Bereich, wird noch an Fahrt zunehmen. Um eine angemessene Datenschutzberatung sicherzustellen, ist es erforderlich, mehr als bisher, Schwerpunkte zu setzen. Um eine effektive Beratung dieser Punkte zu ermöglichen, bedarf es eines flexiblen Konzep-

tes, was auch auf die Organisationsstruktur der Dienststelle durchschlagen muß. Darüber hinaus muß die arbeitsteilige Kooperation mit den anderen Datenschutzbehörden verstärkt werden. Eine Präsenz der Dienststelle im Internet ist bald möglich zu realisieren. Sie ist heute unabdingbares Hilfsmittel zur schnellen Abwicklung bzw. Vermeidung von Arbeit und hilft dem leichteren Zugang sowie der einfacheren Verbreitung von Informationen. Neben verbesserter Aktualität läßt sich auch eine interaktive Beratung realisieren.

An die Dienststelle wird eine Vielzahl von Anforderungen unterschiedlichster Art herangetragen. Bürgereingaben und -beschwerden ist uneingeschränkt nachzugehen. Im übrigen darf sie sich aber nicht verzetteln, muß immer auf der Höhe der technischen Entwicklung sein und sich schwerpunktmäßig mit den großen Projekten mit Breitenwirkung intensiv beschäftigen.

2. Telekommunikation, Teledienste und Medien

2.1. Bundesverfassungsgericht stärkt Fernmeldegeheimnis

Das Urteil des Bundesverfassungsgerichts vom 14. Juli 1999 zu den Verfassungsbeschwerden gegen das Gesetz zu Art. 10 in der Fassung des Verbrechensbekämpfungsgesetzes vom 28.10.1994 (Az. 1-BvR 2226/94, 2420/95 und 2437/95) hat große öffentliche Aufmerksamkeit ausgelöst.

„Ein Meilenstein für den Datenschutz“ – so äußerte sich der Bundesbeauftragte für den Datenschutz, Jacob, nach dem Urteilsspruch aus Karlsruhe. „Bundesverfassungsgericht weist Grundrechtseinschränkung zurück“ war die Pressemitteilung von einigen Länderkollegen und mir betitelt. Die Bundesregierung äußerte sich zufrieden. Kritische Einschätzungen gab es dagegen von den Klägern selbst, sowie von Bürgerrechts- und Strafverteidigerorganisationen.

Eine so heterogene Bewertung überrascht einerseits, verstärkt aber andererseits das Interesse an der Analyse dessen, was die Richter gesagt und was sie nicht gesagt haben.

Ausgangspunkt und Prüfungsgegenstand waren die die Abhörbefugnisse des Bundesnachrichtendienstes (BND) betreffenden Vorschriften des sog. Verbrechensbekämpfungsgesetzes, das am 1.12. 1994 in Kraft getreten ist. Dieses Gesetz führte neue Strafvorschriften ein (etwa zur Verfolgung von rechtsradikalen Delikten), verschärfte Strafandrohungen (zum Beispiel gegen Schlepperbanden) und änderte Vorschriften der Strafprozeßordnung. Der Deutsche Anwaltsverein, die Humanistische Union etc. kritisierten seinerzeit das neue Gesetz scharf.

Die neuen, in das BND-Gesetz eingefügten Bestimmungen (in §§ 3 und 7 BNDG) erweitern zunächst die Befugnis des BND zur sog. „strategischen Überwachung“ des internationalen Fernmeldeverkehrs, die zuvor auf die Gewinnung von Erkenntnissen über das Ausland von außen- und sicherheitspolitischer Bedeutung beschränkt war, auf die Nachrichtensammlung über bestimmte schwere Straftaten mit Auslandsbezug u.a. in den Bereichen Terrorismus, Drogen und Geldwäsche. Anders ausgedrückt: Die Erlaubnis für den BND, alle im und mit dem Ausland geführten sowie über das Gebiet der Bundesrepublik gehenden, nicht leitungsgebundenen (also über Richtfunk oder Satellit laufenden) Gespräche abzuhören, aufzuzeichnen („Staubsaugerprinzip“) und nach bestimmten Suchbegriffen durchzurastern, wurde auf diesen neuen Erkenntniszweck erstreckt. Dabei gewonnene Informationen können den anderen Nachrichtendiensten (Verfassungsschutz, Militärischer Abschirmdienst), weiterhin dem Zollkriminalinstitut und den Strafverfolgungsbehörden übermittelt werden.

Nicht Gesetz geworden ist der im Entwurf noch enthaltene Vorschlag, daß die Staatsanwaltschaften von sich aus an den BND herantreten und von diesem verlangen können sollten, ganz bestimmte für die Strafverfolgung in einzelnen Fällen relevante Suchbegriffe bei der Rasterung des Fernmeldeverkehrs zu verwenden.

2.1.1. Zweifel an der Verhältnismäßigkeit der Abhörbefugnisse

Die Datenschutzbeauftragten haben seinerzeit - wie andere Kritiker auch - vor allem eingewandt, daß unverhältnismäßig in das Fernmeldegeheimnis eingegriffen und gleichzeitig das in Verfassungsrang stehende Trennungsgebot zwischen Polizei und Geheimdiensten bzw. zwischen Strafermittlung und nachrichtendienstlicher Tätigkeit partiell aufgehoben werde. Das „Staubsaugerprinzip" werde unvermeidlich eine große Mehrheit Unbeteiligter in Abhörmaßnahmen einbeziehen. Eine ausreichende Datenschutzkontrolle durch den Bundesbeauftragten sei nicht gegeben. Die Unterrichtung der Betroffenen erfolge unzulänglich.

Das Bundesverfassungsgericht hat erstmals am 5. Juli 1995 und dann durch regelmäßig wiederholte Beschlüsse den Vollzug der Neuregelung partiell außer Kraft gesetzt. Für die Verwendung von durch den BND aufgezeichneten Daten und deren Weitergabe an die Sicherheitsbehörden verlangten die Richter „bestimmte Tatsachen" statt lediglich –so die Gesetzesfassung - „tatsächliche Anhaltspunkte" für die Begründung eines Verdachts für eine Tatplanung oder –begehung. Schon die Begründung der einstweiligen Anordnung ließ erkennen, wie hoch die Verfassungsrichter die Eingriffswirkung der neu eingeführten Maßnahmen einschätzten.

So verwundert es nicht, daß der Inhalt des Judikats vom 14. Juli 1999einige zentrale Bedenken aufgreift, indem es mehrere der 1994 eingeführten BNDG-Bestimmungen für mit dem Grundgesetz unvereinbar erklärt. Der Gesetzgeber erhält eine Frist bis zum 30. Juni 2001, um den verfassungsmäßigen Zustand wiederherzustellen. Im übrigen werden aber die Verfassungsbeschwerden zurückgewiesen.

Entscheidender „Wermutstropfen" des Urteils ist, daß das Gericht die Zweckänderung von BND-Informationen für Zwecke der Strafverfolgung – mit anderen Worten die Verwendung mit nachrichtendienstlichen Mitteln erlangter Informationen in Ermittlungsverfahren, in denen bisher die personenbezogenen Erkenntnisse mit den Mitteln und unter den Kautelen der Strafprozeßordnung beschafft werden mußten - im Grundsatz anerkannt hat. Anders ausgedrückt: Das Trennungsgebot wurde mit höchstrichterlichem Segen aufgeweicht.

Für die Übermittlung vom BND an die Sicherheitsbehörden hat das BVerfG allerdings (oder je nach Sichtweise: nur) die Einhaltung der Verhältnismäßigkeit als gesetzliche Übermittlungsschwelle angemahnt (s.o.). Diesem Prüfungsmaßstab ist zwar zunächst nur die im Ausland begangene Geldfälschung zum Opfer gefallen und auch nur dann, wenn sie nicht die Geldwertstabilität der Bundesrepublik Deutschland bedroht. Doch hält darüber hinaus dem Gericht den umfangreichen Deliktskatalog für die zulässigen Übermittlungen, der auch mittelschwere Taten wie z.B. die Euroscheck-Fälschung enthält, nur für tolerabel, wenn dafür die Voraussetzungen für den Tatverdacht bzw. die Tatprognose verschärft werden.

2.1.2. Bekräftigung der Grundsätze des Volkszählungsurteils

Ist die vielfach geäußerte Kritik zu desem zentralen Punkt des Trennungsgebots auch durchaus verständlich, gibt es gleichwohl viele gute Gründe für eine Bewertung der Entscheidung, die die Bedeutung der Stärkung des Art. 10 GG und die Bekräftigung der Grundsätze des Volkszählungsurteils aus dem Jahr 1983 in den Vordergrund stellt.

Das Gericht betont die Bedeutung des Fernmeldegeheimnisses für die Herstellung bzw. Aufrechterhaltung des – wie die Datenschutzbeauftragten es gerne formulieren – Rechts auf unkontrollierte telekommunikative Selbstbestimmung, das ja die Grundvoraussetzung einer rechtsstaatlich-demokratischen Informationsgesellschaft darstellt. Die Richter sehen das Risiko, daß „die Befürchtung einer Überwachung mit der Gefahr einer Aufzeichnung, späteren Auswertung, etwaigen Übermittlung und weiteren Verwendung durch andere Behörden .. schon im Vorfeld zu einer Befangenheit in der Kommunikation, zu Kommunikationsstörungen und Verhaltensanpassungen führen (kann)."

Von zentraler Bedeutung ist die wiederholte Bezugnahme auf das Volkszählungsurteil vom 15.12.1983: Die grundrechtlichen Bindungen und Maßgaben, die das BVerfG dort anhand des Rechts auf informationelle Selbstbestimmung entwickelt hatte, werden jetzt weitgehend auch auf das Fernmeldegeheimnis des Art. 10 GG übertragen.

Dies ist um so wichtiger, weil dieses Grundrecht nicht nur Telefonate, sondern jede Kommunikation über TK-Netze wie E-Mails, Telefaxe etc. schützt. Es betrifft nicht nur das Abhören bzw. die Kenntnisnahme selbst, sondern – und dies ist neu - erstreckt seine Schutzwirkung auch auf den anschließenden Informations- und Datenverarbeitungsprozeß sowie den Gebrauch, der von den erlangten Informationen gemacht wird. Daraus folgt, daß Gesetze, die in Art. 10 GG eingreifen, nicht nur die Eingriffsvoraussetzungen normenklar regeln müssen. Auch die Zulässigkeit der anschließenden Speicherung, Nutzung und Übermittlung muß genau definiert werden. Dazu gehört z.B., daß sowohl die abhörenden Ämter selbst als auch die Stellen, die zulässigerweise Daten aus Maßnahmen mit Eingriffscharakter in Art. 10 erhalten haben, diese Daten kennzeichnen müssen, um die strenge Zweckbindung der Angaben gewährleisten zu können. Dies gilt z. B. für die Einspeisung von BND-Daten in polizeiliche Informationssysteme.

Die Richter unterstreichen auch die Bedeutung der Transparenz für die Betroffenen. Die nachträgliche Benachrichtigung ist Voraussetzung dafür, daß Bürgerinnen und Bürger, die ja heimlich ausgeforscht werden, von den ihnen zustehenden Datenschutzansprüchen und Rechtsschutzmöglichkeiten jedenfalls nachträglich Gebrauch machen können. Folgerichtig hat der entscheidende Senat die Vorschrift, wonach die Unterrichtungspflicht nur für länger als drei Monate gespeicherte Daten gelten sollte, verworfen.

Schließlich verlangt das höchste Gericht, Kontrolllücken zu schließen und der G10 Kommission nicht nur wie bisher die Entscheidung über die Zulässigkeit der Abhörmaßnahme selbst zu geben, sondern ihr darüber hinaus die Befugnis zur Überwachung des gesamten Prozesses der Erfassung und Verwertung der Daten zu geben. Die Datenschutzbeauftragten wollen übrigens zusätzlich zu bzw. unabhängig von dieser intensivierten parlamentarischen Überwachung auch die teilweise noch bestehenden Restriktionen ihrer Kontrollbefugnisse im Bereich sicherheitsbehördlicher Datenverarbeitung be-

seitigt wissen. Beispiel dafür ist § 24 Abs. 2 Satz 3 Nr. 1 Bundesdatenschutzgesetz, der der Kontrolle der G10-Kommission unterliegende Daten der Überwachungsbefugnis des Bundesbeauftragten für den Datenschutz entzieht.

2.1.3. Konsequenzen für Gesetzgebung und Sicherheitsbehörden

Welche Konsequenzen hat diese Entscheidung? Das Urteil erzeugt Handlungsbedarf für die Gesetzgebung, vor allem für das BNDG sowie das G10. Auf ihre Verfassungsmäßigkeit – genauer: die jetzt strikter formulierten Anforderungen des BVerfG - hin zu überprüfen sind aber auch die Vorschriften in anderen Gesetzen, die Eingriffe in das Fernmeldegeheimnis und die Weitergabe daraus gewonnener Daten erlauben. Handlungsbedarf entsteht auch für die Exekutive. Beispiel: Die Pflicht zur Kennzeichnung von aus Überwachungsmaßnahmen gewonnenen Angaben – Voraussetzung für die Wahrung der strikten, verschärften Zweckbindung (s.o.) – muß im Verwaltungsvollzug, d.h. in den Datensammlungen der selbst überwachenden wie den Empfängerbehörden, konkret umgesetzt werden. Auch die darüber hinaus vom Gericht statuierten Protokollierungspflichten, die sowohl die zweckgebundene wie eine zweckändernde Verwendung der Daten trifft, entfaltet Wirkungen nicht nur für die Änderungen im BDSG, sondern auch im Bereich von StPO und Polizeigesetzen. Weiter ist die Benachrichtigungspraxis den richterlichen Vorgaben anzupassen. Hier verwirft das Urteil eine Regelung, die vorsah, Betroffenen nur über solche Daten zu unterrichten, de länger als drei Monate gespeichert werden. Es ist zu hoffen, daß die Stärkung des Art. 10 GG durch das BVerfG auch dämpfend auf die Anordnungspraxis der Ermittlungsrichter wirkt, die bisher nach der Statistik nur in den seltensten Fällen Behördenanträge auf Telefonüberwachung ablehnen.

Das Urteil bietet aber Anlaß für weitergreifende rechtspolitische Konsequenzen. Die Datenschutzbeauftragten Berlins, Brandenburgs, Bremens, Nordrhein-Westfalens und Schleswig-Holsteins haben vor der Bundespressekonferenz in Berlin am 25. August 1999 eine prinzipielle Trendwende in der deutschen Telekommunikationspolitik gefordert, und zwar unter der Überschrift „Weg vom Anspruch auf lückenlose Überwachung hin zu einem effektiven Schutz des Telekommunikationsgeheimnisses“ (vgl. Ziff. 2.2.).

2.2. Trendwende in der Telekommunikationspolitik erforderlich

Das Internet boomt. Immer mehr Bürgerinnen und Bürger nutzen E-Mail, Mobiltelefon und Teledienste. Ständig werden technische Neuerungen präsentiert, mit denen noch mehr Menschen schneller und bequemer die „Neuen Medien“ nutzen können, z. B. Eltern, deren Kinder im Zuge eines Schüleraustausches sich im Ausland aufhalten, sind dazu übergegangen, über das Internet Telefonate mit ihren Kindern abzuwickeln. Dies ist häufig als "Bildtelefon" realisiert. Die Furcht vor Überwachung ist realistisch: Niemand weiß, ob und von wem die eigenen Äußerungen in den Netzen registriert und aufgezeichnet werden.

In den letzten Jahren sind immer neue Befugnisse zur staatlichen Kontrolle der Telekommunikation geschaffen worden. Vorschriften, die früher nur das Abhören von Telefongesprächen betrafen, wurden zunächst ohne Rechtsänderung auf Telefaxanschlüsse erweitert und sollen jetzt auch für E-Mails und für den Abruf von Informationen aus dem Internet gelten. Die rechtlichen Möglichkeiten werden extensiv genutzt: 1998 wurden mehr als doppelt so viele Telefonüberwachungen angeordnet wie 1995.

Auch die neue Bundesregierung bereitet weitere Kontrollbestimmungen vor (z. B. die Telekommunikations-Überwachungsverordnung). Große Privatunternehmen und Geheimdienste werten systematisch den Internetverkehr aus.

Das von der Verfassung garantierte Recht der Einzelnen, unkontrolliert elektronisch zu kommunizieren, ist unverzichtbare Grundvoraussetzung einer offenen, demokratischen Informationsgesellschaft. Dieses Recht ist in unserem Land durch weitgreifende Überwachungsvorschriften stark gefährdet. Außerdem gibt es bislang keine ausreichende Informationssicherheit im Internet. Das Bundesverfassungsgericht hat im Juli 1999 in seinem Urteil zu den Abhörbefugnissen des Bundesnachrichtendienstes (vgl. Ziff. 2.1.) diese Gefährdung auf den Punkt gebracht: „Die Befürchtung einer Überwachung ... kann schon im Vorfeld zu einer Befangenheit in der Kommunikation, zu Kommunikationsstörungen und zu Verhaltensanpassungen führen."

Der Landesbeauftragte für den Datenschutz Bremen hat zusammen mit den Datenschutzbeauftragten Berlin, Brandenburg, Nordrhein-Westfalen, und Schleswig-Holstein angesichts dieser aktuellen technischen und rechtlichen Entwicklungen am 25. August 1999 vor der Bundespressekonferenz in Berlin eine eindeutige Kehrtwende der deutschen Telekommunikationspolitik gefordert. Das Konzept, staatliche Kontrollen auf immer mehr Bereiche der elektronischen Kommunikation auszudehnen, muß aufgegeben werden. Statt dessen muß der Staat das Telekommunikationsgeheimnis der Bürgerinnen und Bürger aktiv und wirksam schützen, ggf. in einem besonderen Gesetz zur Sicherung der freien Telekommunikation.

Folgende Forderungen im einzelnen wurden vorgetragen:

- Alle Telekommunikationsanbieter sind bei der Geschäftsabwicklung zu Datensparsamkeit und Datenvermeidung zu verpflichten. Optionen für anonyme und pseudonyme Nutzungen sind zur Verfügung zu stellen.
- Verschlüsselung ist als kostenlose Standardleistung anzubieten. Das Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik ist ein wichtiger Schritt in die richtige Richtung.
- Ein Mediennutzungsgeheimnis ist einzuführen: Wie Zeitung, Buch oder Fernsehen müssen auch die Neuen Medien unkontrolliert genutzt werden können.
- Die Mitwirkungspflichten bei Abhörmaßnahmen sind auf lizenzpflichtige Unternehmen (z.B. Telefongesellschaften) zu begrenzen. Nebenstellenanlagen in Hotels, Betrieben oder Krankenhäusern sind auszunehmen.
- Die Anwendung der Überwachungsbefugnisse muss regelmäßig von unabhängiger Seite evaluiert werden.
- Datenschutzfreundliche Techniken sind zu fördern. Sie müssen erforscht und entwickelt sowie kundenfreundlich auf dem Markt angeboten werden.
- Berufliche Schweigepflichten z.B. von Ärzten oder Anwälten sind besonders wirksam zu schützen.
- Der bestehende strafrechtliche Schutz des Kommunikationsgeheimnisses muss endlich ernst genommen werden. Stärkere polizeiliche Prävention, Beendigung des freien Verkaufs von Abhör-

technik, Effektivierung der Strafverfolgung sowie Straffreiheit für die Aufdeckung von Sicherheitslücken („ethical hacking“) müssen der Bagatellisierung von Straftaten gegen den Schutz der Privatsphäre ein Ende setzen.

Die Pressekonferenz hatte ein breites, in der Mehrzahl zustimmendes Medienecho. Die Datenschutzbeauftragten werden genau verfolgen, ob und wenn ja, welche rechtspolitischen Reaktionen dieser Forderungskatalog auslösen wird.

3. Datenschutz durch Technikgestaltung und -bewertung

3.1. MEDIA@Komm

Nachdem sich die Hansestadt Bremen beim Städtewettbewerb Multimedia bereits 1998 unter den letzten zehn förderungswürdigen deutschen Städten platzieren konnte, gelang es nun in einer weiteren Phase, sich zusammen mit der Stadt Esslingen und der Region Nürnberg gegenüber den noch verbliebenen Mitbewerbern als Gesamtsieger erfolgreich durchzusetzen. Dies ist aus datenschutzrechtlicher Sicht insofern erfreulich, als das MEDIA@Komm-Projekt u.a. die Möglichkeit bietet, Verschlüsselungsverfahren und insbesondere digitale Signaturen in unterschiedlichen Bereichen ausgiebig zu testen und unter Beteiligung meiner Dienststelle zu evaluieren (zur grundsätzlichen Bedeutung des Projekts vgl. Ziff. 1.4.).

Zur Koordinierung des Projekts wurde eigens die Projektgesellschaft "Bremen Online Service" (BOS) gegründet, die im Herbst 1999 Ihre Arbeit aufgenommen hat. Vorrangiges Ziel des Projekts ist es, eine Plattform für rechtsverbindliche und vertrauenswürdige Internettransaktionen aufzubauen, die sowohl den Bürger als auch Unternehmen im digitalen Umgang mit Behörden und anderen öffentlichen Stellen unterstützt. Die Plattform soll, soweit im Verfahren erforderlich, in Verbindung mit einem Trust Center die Identität des Bürgers bzw. des Unternehmens prüfen, Anträge entgegennehmen und an die jeweils zuständigen Stellen weiterleiten, sowie ggf. die Abrechnung der Dienstleistungen übernehmen. Darüber hinaus ist geplant, die BOS-Plattform als Datenbank-Plattform für verschiedene Fachgebiete zu benutzen. Beispielsweise würden Anfragen an einzelne Ämter nicht an deren Server weitergeleitet, sondern bereits von der BOS-Plattform bearbeitet. Dies setzt jedoch voraus, daß die jeweiligen Verwaltungs-Server in kurzen Abständen mit der Datenbank der BOS-Plattform synchronisiert würden.

Über die Plattform sollen zunächst folgende Lebens- und Geschäftssituationen abgewickelt werden:

- Umzug und Wohnen
- Studium
- Heirat
- Freizeit
- Bau eines Hauses
- Kauf eines Autos
- Steuern
- Rechtsanwälte und Notare
- Öffentliche Auftragsvergabe

Der Bürger benötigt für die Teilnahme am MEDIA@Komm-Projekt einen speziell konfigurierten Browser; der Anfangskontakt zu BOS kann jedoch über einen Standard-Browser erfolgen. Der Browser wird so konfiguriert, daß nur zertifizierte Java-Applets aufgerufen werden können. Das Nachladen von Java-Klassen erfolgt über ein spezielles Interaktions-Applet.

Die Authentisierung des Bürgers gegenüber der BOS-Plattform erfolgt durch ein Challenge-Response-Verfahren. Der hierfür clientseitig benötigte Schlüssel wird auf einer speziellen Chipkarte – langfristig ist eine Erweiterung der EC-Karte vorgesehen – gespeichert, so daß sich der Bürger lediglich mittels PIN gegenüber dem entsprechenden Chipkarten-Modul authentisieren muss. Diese PIN ist nicht mit der PIN identisch, die bei der Benutzung von Geldautomaten oder Electronic Cash eingegeben werden muss. Nach erfolgreicher Authentisierung wird ein Sitzungsschlüssel mit einer Länge von 128 Bit erzeugt, mit dem die übertragenen Daten verschlüsselt werden.

Die Verbindung zwischen dem Personalcomputer eines Bürgers bzw. eines Unternehmens und der Server-Plattform von BOS soll auf einem eigens von BOS spezifizierten Standard (OSCI, Online Services Computer Interface) basieren, der im wesentlichen auf HBCI (Home Banking Computer Interface) aufbaut. Während HBCI nur zur Abwicklung von Bankgeschäften dient, deckt OSCI auch andere Geschäftsvorfälle ab. Neben der BOS-Plattform existiert noch ein Formular-Server, der allerdings ohne Nutzung des OSCI-Protokolls kontaktiert werden kann.

MEDIA@Komm ist, wie im Vorwort dargestellt, ein Projekt mit weitreichenden Folgen. Meine Kontakte und Beteiligungsmöglichkeiten sind im bisherigen Verlauf als gut zu bezeichnen. Ohne auf die vielfältigen datenschutzrechtlichen, technischen und rechtlichen Fragen im Einzelnen einzugehen, läßt sich folgendes sagen.

Aus Datenschutzsicht ist es notwendig, bei der Gestaltung der Datenbank-Plattform nicht nur zwischen öffentlichem und nicht-öffentlichem Bereich zu trennen, sondern auch Verfahren öffentlicher Stellen gegeneinander abzuschotten. Hierfür würde es ausreichen, die Trennung auf Datenbankebene zu vollziehen. Anstelle einer fachübergreifenden Datenbank und eines Datenbank-Administrators, der fachübergreifend auf sämtliche Daten zugreifen kann, werden für zusammenhängende Lebensbereiche eigene Datenbanken mit jeweils der Fachbehörde zugeordneten Datenbank-Administratoren eingerichtet.

Darüber hinaus sollte soweit wie möglich versucht werden, die auf der BOS-Plattform gespeicherten personenbezogenen Daten einzelner Fachanwendungen zu pseudonymisieren. Anstelle des Namens und der Adresse des Bürgers würden auf der Ebene der BOS-Plattform lediglich ein Pseudonym gespeichert, möglicherweise die Karten-Nummer. Durch die Pseudonymisierung ließen sich die bei einem verfahrensübergreifenden Zugriff entstehenden Datenschutzprobleme erheblich reduzieren.

Mit MEDIA@Komm wird der Schritt unternommen, unter Einbringung von privaten Firmen als Entwickler wie auch als User und dem Bürger, Verwaltungsverfahren über das Internet abzuwickeln. Mein Ziel ist es durch intensive Befassung und Beratung die vielfältigen sich immer weiter entwickelnden technischen Möglichkeiten zu einem datenschutzverträglichen Einsatz zu verhelfen.

3.2. Bremisches Verwaltungsnetz (BVN)

Neben elektronischer Post wird das Bremische Behördennetz (BVN) zunehmend für Anwendungen genutzt, bei denen sensible personenbezogenen Daten verarbeitet werden, beispielsweise Personaldaten im Rahmen von PUMA. Der Aufbau einer behördenübergreifenden Netzinfrastruktur setzt daher gleichzeitig die Schaffung einer Sicherheitsinfrastrukur voraus. Hierzu hat es im Berichtszeitraum weitere Aktivitäten gegeben:

- Im Rahmen der Projekte PUMA und SEKT (vgl. Ziff. 12.2.) wird eine Infrastruktur aufgebaut zur Verschlüsselung von elektronischer Post (vgl. Ziff. 3.4.).
- Im November 1999 hat sich die bereits seit längerem angekündigte Arbeitsgruppe "Sicherheit im BVN" konstituiert. Die Arbeitsgruppe, die sich aus Vertretern der SKP, der BreKomm, des Gesamtpersonalrats, des Rechnungshofs und des Landesbeauftragten für den Datenschutz zusammensetzt, wird auf der Basis einer detaillierten Istanalyse mögliche sicherheitstechnische Schwachstellen zunächst konzeptionell analysieren. Hierauf aufbauend sollen einzelne Netzkomponenten einem gezielten Sicherheitstest unterzogen werden. Geplant sind zudem konkrete Handlungsanleitungen zu den Themen Telearbeit, Fernwartung und Protokollierung.
- Vom TuI-Referat des Senators für Finanzen sind sogenannte NT-Security-Guidelines herausgegeben worden, die Vorgaben zum Aufbau, zur Installation und zu Sicherheitseinstellungen von WindowsNT-Servern und –Workstation enthalten. Die Richtlinie geht u.a. detailliert auf zu vergebene Zugriffsrechte für einzelne Systemverzeichnisse ein und benennt Parameter für Benutzerkonten und zur Protokollierung von Datei- und Objektzugriffen. Die NT-Guidelines sollen in Kooperation mit der Arbeitsgruppe "Sicherheit des BVN" regelmäßig aktualisiert und auf Servern der bremischen Verwaltung öffentlich zur Verfügung gestellt werden.
- Zusammen mit dem Hamburgischen Datenschutzbeauftragten habe ich im Januar 2000 eine Broschüre herausgegeben, die Sicherheitsmaßnahmen für Windows NT sowohl für die öffentliche Verwaltung als auch für Unternehmen beschreibt. Die Broschüre richtet sich an Administratoren und IuK-Verantwortliche, behördliche und betriebliche Datenschutzbeauftragte sowie an Personal- und Betriebsräte, die sich mit Windows NT aus Sicht des Arbeitnehmerdatenschutzes beschäftigen.

Den weiteren Ausbau des bremischen Verwaltungsnetzes, insbesondere die Umsetzung von sensiblen Client-Server-Anwendungen werde ich konstruktiv im Interesse des Datenschutzes begleiten.

3.3. Privatisierung der ID Bremen

Daten der bremischen Verwaltung wurden bislang entweder von den Behörden selbst oder in deren Auftrag von der Informations- und Datentechnik Bremen (ID Bremen) verarbeitet, einem Eigenbetrieb der Stadtgemeinde Bremen. Das bisherige Prinzip, daß Daten öffentlicher Stellen auch nur durch öffentliche Stellen verarbeitet werden, wird nunmehr durch die Gründung einer Gemeinschaftsgesellschaft – Gesellschafter sind das Land Bremen und das debis Systemhaus GmbH (dSH) – erstmals in Bremen durchbrochen. Zwar wird das Gemeinschaftsunternehmen, dem ein Großteil der bislang von der ID Bremen wahrgenommenen Aufgaben übertragen werden soll, sämtliche personenbezogenen

Daten zunächst auch weiterhin am jetzigen Standort des ID Bremen verarbeiten. Es ist jedoch in keiner Weise auszuschließen, daß Verwaltungsdaten in einigen Jahren auch außerhalb Bremens – beispielsweise beim debis-Standort in Hamburg – gespeichert werden.

Da mit der Gründung der Gemeinschaftsgesellschaft zahlreiche Datenschutzfragen verbunden sind, wurde ein umfangreiches Datenschutzkonzept erarbeitet, das nicht nur den bisherigen Sicherheitsstandard des ID Bremen für die Gemeinschaftsgesellschaft festschreibt, sondern auch für die neuen Tätigkeitsfelder, wie beispielsweise den inzwischen schon eingerichteten User-Help-Desk angemessene Sicherheitsstandards definiert. Besondere Bedeutung fiel den senatorischen Bereichen Inneres, Justiz und Finanz zu, bei denen die Datenverarbeitung sehr eng mit hoheitlichen Aufgaben verbunden ist und deshalb zum Teil zusätzlichen Geheimhaltungs- und Sicherungspflichten unterliegt. Dies gilt vor allem für die Finanzverwaltung, bei der die Datenverarbeitung sogar ausdrücklich Inhalt des hoheitlichen Handelns ist.

Um die Gründung des Gemeinschaftsunternehmens nicht gleich zu Beginn mit äußerst problematschen Datenschutzaspekten zu konfrontieren, wurde in dem Datenschutzkonzept festgelegt, daß sämtliche DV-Verfahren, in denen Daten hoheitlich verarbeitet werden, zunächst auch weiterhin im Auftrag der jeweiligen öffentlichen Stelle von der ID Bremen verarbeitet werden. Dies sind sämtliche Steuerverfahren der Oberfinanzdirektion einschließlich des Zwangsvollstreckungsverfahrens, Statistikverfahren des Statistischen Landesamts, DV-Verfahren der Ordnungswidrigkeiten des Stadtamts Bremen, die Verfahren ISA und ISA-D der Polizei Bremen sowie Daten aus dem DV-Verfahren Sijus-Straf der Staatsanwaltschaft Bremen. Ob und unter welchen Rahmenbedingungen die hoheitlich verarbeiteten Daten künftig durch das Gemeinschaftsunternehmen übernommen werden können, wird im Jahr 2000 noch ausführlich zu erörtern sein. Alle anderen Verfahren öffentlicher Stellen können, so wurde es in dem Konzept festgelegt, auf das neue Gemeinschaftsunternehmen übertragen werden.

Neben einer Darstellung der baulichen, organisatorischen und personellen Maßnahmen ging es in dem Sicherheitskonzept daher zum einem darum, die von der neuen Gemeinschaftsgesellschaft und der ID Bremen in den nächsten Jahren noch jeweils getrennt verarbeiteten Daten auf Betriebssystemebene durch entsprechende MVS- und RACF-Mechanismen geeignet voneinander abzuschotten. Zum anderen soll durch die Gründung einer bei der ID Bremen angesiedelten aufsichtführenden Stelle die Überwachung und Kontrolle der ordnungsgemäßen Datenverarbeitung beim Gemeinschaftsunternehmen gewährleistet werden.

Das in einer Erstversion vorliegende und mit meiner Dienststelle in bislang vorbildlicher Weise abgestimmte Datenschutzkonzept wird im Jahr 2000 weiter fortgeschrieben. Ziel wird es vor allem sein, vor dem Hintergrund einer möglichen Standortverlagerung für die Themenbereiche User-Help-Desk, Client-Server-Anwendungen und Netzwerkverbindungen datenschutzkonforme Lösungen zu erarbeiten.

3.4. Elektronische Post in der bremischen Verwaltung

In der bremischen Verwaltung werden immer mehr Schreiben per elektronischer Post verschickt. Sämtliche Dienstellen sind über Sammelpostfächer erreichbar, individuelle Postfächer stehen mittlerweile an fast einem Drittel der 12 000 Bildschirmarbeitsplätze zur Verfügung. Damit ist die seinerzeit projektierte Erprobungsphase praktisch abgeschlossen, so daß die hierbei gemachten Erfahrungen nunmehr in eine abschließende Regelung zum Einsatz von Elektronischer Post in der bremischen Verwaltung einfließen sollten. Neben Vertretungs- und Abwesenheitsregelungen sollte eine derartige Vereinbarung auf Verschlüsselungsmaßnahmen einschließlich Schlüsselverwaltung, auf Zugriffsrechte der Mail-Administratoren sowie lokale Sicherheitsmaßnahmen eingehen. Ein Anwendungsbeispiel stellen die unter Ziff. 8.8 beschriebenen Regelungen der Polizei Bremen dar.

3.4.1. Rechtliche Regelungen

Elektronische Post ist sowohl als Telekommunikationsdienst als auch je nach Ausprägung als Teledienst zu bewerten. Damit sind nicht nur das Bremische Datenschutzgesetz (BrDSG) und das Bundesdatenschutzgesetz (BDSG), sondern auch das Teledienstedatenschutzgesetz (TDDSG) und das Telekommunikationsgesetz (TKG) einschlägig. Das TDDSG und das TKG – insbesondere § 85 TKG über das Fernmeldegeheimnis und § 89 TKG über den Datenschutz – gelten allerdings nur, wenn der Telekommunikationsdienst Dritten zur Verfügung gestellt wird. Dritte im Sinne des TKG sind Behörden und Unternehmen, für die elektronische Post weitergeleitet und in Postfächern gespeichert wird. Dritte sind aber auch – darauf wird in der Gesetzesbegründung explizit hingewiesen – solche Mitarbeiter, die den Dienst der elektronischen Post für private Zwecke nutzen bzw. bei denen die private Nutzung vom Arbeitgeber geduldet wird, wie es in den "Empfehlungen für die Erprobungsphase des E-Mail-Systems und der elektronischen Informationsordner in der bremischen Verwaltung" zum Ausdruck kommt.

Individuelle Postfächer der bremischen Verwaltung, die sich gemäß der Namenskonvention aus dem Nachnamen und dem ersten Buchstaben des Vornamens des jeweiligen Mitarbeiters zusammensetzen und damit neben der dienstlichen auch eine private Nutzung suggerieren, unterliegen demnach dem Fernmeldegeheimnis gemäß § 85 TKG. Die Anwendbarkeit des TKG, das den Inhalt der elektronischen Post unter das grundrechtlich geschützte Fernmeldegeheimnis stellt, hat zur Folge, daß individuelle Postfächer nicht von den für den Mail-Server zuständigen Administratoren eingesehen werden dürfen. Auch dürfen keine fehlgeleiteten, persönlich adressierten Mails geöffnet werden, um anhand des Inhalts den korrekten Absender zu ermitteln.

3.4.2. Vertretungs- und Abwesenheitsregelungen

Im Vordergrund der Beratungen steht allerdings das Handling dienstlicher E-Mails. Noch zu schaffende Regelungen betreffen vor allem die Vertretungs- und Abwesenheitsregelungen in den einzelnen Dienststellen. Um das Fernmeldegeheimnis zu wahren, sollten ohne Zustimmung des Betroffenen keine Mails an andere E-Mail-Adressen weitergeleitet werden. Und auch mit Zustimmung des Betroffenen ist eine Weiterleitung problematisch, da hiervon ebenso der Absender der Nachricht betroffen ist. Dieser müsste vorab ebenfalls um Zustimmung gebeten werden.

Um die Komplexität datenschutzkonformer Vertretungs- und Abwesenheitsregelungen in der bremischen Verwaltung zu reduzieren, wird daher vorgeschlagen, derartige Regelungen nur für Sammel-

postfächer zu treffen. Potentielle Absender sollten darauf hingewiesen werden, wichtige rechtsverbindliche elektronische Post, die auch in Abwesenheit des Absenders geöffnet werden soll, nur an Sammelpostfächer zu senden und nicht an individuelle Postfächer.

3.4.3. Datenverschlüsselung und digitale Signatur

Personaldaten (Projekt PUMA) und Haushaltsanordnungen (Projekt SEKT, vgl. Ziff. 12.2.) können demnächst innerhalb des bremischen Verwaltungsnetzes auf der Basis des X.509-Standards verschlüsselt und digital signiert verschickt werden. Damit wird sowohl die Vertraulichkeit als auch die Authentizität der übertragenen Daten in ausreichendem Maße sichergestellt. Die Signaturen sind im Vergleich zu den im MEDIA@Komm-Projekt verwendeten Zertifikaten jedoch nicht rechtsverbindlich, da sie nicht von einem zertifizierten Trust-Center generiert werden. Die zentrale Zertifizierungsinstanz und das Key-Management-System werden von der BreKom betrieben.

Um die Vertraulichkeit sämtlicher per E-Mail übertragenen Daten zu garantieren, sollte nach erfolgreicher Einführung des Key-Management-Systems in den Projekten PuMa und SEKT die Verschlüsselung elektronischer Post möglichst bald auch im gesamten bremischen Verwaltungsnetz angeboten werden.

3.4.4. Zunehmendes Datenschutzrisiko durch "Trojanische Pferde"

Ein zunehmendes Problem stellen Viren und Trojanische Pferde dar, die entweder als Anlage oder – angesichts HTML-fähiger Client-Software – als direkter Bestandteil einer Mail verschickt und lokal auf dem Arbeitsplatz-PC zur Ausführung gelangen können. Da im Internet Werkzeuge verfügbar sind, die die Entwicklung von Viren vereinfachen bzw. das Muster von Viren entscheidend verändern, kann auf die Wirksamkeit von Virenscannern allein nicht mehr vertraut werden. Durch Trojanische Pferde wie beispielsweise Back Orifice oder NetBus besteht einerseits die Gefahr, daß die Trojanischen Pferde über den Mail-Server selbstständig Daten aus dem lokalen Netz heraus an beliebige Internetadressen versenden, ohne daß es der Benutzer bemerken würde. Andererseits besteht das Risiko, daß die Trojanischen Pferde Server-Funktionen enthalten, die von anderen Netzanwendern aufgerufen und zur Fernsteuerung des jeweiligen PC genutzt werden. Zwar wird die Fernsteuerung eines Arbeitsplatz-PC aus dem Internet oder aus dem bremischen Verwaltungsnetz heraus durch eine Adressumsetzung auf Firewallebene sowie durch die zentrale Struktur des bremischen Verwaltungsnetzes zurzeit weitgehend verhindert. Dennoch können Trojanische Pferde wie Back Orifice oder NetBus zumindest innerhalb eines Behördennetzes in der Regel ungehindert von jedem Client-PC aus aufgerufen werden.

Diese Risiken können durch den Einsatz einer Firewall nicht wirksam unterbunden werden, da Trojanische Pferde in einer rechtmäßigen Umgebung aufgerufen werden und sich von anderen Anwendungsfunktionen technisch kaum unterscheiden lassen. Über den Einsatz von aktuellen Virenscannern hinaus ist es daher erforderlich, den Zugriff potentieller Viren auf personenbezogene Daten von vornherein einzuschränken. Dies kann durch unterschiedliche Maßnahmen erreicht werden:

- Getrennte Arbeitsumgebungen:
  Auf dem Internet-PC werden zwei getrennte Arbeitsumgebungen eingerichtet. In der sog. Produktionsumgebung wird auf Client-Server-Anwendungen einschliesslich Bürokommunikation zugegriffen, während die Transportumgebung ausschließlich für elektronische Post und auch für den Internetzugang zur Verfügung steht. Die beiden Umgebungen werden auf zwei verschiedene NT-Kennungen abgebildet, denen verschiedene Rechte im lokalen System und auf den Dateiservern zugeordnet sind. Der Anwender wechselt je nach Erforderlichkeit zwischen den beiden Umgebungen, indem er sich beim Betriebssystem ab- und wieder anmeldet; ein Neustart des Systems ist dafür nicht erforderlich. Zusätzlich zu den beiden Arbeitsumgebungen ist es notwendig, daß die für E-Mail- und Web-Zugriff benötigten TCP/IP-Ports entweder durch den Mail-Server, durch einen Proxy-Server oder durch die eingesetzte Firewall benutzerbezogen gefiltert bzw. aktiviert werden.

- Virtual Network Computing (VNC):
  Sämtliche sicherheitskritischen Internetdienste werden auf einem VNC-Server ausgeführt, so daß Webseiten oder Inhalte von elektronischer Post lediglich in Form einer Grafik vom VNC-Server an die jeweiligen Arbeitsplatz-PC übertragen werden. Da der VNC-Server die eigentliche Datenverarbeitung übernimmt, können auch keine unerwünschen Fehlfunktionen auf dem Arbeitsplatz-PC zur Ausführung gelangen. Dies setzt jedoch voraus, daß die Verbindung zwischen VNC-Server und dem zu schützenden lokalen Netz durch eine Firewall kontrolliert wird und die sicherheitsrelevanten Dienste aus dem lokalen Netz ausgelagert werden.

- Laufzeitüberwachung von Programmen:
  Per elektronischer Post oder über das Internet übertragene Programme werden einer Laufzeitüberwachung – mit der Java-Sandbox vergleichbar – unterstellt. Die Laufzeitüberwachung kann sich auf bestimmte sensible Dateien beziehen, die auf der Festplatte gespeichert werden.

Vor- und Nachteile der jeweiligen Maßnahmen werden derzeit in der Arbeitsgruppe "Sicherheit im BVN" (vgl. Ziff. 3.2.) erörtert.

4. Bürgerschaft - Die Arbeit des Datenschutzausschusses

4.1. Ergebnisse der Beratung des 21. Jahresberichts

Nach intensiver Beratung des 21. JB des Landesbeauftragten für den Datenschutz vom 24.04.1999 (Bürgerschafts-Drs. 14/1399) und der Stellungnahme des Senats vom 12.10.1999 (Bürgerschafts-Drs. 15/75) hat der Datenschutzausschuß einen Bericht und Antrag vom 23.02.2000 verabschiedet. Die Behandlung soll in der März-Sitzung der Bürgerschaft (Landtag) erfolgen. Die Abgeordneten haben dann über folgenden Antrag zu befinden: "Die Bürgerschaft (Landtag) tritt den Bemerkungen des Datenschutzausschusses bei."

Der vom Ausschuß angenommene Text hat folgenden Wortlaut:

"Die Bürgerschaft (Landtag) hat in ihrer Sitzung am 20. Mai 1999 den 21. Jahresbericht des Landesbeauftragten für den Datenschutz und in ihrer Sitzung am 18. November 1999 die Stellungnahme des Senats zur Beratung und Berichterstattung an den Datenschutzausschuss überwiesen.

Der Ausschuss hat bei der Behandlung des Jahresberichts und der Stellungnahme des Senats den Landesbeauftragten für den Datenschutz und Vertreter der betroffenen Ressorts angehört. Die wesentlichen Beratungsergebnisse sind nachfolgend aufgeführt. Die Textziffern in den verwendeten Überschriften sind identisch mit denen des 21. Jahresberichts.

- PuMa: Komprimierung ersetzt nicht Kryptierung (Tz. 8.2)

Das Datenschutzkonzept zu dem in allen senatorischen Behörden und nachgeordneten Dienststellen zur Personalverwaltung und für das Personalmanagement eingesetzten Verfahren (PuMa) sieht für DV-Geräte mit Schreibzugriff auf das Diskettenlaufwerk ein Programm zur Verschlüsselung der Daten vor. Wie der Landesbeauftragten für den Datenschutz bei einer Prüfung einer senatorischen Behörde festgestellt hat, ist dort eine entsprechende Verschlüsselung nicht eingesetzt worden.

Der Ausschuss begrüßt, daß es nach den übereinstimmenden Erklärungen des Landesbeauftragten für den Datenschutz und des Vertreters des Senators für Finanzen vor dem Ausschuss aufgrund vielfältiger Bemühungen nunmehr gelungen ist, entsprechend der Forderung des Ausschusses ein geeignetes Verschlüsselungsprogramm mit der Bezeichnung "PGP Disk" zu finden.

Der Ausschuss geht davon aus, daß die konkreten Einsatzbedingungen bei den personaldatenverarbeitenden Stellen nunmehr unverzüglich abgestimmt werden, damit die ausgewählte Verschlüsselungssoftware bei PuMa möglichst bald zum Einsatz kommen kann.

- Stagnation im Melderecht (Tz. 9.6)

Im Jahre 1994 änderte der Bund das Melderechtsrahmengesetz (MRRG), das in seiner neuen Fassung am 20. März 1994 in Kraft trat. Eine Anpassung des Bremischen Meldegesetzes ist bis heute nicht erfolgt. Die Frist zur Anpassung der Landesmeldegesetze an das MRRG ist im März 1996 abgelaufen. Der Datenschutzausschuss der 14. Wahlperiode hat wiederholt auf dieses Versäumnis hingewiesen, zuletzt in seinem Bericht und Antrag vom 21. Januar 1999 zum 20. Jahresbericht des Landesbeauftragten für den Datenschutz (Drs. 14/1321), wobei der Ausschuss die Erwartung geäußert hat, daß noch in der 14. Legislaturperiode ein Gesetzentwurf zur Novellierung des Bremischen Meldegesetzes vorgelegt werde.

Auch zahlreiche Beschwerden von Bürgern über die nach dem Meldegesetz mögliche Übermittlung von Wählerdaten an politische Parteien im Vorfeld von Wahlen sind wiederholt Gegenstand von Erörterungen im Datenschutzausschuss gewesen. Sowohl in seinem Bericht und Antrag vom 6. Februar 1996 zum 17. Jahresbericht (Drs. 14/214) als auch in seinem Bericht und Antrag vom 21. Januar 1997 zum 18. Jahresbericht (Drs. 14/564) hat der Ausschuss den Senator für Inneres aufgefordert, für eine landeseinheitliche Handhabung der Weitergabe von Wählerdaten an die Parteien Sorge zu tragen und sicherzustellen, daß Daten aus den Melderegistern Bremens und Bremerhavens nur zu dem nach dem Meldegesetz erlaubten Zweck verwendet und insbesondere nicht an Parteigliederungen außerhalb Bremens weitergegeben werden.

In seinem Bericht und Antrag vom 11. März 1998 zum 19. Jahresbericht (Drs. 14/981) hat der Datenschutzausschuss gefordert, daß entsprechend der Ankündigung des Senators für Inneres vor dem Ausschuss in das an das geänderte MRRG anzupassende Meldegesetz eine Bestimmung aufge-

nommen wird, die die Weitergabe von Wählerdaten auf Parteigliederungen innerhalb des Landes Bremen beschränkt. In seinem Bericht und Antrag vom 21. Januar 1999 zum 20. Jahresbericht (Drs. 14/1321) hat der Ausschuss diese Forderung erneut erhoben und dazu weiter ausgeführt, er gehe davon aus, daß bei der Novellierung des Meldegesetzes auch die bisherige Regelung zur Übermittlung von Meldedaten an Adressbuchverlage überprüft werde.

In der Sitzung des Datenschutzausschusses am 1. Dezember 1999 hat der Vertreter des Innensenators eingeräumt, daß die Novellierung des Meldegesetzes auch im Hinblick auf die Entwicklung in anderen Rechtsgebieten dringend erforderlich sei und dazu weiter ausgeführt, daß bis zum Ende des Jahres 2000 mit dem In-Kraft-Treten des geänderten Bremischem Meldegesetzes zu rechnen sei. Für die Verzögerung seien personelle Engpässe im Innenressort verantwortlich.

Bei allem Verständnis dafür, daß Sparzwänge eine nicht immer zeitgerechte Erledigung der Aufgaben eines Ressorts zur Folge haben können, ist der Datenschutzausschuss der Auffassung, daß derartig lange Verzögerungen, wie sie bei der Anpassung des Bremischen Meldegesetzes aufgetreten sind, nicht mehr hinnehmbar sind. Der Ausschuss erwartet, daß der Gesetzentwurf zur Novellierung des Bremischen Meldegesetzes nunmehr unverzüglich erstellt und nach Abstimmung mit dem Landesbeauftragten für den Datenschutz so rechtzeitig der Bürgerschaft (Landtag) vorgelegt wird, daß er noch im Laufe dieses Jahres in Kraft treten kann. Die Vertreterin der Fraktion von Bündnis 90/Die Grünen tritt im Übrigen dafür ein, die Weitergabe von Daten aus dem Melderegister künftig von der vorherigen Zustimmung der Betroffenen abhängig zu machen.

- ID Cash - Haushaltskontrolle mit Bürgerdaten (Tz. 9.8)

Das der Haushaltskontrolle dienende Verfahren ID Cash (Control Access System Haushalt) bietet dem Innenressort die Möglichkeit, alle Zahlungsbewegungen seines senatorischen Bereichs einschließlich der nachgeordneten Ämter laufend zu beobachten. Die entsprechenden Datensätze enthalten auch personenbezogene Daten von Bürgerinnen und Bürgern, die entstehen, wenn diese eine Zahlung von der Landeshauptkasse erhalten oder an sie leisten. Die dagegen vom Landesbeauftragten für den Datenschutz vorgetragenen Bedenken, die sich im Wesentlichen auf im Umfang rechtlich nicht zulässige Datenübermittlungen und ein nicht ausreichendes Datenschutzkonzept bezogen, wurden vom Datenschutzausschuss geteilt.

Nachdem der Datenschutzausschuss die Beteiligten aufgefordert hatte, weiterhin um eine Lösung des Problems bemüht zu sein, haben sich der Datenschutzbeauftragte und der Senator für Inneres, Kultur und Sport unter Beteiligung der Informations- und Datentechnik Bremen GmbH darauf verständigt, daß durch den Einsatz entsprechender Filter dem Verfahren ID Cash nur noch anonymisierte Daten zur Verfügung gestellt werden. Damit sind die grundsätzlichen Probleme gelöst.

Der Datenschutzausschuss begrüßt, daß ein Weg gefunden worden ist, der einerseits dem Senator für Inneres, Kultur und Sport die für seine Haushaltskontrolle erforderlichen Daten zur Verfügung stellt und andererseits eine Übermittlung personenbezogener Daten vermeidet.

- **Bremisches Krebsregister - Einführungsprobleme (Tz. 11.1)**

Insbesondere zur Erforschung der Ursachen von Krebskrankheiten ist durch das am 1. Oktober 1997 in Kraft getretene Gesetz über das Krebsregister der Freien Hansestadt Bremen (BremKRG) ein Krebsregister eingerichtet worden. Das Krebsregister besteht aus der Vertrauensstelle und der Registerstelle. Die Vertrauensstelle nimmt die Meldungen der Ärzte und Kliniken entgegen. Die Meldungen enthalten die Identitätsdaten und die medizinischen Daten der einzelnen gemeldeten Patienten. Die medizinischen Daten hat die Vertrauensstelle unverzüglich an die Registerstelle zu übermitteln und anschließend aus ihrem Bestand zu löschen. Die Identitätsdaten hingegen bleiben auf Dauer bei der Vertrauensstelle gespeichert. Diese hat sicherzustellen, daß diese Daten nur für die gesetzlich zugelassenen Zwecke genutzt werden können. Die Registerstelle ihrerseits speichert auf Dauer die medizinischen Daten.

Der Datenschutzausschuss begrüßt, daß inzwischen Vertrauensstelle und Registerstelle in Abstimmung mit dem Landesbeauftragten für den Datenschutz Datenschutzkonzepte entwickelt und umgesetzt haben. Diese stellen durch technische und organisatorische Vorkehrungen sicher, daß die Vertrauensstelle die bei ihr gespeicherten Identitätsdaten der gemeldeten Patienten nur zu den gesetzlich erlaubten Zwecken nutzen kann und daß die Registerstelle die ihr von der Vertrauensstelle übermittelten medizinischen Daten nicht auf bestimmte Personen beziehen kann.

Der Datenschutzausschuss begrüßt weiterhin den durch das BremKRG und dessen Umsetzung erreichten hohen Standard des Schutzes der Persönlichkeitsrechte bremischer Krebspatienten. Er bittet den Senat, diesen Standard bei der anstehenden Novellierung des BremKRG aufrechtzuerhalten.

- **Kindergarten-Informationssystem KIS (Tz. 12.3)**

Das Kindergarten-Informationssystem (KIS) ist ein vom damaligen Senator für Frauen, Gesundheit, Jugend, Soziales und Umweltschutz entwickeltes EDV-Projekt, mit dem teilweise sehr sensible Daten von Eltern und Kindern für die Aufnahme in Kindertagesheimen und für die Beitragsberechnung verarbeitet werden.

Wie dem Ausschuss vom zuständigen Ressort und vom Landesbeauftragten für den Datenschutz übereinstimmend mitgeteilt worden ist, sind anfängliche Probleme, die dadurch entstanden waren, daß zunächst kein Datenschutzkonzept vorlag, inzwischen behoben. Zudem hat eine vom Landesbeauftragten für den Datenschutz in jüngster Zeit in zwei Kindertagesheimen vorgenommene Prüfung ergeben, daß die gesetzlichen Vorgaben zum Datenschutz nunmehr auch in der konkreten Anwendung beachtet werden. Der Datenschutzausschuss sieht die Angelegenheit damit als erledigt an."

4.2. Aktuelle Themen

Nach der Bürgerschaftswahl ist der Datenschutzausschuß in personell veränderter Form zusammengetreten. Die Tatsache, daß mehrheitlich neu in das Parlament gewählte Abgeordnete Mitglieder des Ausschusses geworden sind, hat das Interesse an der Erörterung aktueller Themen noch verstärkt.

Behandelt und diskutiert wurden u.a. die Datenschutzprobleme eines Bremer Call Centers (vgl. Ziff. 16.2.), die in einer bundesweiten Fernsehsendung (ARD – „Panorama“) aufgezeigt worden waren. Kritisiert wurde in der Ausstrahlung vor allem die technische Möglichkeit, sich von außen in Telefonate

zwischen Kunden und Mitarbeitern/innen ohne deren Kenntnis einzuwählen. Der LfD hatte die betriebliche Datenschutzbeauftragte bereits bei der Betriebsaufnahme beraten. Ein Mitarbeiter des Landesbeauftragten hat nach Bekanntwerdens des Berichts die Firma umgehend aufgesucht und den Sachverhalt sowie die zu ziehenden Konsequenzen mit der Geschäftsführung geklärt. Der Datenschutzausschuß hat eine Einladung des Unternehmens zu einem Besuch vor Ort Anfang des Jahres 2000 angenommen.

Angesprochen wurde auch das Thema Videoüberwachung auf öffentlichen Plätzen anläßlich von Medienberichten über eine mögliche Installation auf dem Vorplatz des Bremer Hauptbahnhofs, eine Thematik, die im Kontext der Novellierung des Bremischen Polizeigesetzes (vgl. Ziff. 6.1.) noch debattiert werden wird.

Angesprochen wurden auch die Konsequenzen der Novellierung des Bundesdatenschutzgesetzes für die Presse und das ihr grundgesetzlich gewährleistete Redaktionsgeheimnis. Die im November 1999 bundesweit in den Medien geäußerte Kritik an den entsprechenden Regelungen im Referentenentwurf des Bundesinnenministeriums wurde allerdings dadurch gegenstandslos, daß der Bundesinnenminister für den inzwischen vorgelegten Regierungsentwurf eine Überarbeitung der entsprechenden Bestimmungen zugesagt hatte.

5. Personalwesen

5.1. Prüfung bei Personalstellen über die Aufbewahrung sensibler Personaldaten

Im Jahre 1994 sind gesetzliche Regelungen über die Verarbeitung von Personalaktendaten in das Bremische Beamtengesetz (BremBG) aufgenommen worden (vgl. 16. JB , Ziff. 4.3). Die Senatskommission für das Personalwesen hatte damals die nach § 93 BremBG erforderlichen Richtlinien über die Erhebung und Verarbeitung von Daten in Personalakten bereits im Jahre 1996 erlassen (vgl. 19. JB, Ziff. 8.4).

Inzwischen hat auch der Magistrat als oberste Dienstbehörde für die Stadtgemeinde Bremerhaven entsprechende Richtlinien mit datenschützendem Charakter erlassen. Sie entsprechen im wesentlichen den bremischen Richtlinien und sind am 01. Januar 1999 in Kraft getreten.

Im Berichtszeitraum habe ich bei sechs Personalstellen überprüft, ob besonders sensible Personaldaten entsprechend den Richtlinien über die Erhebung und Führung von Personalaktendaten (RiLi) aufbewahrt werden. Es handelt sich hierbei um folgende Datenarten:

- Ärztliche Unterlagen (Gesundheitszeugnisse und Untersuchungsergebnisse)
- Unterlagen über Erkrankungen (ärztliche Atteste, sonstige Krankmeldungen und Beihilfe)
- Unterlagen über Disziplinarmaßnahmen und Abmahnungen

5.1.1. Ärztliche Unterlagen

Nach Ziffer 7 Abs. 2 und 3 der RiLi sind diese Unterlagen in einem verschlossenen Umschlag in der Personalakte aufzubewahren, soweit sie zur Personalakte zu nehmen sind. Auf dem Umschlag ist ein Hinweis auf den Inhalt anzubringen. Der Umschlag darf nur von zugangsberechtigten Personen geöff-

net und eingesehen werden, für die die Kenntnisnahme des Inhalts im Einzelfall erforderlich ist. Die Einsichtnahme ist auf dem Umschlag durch Namenszeichen unter Datumsangabe zu vermerken.

Lediglich zwei der überprüften Personalstellen haben diese Vorschrift beachtet. Bei den anderen Dienststellen befanden sich die ärztlichen Unterlagen offen in der Personalakte, so daß der besondere Schutz dieser Personaldaten nicht gewährleistet war. Letztgenannte Personalstellen haben inzwischen erklärt, sie würden in Zukunft die besondere Regelung einhalten.

5.1.2. Unterlagen über Erkrankungen

Nach Ziffer 21 Abs. 3 der RiLi sind Unterlagen über Erkrankungen, Beihilfe u. a. fünf Jahre nach Ablauf des Jahres aufzubewahren, in dem die Bearbeitung eines einzelnen Vorgangs abgeschlossen wurde. Teilweise werden neben den Urlaubs- und Krankheitsakten auch Karteikarten geführt.

Meine Prüfung ergab folgendes Bild: In zwei Personalstellen enthielten die überprüften Akten zwar nur Unterlagen über die letzten fünf Jahre. Allerdings wurden auf den Karteikarten weit über 10 bis 20 Jahre zurückliegende Krankmeldungen aufgeführt. In einer Personalstelle war die Vorschrift zwar bekannt, es wurde aber darauf verwiesen, daß schon immer so verfahren worden sei. Inzwischen haben die Personalstellen, in denen die fünfjährige Aufbewahrungsfrist nicht beachtet wurde, erklärt, sie würden die Akten unverzüglich bereinigen und neue Karteikarten anlegen.

Darüber hinaus verfügten zwei Personalstellen noch über alte Beihilfeakten, obwohl sich die Beihilfesachbearbeitung zentral bei der Senatskommission für das Personalwesen befindet, die Anträge dort direkt zu stellen sind und die Beihilfeakten seitdem dort geführt werden. Die alten Beihilfeakten sind nach Mitteilung der beiden Personalstellen inzwischen vernichtet worden.

5.1.3. Unterlagen über Disziplinarmaßnahmen und Abmahnungen

Ziffer 20 der Rili enthält dezidierte Regelungen über die Tilgung von Vorgängen, die zu den Personalakten genommen wurden. Die überprüften Personalstellen führen hierzu Wiedervorlagen, die gewährleisten, daß sämtliche Eintragungen rechtzeitig getilgt werden. Eintragungen über die jeweilige Tilgungsfrist hinaus sind nicht festgestellt worden.

5.1.4. Fazit

Insgesamt zeigt die Prüfung, daß die Richtlinien nur unzureichend eingehalten werden. Weil bei den Prüfgesprächen teilweise Unkenntnis über die einzelnen Bestimmungen festzustellen war, halte ich es für erforderlich, die Beschäftigten regelmäßig auf die geltenden die Richtlinien hinzuweisen und sie über die Handhabung zu unterrichten. Darüber hinaus bietet das Aus- und Fortbildungszentrum jährlich die zweitägige Veranstaltung "Datenschutz im Personalwesen" an. Die Personalsachbearbeiter sollten verstärkt darauf hingewiesen werden.

5.2. Amtsärztliche Untersuchungen wegen Dienstunfähigkeit

Seit dem 01. Dezember 1998 gilt § 47a Bremisches Beamtengesetz (BremBG), wonach bei einer ärztlichen Untersuchung zur Feststellung der Dienstunfähigkeit eines Beamten der Arzt nur im Einzelfall auf Anforderung der Behörde das die tragenden Feststellungen und Gründe enthaltene Gut-

achten mitteilt und zwar soweit deren Kenntnis für die Behörde unter Beachtung des Grundsatzes der Verhältnismäßigkeit für die von ihr zu treffende Entscheidung erforderlich ist.

Aufgrund dieser Neuregelung hat mir in 1999 die damalige Senatskommission für das Personalwesen den Entwurf einer "Vereinbarung mit dem Gesundheitsressort über amtsärztliche Untersuchungen von Beamtinnen und Beamten sowie Richterinnen und Richtern der Freien Hansestadt Bremen (Land und Stadtgemeinde) im Zusammenhang mit der Versetzung in den Ruhestand wegen Dienstunfähigkeit" vorgelegt.

Ich konnte folgende Verbesserungen erreichen:

- Die Vereinbarung regelt, daß das Gesundheitsamt der Behörde, die das Gutachten anfordert, nur das mitteilt, was der Wortlaut des § 23 Abs. 4 ÖGDG erlaubt, nämlich das Ergebnis und, soweit erforderlich, tätigkeitsbezogene Risikofaktoren. Dies ist eine Verbesserung gegenüber dem Entwurf.
- Die Verpflichtung zur Versendung der Untersuchungsbefunde in einem gesonderten, verschlossen und versiegelten Umschlag und dessen verschlossene Aufnahme in die Personalakte ist in die Vereinbarung aufgenommen worden.

Meinen Bedenken gegen den vorgesehenen Umfang des zu übermittelnden Untersuchungsergebnisses wurden beim Abschluss der Vereinbarung leider nicht Rechnung getragen. Nach Ziff. 3.3 der Vereinbarung gehören dazu das Krankheitsbild einschließlich der Prognose über den weiteren Krankheitsverlauf und Einzelergebnisse des Untersuchungsbefundes. Ich halte es für erforderlich, die Vereinbarung insoweit nach Ablauf eines Jahres zu überprüfen.

Die Vereinbarung ist inzwischen von beiden senatorischen Behörden unterzeichnet und im Bremischen Amtsblatt vom 25. August 1999 (S. 635) veröffentlicht worden.

5.3. Trennung der Freien Heilfürsorge von der Personalverwaltung

Mit Wirkung vom 01. Januar 1999 wurde die Polizei Bremen neu organisiert. Mehrere Polizeibeamte haben mir mitgeteilt, die Geschäftsverteilung in der Fachdirektion „Personal“ sehe vor, daß der Leiter des Abschnitts „Grundsatzangelegenheiten, Planung, Organisation und Personalentwicklung“ gleichzeitig für die Freie Heilfürsorge der Polizeibeamten zuständig sein solle. Sie befürchteten, daß dadurch Krankheitsdaten bei Personalentscheidungen verwertet würden.Ich fand dies im Geschäftsverteilung bestätigt. Ich habe die Polizei Bremen darauf hingewiesen, daß dies gegen § 93b Bremisches Beamtengesetz verstößt. Danach sollen Angelegenheiten der Freien Heilfürsorge in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden. Dieses Trennungsgebot soll die besondere Schutzbedürftigkeit der Unterlagen auch und gerade gegenüber den mit anderen Personalangelegenheiten befassten Beschäftigten gewährleisten. Im Ergebnis soll der Beamte insgesamt hinsichtlich der Offenbarung und Verwendbarkeit seiner Krankheitsunterlagen grundsätzlich so stehen, wie er stehen würde, wenn er seine Behandlungskosten nicht mit dem Dienstherrn, sondern allein mit einer dem Dienstherrn fremden Versicherung abzurechnen hätte.

Der Senator für Inneres, Kultur und Sport hat in diesem Zusammenhang erklärt, diese Geschäftsverteilung gelte nur vorläufig. Es werde geprüft, die Freie Heilfürsorge auf die Beihilfestelle der Senats-

kommission für das Personalwesen (jetzt: Performa Nord) zu übertragen, wie dies bereits bei der Freien Heilfürsorge der Feuerwehr der Fall sei.

Inzwischen hat der Senator für Inneres, Kultur und Sport mitgeteilt, die Verlagerung dieser Aufgabe von der Polizei Bremen auf Performa Nord solle bis zum 31. März 2000 abgeschlossen sein.

5.4. Bekämpfung der Korruption in der bremischen Verwaltung

Der Senat hat Anfang 1999 einen Beschluss zur Bekämpfung der Korruption gefasst. Danach ist die Einrichtung von Antikorruptionsbeauftragten und Innenrevisionen in den Ressorts bzw. nachgeordneten Dienststellen sowie einer zentralen Antikorruptionsstelle (AKS) beim Senator für Finanzen vorgesehen. Außerdem soll dort eine Melde- und Informationsstelle für Vergabesperren geschaffen werden.

Die AKS ist inzwischen beim Senator für Finanzen angesiedelt worden und hat mir Entwürfe einer "Verwaltungsvorschrift zur Vermeidung und Bekämpfung der Korruption" sowie einer "Richtlinie Innenrevision" zur Stellungnahme vorgelegt. Danach unterstehen die Antikorruptionsbeauftragten und Innenrevisionen direkt den jeweiligen Dienstvorgesetzten. Die damit verbundene Verarbeitung personenbezogener Daten richtet sich nach § 12 Abs. 3 Bremisches Datenschutzgesetz (BrDSG). Danach gilt die Wahrnehmung von Aufsichts- und Kontrollbefugnissen nicht als Verarbeitung für andere Zwecke. Gleichwohl haben diese Stellen die Grundsätze der Verhältnismäßigkeit und Erforderlichkeit zu beachten. Unter dieser Prämisse habe ich die vorgenannten Entwürfe mit der AKS erörtert und Änderungen vorgeschlagen. Diese beziehen sich u. a. auf:

- den Umfang der und Berechtigung zur Unterrichtung,
- den Umfang von Einsicht in Akten und Dateien durch die Innenrevision sowie auf Auskunftspflichten,
- Aufbewahrungs- und Lösch- bzw. Vernichtungspflichten von Unterlagen bei den Antikorruptionsbeauftragten,
- Auskunftsverfahren über die Zuverlässigkeit von Bietern und Bewerbern,
- Aufklärung der Bieter und Bewerber über das Verfahren und die dabei verarbeiteten Daten.

Die mir bisher vorgelegten Entwürfe haben zwar schon eine Reihe meiner Anregungen aufgegriffen, bedürfen aber noch weiterer Überarbeitung für eine datenschutzgerechte Ausgestaltung des gesamten Verfahrens.

5.5. Telearbeit und das fehlende Technikkonzept

Im Berichtszeitraum tagte die Arbeitsgruppe "Telearbeit", über deren Einsetzung ich berichtet habe (vgl. 21. JB, Ziff. 8.1.). Es ging um die Anbindung der in den Privatwohnungen der Beschäftigten stehenden Rechner über ein Netz. Zunächst wurde in der Arbeitsgruppe ein Technikkonzept mit zwei Alternativen für den Fernzugriff (Remote-Access) vom Telearbeitsplatz auf die Netze der Dienststellen vorgestellt. Eine Alternative sah die dezentrale Einwahl vom Telearbeitsplatz in das Dienststellennetz vor. Bei dieser Alternative müssten alle Sicherheitsmaßnahmen lokal umgesetzt werden. In der zweiten Alternative wurde die zentrale Einwahl beschrieben, bei der der Anmeldeserver mit kryptographischen Verfahren die Authentizität prüft. Nach erfolgreicher Anmeldung teilt der Anmeldeserver

einen Schlüssel zu und baut eine verschlüsselte Verbindung zum lokalen Netz auf, in dem der Benutzer mit den dort geltenden Rechten im Netz zugelassen wird (Virtuelles privates Netzwerk – VPN).

In der Arbeitsgruppe wurde die zweite Alternative befürwortet und die BreKom beauftragt Machbarkeit und Kosten festzustellen. Eine Stellungnahme sowie ein Sicherheitskonzept für die Anbindung von Telearbeitsplätzen an das BVN liegen bisher nicht vor.

Eine Voraussetzung für die Telearbeit soll die Erreichbarkeit der Telearbeiterinnen per E-Mail für die Kommunikation mit der Dienststelle sein. Da die Anbindung der Telearbeitsplätze an das BVN-Netz und damit die Nutzung der elektronischen Post in der bremischen Verwaltung (vgl. Ziff. 3.4.) bisher nicht realisiert wurde, wurden die erforderlichen E-Mail-Postfächer - ohne Abstimmung mit mir - bei einem privaten Provider eingerichtet. Dieses habe ich nur hingenommen, weil von den Arbeitsplätzen aus keine personenbezogenen Daten übertragen werden und dort auch nicht gespeichert sind.

In der zunächst letzten Sitzung der Arbeitsgruppe im Oktober 1999 ist zwar vereinbart worden, den Modellversuch mit den bisherigen Teilnehmerinnen weiterzuführen, da diese Telearbeitsplätze nicht auf eine Verbindung zum Dienststellennetz angewiesen sind. Die Aufgabenerledigung erfolgt am Telearbeitsplatz, der für die Aufgabenerledigung als stand-alone-PC genutzt wird. Sollte ein Datentransport erforderlich sein, so erfolgt dieser auf Diskette. Neue Teilnehmer werden bis zum Vorliegen eines abgestimmten Technikkonzeptes nicht mehr zugelassen.

6. Inneres

6.1. Bremisches Polizeigesetz

6.1.1. Der Auftrag der Koalition

Der Senator für Inneres, Kultur und Sport hat mir im August einen Referentenentwurf zur Änderung des Bremischen Polizeigesetzes übersandt und um Stellungnahme gebeten. Mit dem Entwurf kommt der Senator einem Auftrag aus der Koalitionsvereinbarung nach, die vorsieht, das Bremische Polizeigesetz entsprechend den Vorgaben des Bundesverfassungsgerichts umfassend zu reformieren. Der Entwurf enthält eine Vielzahl von Bestimmungen, die in erheblichem Umfang die polizeiliche Datenverarbeitung berühren und die von datenschutzrechtlicher Relevanz sind.

6.1.2. Zur Entwicklung des Polizeirechts

Das geltende Bremische Polizeigesetz (BremPolG) ist am 21.03.83 in Kraft getreten. Es hat zwar in den zurückliegenden Jahren einige kleine Änderungen erfahren, ist aber bezogen auf die Regelungen der polizeilichen Datenverarbeitung in seinen wesentlichen Zügen erhalten geblieben. Es stammt daher im großen und ganzen, wenn man den Zeitraum der politischen Diskussion mit einbezieht, aus den Jahren 1982/83, also aus einer Zeit vor der Verkündung des Volkszählungsurteils.

Dies bedeutet aber nicht, daß das Bremische Polizeigesetz – wie die meisten anderen Polizeigesetze der Länder der damaligen Zeit – keine Regelungen zur Informationsverarbeitung enthält. Vielmehr war der Gesetzgeber auf der Höhe der damaligen datenschutzrechtlichen und datenschutzpolitischen Diskussion und hat bereits damals die mit dem Volkszählungsurteil des Bundesverfassungsgerichts aufgestellten Grundsätze in weiten Teilen antizipiert und aufgenommen. Die im geltenden Gesetz enthaltene enge Ausgestaltung der Informationsgewinnung (Datenerhebung) hat daher ihre wesent-

liche Ursache nicht darin, daß die vielfältigen Formen möglicher Datenerhebungen nicht gesehen wurden. Sie beruht vielmehr darauf, daß aufgrund intensiver politischer Diskussionen der Gesetzgeber sich entschieden hat, polizeirechtliche Eingriffe in das informationelle Selbstbestimmungsrecht möglichst restriktiv und nicht intensiv zu regeln. Fachleute bezeichnen daher das geltende Bremische Polizeigesetz auch als "liberalstes Polizeigesetz der Länder".

Es dabei bewenden zu lassen, würde aber die neue Entwicklung des Polizeirechts in Bund und Ländern und die damit verbundene breit angelegte und facettenreiche Diskussion um die zulässige Reichweite und notwendige Regelungstiefe staatlicher Informationsverarbeitung im Sicherheitsbereich außer acht lassen. Denn bei allen Entwürfen der letzten Jahre zur Novellierung des Polizeirechts im Bund und den anderen Ländern spielt das Bemühen eine Rolle, für die Datenerhebung und –verwendung durch die Polizeibehörden umfassende Erhebungs-, Speicherungs-, Verwertungs- und Übermittlungsregelungen zu schaffen. Im Grunde genommen ist solchermaßen neben dem Einfluß der technischen Entwicklung durch das Datenschutzrecht die Fortentwicklung des Polizeirechts vorangetrieben worden. Verbunden ist damit aber auch die Verbreiterung der Möglichkeiten zum Einsatz besonderer und geheimer polizeilicher Methoden zur Informationsgewinnung.

Mittlerweile kann man feststellen, es gibt in Deutschland ein "neues Polizeirecht". Die Novellierungen der Polizeigesetze in den Bundesländern und die Änderungen des Bundeskriminalamts- und Bundesgrenzschutzgesetzes erweitern jedenfalls die Handlungsgrundlage der Sicherheitsbehörden erheblich. War parallel zum Innenbereich diese Entwicklung im Justizbereich zunächst dadurch geprägt, daß der Bundesgesetzgeber in manchen Bereichen der Strafverfolgung noch zögerte, besondere Eingriffsmethoden zuzulassen, ist der angesprochene Bereich auch bei der Strafverfolgung mittlerweile weitgehend durch neue Regelungen in der StPO abgedeckt, man denke nur an die erst vor kurzem erfolgte Grundrechtsänderung zur Einführung des Lauschangriffs. So gesehen liegt der vorliegende Gesetzentwurf des Senators für Inneres, Kultur und Sport im „Mainstream“.

Zu fragen ist aber, inwieweit für Zwecke der vorbeugenden Straftatenbekämpfung sämtliche in den Polizeigesetzen normierten besondere Eingriffsbefugnisse unter dem Gesichtspunkt der Erforderlichkeit noch ihren Bestand und ihre Berechtigung haben. Dies ist bisher genau so wenig untersucht worden, wie ihre Effektivität. Auch Instrumente der Strafprozeßordnung, wie die Rasterfahndung, die bereits frühzeitig in Kraft gesetzt wurden, wurden bisher nicht evaluiert. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf dieses Manko in einer Entschließung vom 05./06.10.1998 hingewiesen (vgl. 21 JB., Ziff. 20.6.). Insoweit stehen wissenschaftlich aufbereitete Erfahrungen anderer Länder hinsichtlich der Erforderlichkeit und der Effektivität neuer polizeirechtlicher Erhebungsmethoden für die Diskussion des BremPolG-E nicht zur Verfügung.
Im Ergebnis kann festgehalten werden, daß die Regelungen zur geheimen Datenerhebung in den Polizeigesetzen anderer Länder rasch eingeführt wurden, während die entsprechenden Regelungen für Zwecke der Strafverfolgung erst nach sorgfältiger Diskussion erlassen wurden. Viele Polizeigesetze anderer Länder, die in drei, vier Novellierungsschüben alle neuen Entwicklungstendenzen aufgenommen haben, sind verschachtelt und unübersichtlich geworden, so daß sie im Grunde genommen selbst ihre rechtmäßige Handhabung in Frage stellen. Diesen Fehler hat der bremische Gesetzgeber nicht gemacht. Vielmehr besteht hier die Chance, einen schlanken, einheitlichen und über-

sichtlichen Entwurf des Bremischen Polizeigesetzes vorzulegen. Wenn es gelingt, die mit dem übersandten Entwurf bereits vorgegebene klare Struktur zu erhalten und in einigen Punkten noch zu verbessern, ist dies die beste Gewähr dafür, daß die vom Gesetz gegebenen Vorgaben von dem einzelnen Polizeibeamten auch noch handhabbar sind. Schließlich muß berücksichtigt werden, daß viele polizeiliche Situationen, z. B. bei Gefahr im Verzuge, schnelle Entscheidungen erfordern.

In den letzten 15 Jahren ist es zu tiefgreifenden Änderungen und damit verbunden zu Aufweichungen hergebrachter Grundsätze des bisherigen Polizei- und Ordnungsrechts in Deutschland gekommen. Man kann daher festhalten, daß die bisher in Bund und Ländern erfolgten, bzw. im Land Bremen jetzt mit der Novellierung des Polizeigesetzes beabsichtigten Rechtsänderungen, zu denen noch solche des europäischen Sicherheitsrechts hinzutreten und hinzutreten werden (hingewiesen sei in diesem Zusammenhang nur auf das Schengener Informationssystem und auf Europol), in den gewählten Handlungsformen und Instrumenten im Grunde genommen den eigentlichen Funktionswandel des öffentlichen Sicherheits- und Ordnungsrechts abbilden. Und diese Entwicklung hängt nicht mit dem Volkszählungsurteil zusammen.

Dieser Entwicklung kann und will sich der Datenschutz nicht verschließen. Im Gegenteil, immer wieder wird deutlich, daß durchaus gemeinsame Interessen bestehen, wenn es darum geht, das Recht konkreten Lagen anzupassen. Soweit daher polizeipflichtige Personen in dem Umfang zur Informationsverarbeitung herangezogen werden, in dem sie für eine Gefahrenlage verantwortlich sind, bestehen keine Probleme, diese Personen in verfassungsrechtlich angemessenem Maße mit in die Pflicht zu nehmen und zwar auch bei der Informationsverarbeitung.
Problematisch wird es jedoch, wenn unbeteiligten Dritten Rechtspflichten vom Gesetz auferlegt werden, die zugleich einen tiefen Eingriff in ihre Freiheitsrechte darstellen. Beispiele hierfür sind die im Gesetzentwurf enthaltene technische Wohnraumüberwachung mit Ton- und Bildaufzeichnung oder die polizeiliche Beobachtung sogenannter "anderer Personen", die auch über Monate erfolgen kann.

Die neueren Polizeigesetze, auch der Entwurf des Bremischen Polizeigesetzes, versuchen zur "Erleichterung der polizeilichen Arbeit" zunehmend jedermann polizeipflichtig zu machen, sei es zur Mitwirkung durch Auskünfte, sei es zur Duldung von Kontrollen, wenn es zur Gefahrenvorsorge opportun erscheint.

Dem polizeilichen Pragmatismus entsprechen dabei oft nur solche Regelungen, die durch weitreichende Eingriffsermächtigungen und in hohem Maße auslegungsfähige Begrifflichkeiten gewünschte Flexibilität polizeilicher Arbeit sicherstellen. Die Aufrechterhaltung der empfindlichen Machtbalance im Rechtsstaat und die Gewährleistung von Rechtssicherheit wie auch die Vorhersehbarkeit polizeilicher Maßnahmen als Maßstab legislativen Handelns spielen bei einer vornehmlich an den praktischen Bedürfnissen der Polizei ausgerichteten Gesetzgebung dagegen oft nur eine untergeordnete Rolle.

Anliegen des Datenschutzes ist es, sicherzustellen, daß nicht eine Umkehrung der Rolle und damit auch eine Umkehrung der "Beweispflicht" der Bürger bei der Informationsverarbeitung eintritt. Es darf nicht passieren, daß jedermann als potentielles Sicherheitsrisiko eingestuft werden und daher jederzeit in Anspruch genommen werden kann, es sei denn, er oder ihn begleitende Dritte beweisen, daß

sie kein Sicherheitsrisiko darstellen. Ein weiteres Anliegen des Datenschutzes ist, die Normen so präzise zur formulieren und die Tatbestandsvoraussetzungen so klar zu beschreiben, daß nur dann ein Eingriff in das informationelle Selbstbestimmungsrecht erfolgen darf, wenn die tatsächliche Situation auch der jeweils vom Gesetzgeber angenommenen Gefahrenlage entspricht. Schließlich wird versucht, durch gesetzlich vorgeschriebene Verfahrensvorschriften eine ausufernde Anwendungspraxis zu verhindern.

Die Entscheidung darüber, welche Methoden zur Datenerhebung im Lande der Polizei zur Verfügung gestellt werden sollen, ist aber zunächst auch politischer Natur und daher insoweit den parlamentarischen Beratungen überantwortet.

6.1.3. Inhalt des Gesetzentwurfs

Abweichend von den Regelungen des bisherigen Polizeigesetzes werden im Gesetzentwurf die Aufgaben der Polizei u. a. in dem Vorfeldbereich von Gefahren dahin erweitert, daß sie Vorbereitungen trifft, insbesondere auch durch vorsorgliche Datenerhebung, um künftige Gefahren abwehren zu können. Weiter werden Regelungen zur Videoüberwachung auf öffentlichen Plätzen und bei Veranstaltungen vorgeschlagen, darüber hinaus soll ein Kanon von verdeckten polizeilichen Maßnahmen ermöglicht werden, hierzu zählen die polizeiliche Beobachtung, die längerfristige Observation, der Einsatz verdeckter technischer Mittel zur Aufnahme von Bild- und Tonaufzeichnungen des nicht öffentlich gesprochenen Wortes auch aus Wohnungen sowie die Datenerhebung durch sogenannte Vertrauenspersonen (V-Personen) und durch Polizeibeamte, die unter einer falschen Identität agieren, der sog. verdeckte Ermittler. Darüber hinaus präzisiert der Entwurf die bisher geltenden Regelungen zur Datenerhebung, Speicherung, Verwendung und Löschung. Neu ist auch eine Regelung, die dem Senator für Inneres, Kultur und Sport eine Auskunftspflicht gegenüber einem von der Bürgerschaft zu bildenden Ausschuß vorsieht, um neben der allgemeinen Datenschutzkontrolle durch den Landesbeauftragten für den Datenschutz auch eine regelmäßige parlamentarische Kontrolle eines Teils der mit verdeckten Methoden erhobenen Daten zu ermöglichen.

6.1.4. Konkrete datenschutzrechtliche Vorschläge

Ich habe dem Senator für Inneres, Kultur und Sport meine Stellungnahme zu dem Referentenentwurf im Oktober übermittelt. Da die Stellungnahme rund 45 Seiten umfaßt, können an dieser Stelle nur auszugsweise einige Vorschläge aufgegriffen werden.

So habe ich darauf hingewiesen, daß prinzipiell nur das bereichsspezifisch im Polizeigesetz geregelt werden sollte, was unbedingt erforderlich ist, und daher verlangt, Regelungen zurückzunehmen, die im Bezug auf die Rechte von Betroffenen von den Regelungen des Bremischen Datenschutzgesetzes abweichen und damit eine nicht begründete Verschlechterung der Rechtstellung dieses Personenkreises bewirken würde. Die Polizei ist über Jahre mit den allgemeinen Regelungen der Betroffenenrechte im BrDSG gut gefahren, im übrigen trägt eine Vermeidung von Parallelregelungen zur Begrenzung der oft beklagten Normenflut bei. Auch bedarf es nach meiner Auffassung einer Rechtsgüterabwägung mit den Interessen des Betroffenen, wenn seine Rechte auf informationelle Selbstbestimmung wegen der Gefährdung der Erfüllung jeglicher polizeilicher Aufgabe oder eines unverhältnismäßigen Aufwandes zurücktreten sollen.

Soweit besondere Vertrauensverhältnisse, wie z. B. zwischen Arzt und Patient oder Rechtsanwalt und Mandanten vom Einsatz besonderer technischer Mittel betroffenen sein können, habe ich gefordert, daß vom Gesetz ein umfassender Schutz und ein absolutes Verwertungsverbot sicherzustellen sind. Dies gilt insbesondere auch dann, wenn sich erst nachträglich herausstellen sollte, daß in diesem Feld von der Polizei Daten erhoben worden sind.

Sind Daten durch den verdeckten Einsatz technischer Mittel oder mit anderen verdeckten Erhebungsmethoden von der Polizei gewonnen worden, können diese Erkenntnisse selbstverständlich auch in anderen Verfahren von Interesse sein. Auch könnten von der Strafprozeßordnung aufgebaute Schutzmechanismen dadurch umgangen werden, daß die Daten durch den präventiven Einsatz gleicher Mittel gewonnen würden, um dann im Strafverfahren verwendet zu werden. Ich habe daher eine Gleichwertigkeitsregelung gefordert, die sicherstellen soll, daß bei der Verwendung mit besonderen Mitteln und Methoden nach dem Polizeigesetz erhobener und gespeicherter Daten, diese Daten für Zwecke anderer Aufgaben nach dem Polizeigesetz, nur verwendet werden dürfen, wenn bei den anderen Sachverhalten auch die tatbestandlichen Voraussetzungen für den Einsatz dieser Mittel gegeben wären. Soweit besondere Verfahrensregelungen vorgesehen sind, wie z. B. richterliche Kontrolle, muß – genauso wie dieses Prinzip auch in der Strafprozeßordnung konsequent durchgehalten wird – dieses Verfahren auch vorgeschaltet werden, wenn diese verdeckt, mit besonderen Methoden erhobenen Daten für ein anderes Verfahren oder für andere Zwecke nach dem Polizeigesetz verwendet werden sollen. Weiter habe ich zur Vereinfachung und besseren Übersichtlichkeit möglichst einheitliche Verfahrensregelungen hinsichtlich der Entscheidungsebenen, der Anordnungsbefugnis, der Eilzuständigkeit, der Fristen und der Dokumentationspflicht gefordert, wenigstens aber eine Harmonisierung empfohlen. Hinsichtlich der neu eingeführten Erhebungsmethoden, die zum Teil einen verdeckten Einsatz beinhalten, habe ich auf prinzipielle in Literatur und Rechtsprechung vertretene Bedenken hingewiesen, besondere verfahrenssichernde Maßnahmen vorgeschlagen und bei einer starken tatbestandlichen Abweichung auf gleichwertige Bundesregelungen, wie sie die Regelungen im Bundeskriminalamtsgesetz, in der Strafprozeßordnung und im Strafverfahrensänderungsgesetz darstellen, hingewiesen und auf eine Harmonisierung gedrungen. Schließlich habe ich Verbesserungsvorschläge unterbreitet, soweit die vorgeschlagenen Regelungen nicht im Einklang mit der Rechtsprechung verschiedener Verfassungsgerichtshöfe anderer Länder zu Regelungen der dortigen Landespolizeigesetze standen.

6.1.5. Weiteres Verfahren

Der Senator für Inneres, Kultur und Sport hat mir im Dezember einen überarbeiteten Gesetzentwurf übersandt, in dem eine Vielzahl meiner Anregungen übernommen worden sind. Im Januar sind daraufhin in einer Gesprächsrunde zusammen mit einem Vertreter des Senators für Justiz und Verfassung noch einmal die verbleibenden Kritikpunkte angesprochen worden. Die fachlich offen geführte Diskussion war fruchtbar und wird zu weiteren Verbesserungen des Gesetzentwurfes führen. Der Vertreter des Senators für Inneres, Kultur und Sport beabsichtigt, einen im Haus abgestimmten Entwurf zu erarbeiten, den er dann auch mir zur Verfügung stellen will. Ich gehe davon aus, daß die dann noch aus datenschutzrechtlicher Sicht verbleibenden Kritikpunkte auch in der politischen Diskussion noch eine Rolle spielen werden.

Rückblickend läßt sich positiv hervorheben, daß insbesondere unter Berücksichtigung der Erfahrungen mit anderen Gesetzentwürfen bei den Beratungen des Polizeigesetzentwurfs in jeder Phase meine Beteiligung sichergestellt war und - soweit es aus politischer Sicht des Hauses vertretbar schien – weitgehend versucht wurde, meinen Verbesserungsvorschlägen Rechnung zu tragen.

6.2. Zur polizeilichen Datenverarbeitung

6.2.1. Richtlinien zur Telefonüberwachung

Aufgrund meiner Prüfergebnisse bei der Durchführung von Telefonüberwachungs-Maßnahmen durch die Polizei (vgl. 19. JB, Ziff. 9.2.) habe ich dem Senator für Inneres die Überarbeitung der völlig veralteten "Richtlinien für das taktische Vorgehen anläßlich einer Überwachung des Fernmeldeverkehrs nach §§ 100 a und 100 b StPO" vorgeschlagen.

Bei Durchführung meiner Prüfung wurden die Telefonüberwachungs-Maßnahmen noch dezentral von den einzelnen Organisationseinheiten durchgeführt. Inzwischen hat sich einiges geändert. So erfolgt die Durchführung von Telefonüberwachungs-Maßnahmen durch eine zentrale Organisationseinheit. Durch die Übermittlung richtungsgetrennter Daten (Inhalts- und Verbindungsdaten) verringert sich bei Einsatz der vorhandenen Technik die Kapazität für die Durchführung von Überwachungen. Geplant wurde daher die Beschaffung eines neuen Systems, in dem die Gesprächsdaten zunächst auf Festplatte gespeichert und auf optische Datenträger (MOD) übertragen werden sollen. Die Datenträger sollen zentral in einer an das System angeschlossenen Juke-Box vorgehalten werden. Vorgesehen ist dabei die Anlage von zwei MOD für jede Telefonüberwachungs-Maßnahme mit gleichem Inhalt: eine Beweis-MOD und eine Arbeits-MOD. Die Beweis-MOD ist nicht beschreibbar und wird zentral verwahrt. Der Zugriff auf die Arbeits-MOD soll für jede Maßnahme einem zuständigen Sachbearbeiter zur Verschriftung erteilt werden. Auf den MOD's soll jedes Gespräch in eine eigene WAVE-Datei gespeichert und jeder Zugriff auf die Arbeits-MOD auf dem Administrations-PC protokolliert werden. Vorgesehen ist die Implementierung des neuen Systems in den Räumen des neuen Polizeipräsidiums. Mir sind in diesem Zusammenhang noch nähere Informationen über die eingesetzte Technik versprochen.

Mit der Überarbeitung der Richtlinien ist nach Beseitigung eines Personalengpasses (vgl. 20. JB, Ziff. 12.3.) begonnen worden. Mir ist im Sommer der Entwurf eines Erlasses vorgelegt worden, der Rahmencharakter hat. Den geschilderten Veränderungen kann damit allein in keiner Weise ausreichend Rechnung getragen werden. In einem Gespräch legten Vertreter des Senators für Inneres und der Polizei dar, daß der Erlaß um eine von der Polizei zu erstellende Dienstanweisung mit entsprechend technischen, personellen und rechtlichen Regelungen ergänzt werden solle. Eventuell wird auch eine Änderung der Errichtungsanordnung und des Datenschutzkonzeptes erforderlich. Ich habe darauf hingewiesen, daß in diesem Fall Erlaß und Dienstanweisung nur zusammen bewertet werden können.

Ich erwarte, daß neben dem Erlaß, die Dienstanweisung sowie, soweit erforderlich, auch die Änderungen der Errichtungsanordnung bzw. des Datenschutzkonzeptes im Frühjahr vorgelegt und der Abstimmungsprozeß im ersten Halbjahr abgeschlossen werden kann.

6.2.2. Informationssystem der Polizei (INPOL-neu)

Bereits im letzten Jahresbericht (21. JB, Ziff. 9.4.1.) habe ich über die geplante bundesweite Einführung von INPOL-neu zum 01.01.2000 berichtet. Die Erstellung der Fachkonzepte ist abgeschlossen. Zur Zeit sind Systemtests durch die Arbeitsgruppe 'AGIL' mit Vertretern fast aller Bundesländer vorgesehen. Geplant ist die Fahndungsabfrage aller Verbundteilnehmer bis zum Mai 2000 zu realisieren. Dafür sollen die in der Arbeitsgruppe vertretenen Länder über Clients mit dem Zugangsserver des Bundeskriminalamtes (BKA) verbunden werden. Die Client-Anbindung ist noch nicht verifiziert: möglich wäre diese über eine Emulation im HTML-Format oder über auf dem PC ablaufende ausführbare Programme. Der Produktionsbetrieb soll Mitte 2002 aufgenommen werden, wobei Test- und Produktionsbetrieb zeitlich begrenzt parallel laufen sollen. Mit Aufnahme des Produktionsbetriebes wird die Abschaltung der Falldateien aus INPOL-alt erfolgen.

Entwürfe für die Errichtungsanordnungen zu den Anwendungen von INPOL-neu sind dem BfD vorgelegt worden. Die Entwürfe sollen gemeinsam von der INPOL-Arbeitsgruppe, der INPOL-Projektgruppe, dem BMI und dem BfD beraten werden.

Ungeklärt ist noch die Migration der in INPOL-alt gespeicherten Daten in INPOL-neu. Vorgesehen ist, Daten, die nicht die Kriterien des BKAG erfüllen, nicht ungeprüft in INPOL-neu zu überführen. Eine automatisierte Filterung der Daten ist mangels Definition von Kriterien nicht möglich.

Unklar ist immer noch die Frage eigener Landesdatenhaltungen oder Auftragsdatenverarbeitung durch das BKA. Die Innenverwaltungen einiger Länder favorisieren eine Auftragsdatenverarbeitung durch das BKA, um sich zu entlasten. Der Bundesbeauftragte für den Datenschutz (BfD) und eine Reihe von Landesbeauftragten für den Datenschutz sprechen sich dagegen aus, da aus Sicht der Datenschutzbeauftragten eine zentrale Datenhaltung für Deutschland entstehen würde. Auch sieht das BKA-Gesetz eine Auftragsdatenverarbeitung in diesem Umfang nicht vor. Aus der Sicht des Datenschutzes ist bei enger technischer Abstimmung ein eigenes System für die Länderdaten zu favorisieren, weil sonst langfristig zu befürchten ist, daß diese Differenzierung zwischen Daten von Bund und Land fallengelassen wird. Eine Alternative wäre ein kostenloses Angebot der für INPOL-neu entwickelten Datenbanksoftware für die Länder durch das BKA.

Ein weiterer offener Punkt ist die Protokollierung. Das BKA sieht eine Protokollierung aller Transaktionen vor, möchte aber nur 10 % der Protokolldaten für Zwecke der Datenschutzkontrolle zur Verfügung stellen. Die Länder sprechen sich für eine Vollprotokollierung der positiven Abfragen (Treffer) aus. Der BfD hat ein Thesenpapier zur Protokollierung von Abrufen des polizeilichen Informationssystems INPOL-neu vorgelegt. Eine Stellungnahme durch den BfD ist noch nicht erfolgt.

Ich werde mich weiterhin in regelmäßigen Zeitabständen über die Entwicklung der einzelnen Stufen und deren Umsetzung informieren.

6.2.3. Neues polizeiliches Landesinformationssystem

Ich habe bereits im letzten Bericht (vgl. 21. JB, Ziff. 9.4.2) über die Auswirkungen bei der Einführung von INPOL-neu auf die polizeiliche Informationsverarbeitung im Lande Bremen berichtet. Im Berichtszeitraum habe ich mich bei der Polizei über die Entwicklungen im Bereich Hard- und Software-Be-

schaffung und die daraus resultierenden organisatorischen Maßnahmen informiert. Im Herbst wurde eine Arbeitsgruppe für die Evaluation eines Vorgangsbearbeitungssystems für die Polizei, einschließlich Wasserschutzpolizei und Polizei Bremerhaven, gegründet. Im Frühjahr soll die Auswahl getroffen und der Einführungsprozeß gestartet werden.

Die Polizei hat meinen Hinweis über die Verbesserung des Zugangsschutzes zu den Systemen (vgl. 21. JB, Ziff. 9.4.3.) aufgegriffen. Die neubeschafften PC verfügen über eine Cherry-Tastatur mit integriertem Chipkarten-Lesegerät. Die Anmeldung über Chipkarte wird umgehend nach Lieferung der Karten umgesetzt. Bis dahin wird der Zugangsschutz über das Betriebssystem gewährleistet. Nach Entfernen der Karte aus dem Lesegerät soll automatisch eine Abmeldung des laufenden Programms erfolgen und der Anmeldebildschirm angezeigt werden. Die Polizei hat zugesagt, den bisherigen Standard der Protokollierung bei Abfragen beizubehalten.

6.2.4. E-Mail-Server bei der Polizei

Die durch den Umzug des Polizeipräsidiums vorgenommene Neukonzeption der DV-Landschaft beinhaltet die Einführung von E-Mail für den Polizeibereich. Für die Polizei wird eine eigene Domäne eingerichtet. Über einen Server mit zwei Netzkarten werden die Verbindungen zum BVN und zum ISA-D-Netz realisiert.

Vor der Einführung wurden mir ein Konzept, eine Benutzerordnung und eine Dienstanweisung für den E-Mail-Einsatz vorgelegt. Wichtige Punkte der Benutzerordnung sind u.a.

- der Verzicht auf die Versendung sensibler personenbezogener Daten ohne Verschlüsselung sowie die Verschlüsselung von Attachments,
- ein Hinweis auf Sicherung der Nachrichten und Dateianhänge durch eine digitale Signatur,
- eine Dateienprüfung auf Viren vor Versendung und Übermittlung des Prüfprotokolls als Anlage der E-Mail und
- auf eine Paßwortspeicherung in der Mail-Software wird verzichtet.

Die Benutzerordnung wird jedem E-Mail-Anwender ausgehändigt. Die Dienstanweisung regelt den Geltungsbereich und die Organisation für das Handling der E-Mails. Im Kapitel Datenschutz wird u.a. auf den Einsatz von Verschlüsselung und digitaler Signatur hingewiesen, die Übermittlung von ausführbaren Programmen verboten und die Verpflichtung zur Prüfung übersandter Programme und Dateien betont.

Das Konzept beinhaltet u.a. Regelungen für das Namenskonzept und die Ausstattung der PC auf denen E-Mail möglich ist. Die E-Mail-Einführung in der Polizeibehörde wird stufenweise unter Einbeziehung vorhandener Hardwarekomponenten erfolgen. Jede angeschlossene Organisationseinheit ist für die Bearbeitung der E-Mails verantwortlich.

Nach Durchsicht der Unterlagen habe ich der Polizei die Berücksichtigung der unter Ziff. 5.4. aufgeführten Punkte empfohlen. Die Unterlagen werden derzeit von der Polizei überarbeitet und mir anschließend zugesandt. Ich werde die E-Mail-Einführung bei der bremischen Polizei weiter beraten.

6.2.5. DNA-Analyse-Datei

Im Sommer 1999 übersandte mir der Senator für Inneres, Kultur und Sport den ihm vom Bundesminister des Innern zugegangenen Entwurf einer Errichtungsanordnung für die DNA-Analyse-Datei. In meiner Stellungnahme habe ich einige Anregungen zur Verbesserung des Datenschutzes gemacht. Der Senator für Inneres, Kultur uns Sport hat diese in die Beratungen eingebracht. Im Zustimmungsverfahren mit den Ländern gem. § 34 Abs. 2 BKAG sind einige Punkte geändert worden. Der Senator für Inneres, Kultur und Sport hat mir die mittlerweile in Kraft getretene Errichtungsanordnung "DNA-Analyse-Datei" Ende des Jahres zur Kenntnis gegeben.

6.2.6. Umzug der Polizei Bremen

Die Polizei Bremen ist im letzten Quartal 1999 - im Schwerpunkt im November 1999 - aus verschiedenen Häusern, insbesondere aus dem Polizeipräsidium, in neue Räumlichkeiten in das Dienstgebäude in der Vahr umgezogen. Deshalb hatte ich mich bereits rechtzeitig vor dem Umzug über die getroffenen Sicherheitsmaßnahmen durch die Polizei Bremen informiert. Zugesichert war, daß die Beamten das schutzwürdige Material selbst in entsprechende Umzugscontainer verpacken. Diese sollten verschlossen und in der Dienststelle registriert werden. So entstandene Begleitlisten sollten dann dazu genutzt werden, beim Eingang im neuen Dienstgebäude die Vollständigkeit der angelieferten Container sicherzustellen. Gleichzeitig hatte ich mir eine Umzugsliste von der Polizei Bremen geben lassen und in einer Stichprobe die Einhaltung der zugesicherten Maßnahmen überprüft.

Selbstverständlich habe ich in diesem Zeitraum auf Prüfungen verzichtet. Nur soweit dies unabweisbar war und der Sachverhalt eine zeitnahe Aufklärung erforderte, habe ich im Einzelfall auf Datenschutzprobleme hingewiesen. Ein solcher Fall ergab sich, als im November ein Journalist einer auch in Bremen erscheinenden Tageszeitung mich darauf hinwies, daß aus dem Umzug stammende erkennungsdienstliche Unterlagen in der Öffentlichkeit aufgefunden worden seien. Nachforschungen ergaben, daß scheinbar beim Abtransport alter Möbel aus dem bereits teilweise geräumten Polizeipräsidium entsprechendes Fotomaterial von Beschäftigten der Entsorgungsfirma gefunden wurde. Ich habe mich daraufhin umgehend mit dem behördlichen Datenschutzbeauftragten bei der Polizei Bremen in Verbindung gesetzt, auf die Schwachstelle hingewiesen und ihn gebeten, die Dienststellen, bei denen noch der Umzug ansteht, sofort auf diese Schwachstelle hinzuweisen und noch im Polizeipräsidium zurückgelassenes Mobiliar daraufhin zu untersuchen, ob sich in ihm noch personenbezogenes Datenmaterial befindet. Weiter habe ich darum gebeten, das abhanden gekommene Datenmaterial bei der Redaktion herauszuverlangen und seinem rechtmäßigen Gebrauch zuzuführen oder zu vernichten.

Angesichts des immensen Datenmaterials, das transportiert werden mußte, betrachte ich die von der Presse aufgedeckte Schlamperei als einen geringfügigen Verstoß. Insgesamt bin ich froh, daß das gesamte Umzugsprojekt scheinbar ohne gravierende Datenschutzverstöße von statten gegangen ist.

Nur eins sei noch zum Umzug angemerkt. Die Mengen von Materialien mit personenbezogenen Daten, die aus Anlaß des Umzuges vernichtet worden sind, führen zwar nicht zu dem Wunsch, die Polizei möge alle zehn Jahre umziehen, gleichwohl zeigt es aber, daß in regelmäßigen Abständen

überprüft werden sollte, ob die vielen Akten mit personenbezogenen Daten tatsächlich noch für die Aufgabenerfüllung erforderlich sind. Aber auch hier könnte mit der Novellierung des Bremischen Polizeigesetzes eine Verbesserung eintreten, wenn bereichsspezifische Prüffristen und Löschungsbestimmungen verabschiedet werden.

6.2.7. Bürgereingaben zur polizeilichen Datenverarbeitung

Auch in diesem Berichtsjahr habe ich zusammen mit dem polizeilichen Datenschutzbeauftragten eine Reihe von Bürgereingaben erledigen können. In dem einen oder anderen Fall konnten für den Bürger insbesondere durch Löschungen von Daten in polizeilichen Informationssystemen datenschutzrechtliche Verbesserungen erreicht werden. In einem Fall, in dem ein Betroffener mir gegenüber behauptete, ein Bremer Polizeibeamter habe über ihn Daten aus den Polizeicomputern abgefragt und diese privat gegenüber einer Mitbewohnerin offenbart, habe ich eine Protokollauswertung verlangt. Im bremischen Informationssystem ISA haben wir eine Vollprotokollierung aller Zugriffe auf personenbezogene Datensätze. Diese Protokolldaten können dazu genutzt werden, rechtmäßiges Handeln der Polizeibeamten zu überprüfen, gleichzeitig wirkt eine Vollprotokollierung präventiv. Eine Protokollauswertung kann zwar einen Polizeibeamten belasten, sie kann aber eben auch einen Verdacht entkräften. So war es im vorliegenden Fall, der Verdacht des Bürgers bestätigte sich nicht.

6.3. Meldewesen

6.3.1. Änderung des Landesmeldegesetzes - noch keine Fortschritte

Die obsuleten Änderungen des Landesmeldegesetzes (vgl. auch 20. JB, Ziff. 12.8 und 21. JB, Ziff. 9.6) erfolgten bisher nicht. Obwohl dem Datenschutzausschuß der Bremischen Bürgerschaft bereits in der letzten Legislaturperiode Zusagen seitens des Innensenators gemacht worden sind, ist es auch im Berichtsjahr nicht zur Vorlage eines Gesetzentwurfes gekommen. Es lag bis zum Redaktionsschluß dieses Berichtes noch nicht einmal ein Referentenentwurf vor.

Im Datenschutzausschuß der Bremischen Bürgerschaft wurde im Zusammenhang mit der Diskussion meines letzten Jahresberichts ausführlich auch über die Stagnation im Melderecht diskutiert. Im Datenschutzausschuß wurde der Vorgang als Mißachtung eines eindeutig geäußerten parlamentarischen Willens gerügt. Der Datenschutzausschuß erwartet, daß ein Entwurf unverzüglich erstellt wird und der Bremischen Bürgerschaft (Landtag) so rechtzeitig vorgelegt wird, daß das Gesetz noch im Laufe des Jahres 2000 in Kraft treten kann (vgl. Ziff. 4.1.).

6.3.2. Mängel bei der Übermittlung von Meldedaten an die Parteien vor der Bürgerschaftswahl

Auch der folgende Sachverhalt war bereits Gegenstand der Beratungen des Datenschutzausschusses (vgl. Ziff. 4.1.). Zahlreiche Bürger haben sich im Vorfeld der Bürgerschaftswahlen an mich gewendet und sich über unverlangt zugesandte Wahlwerbung beschwert. Ich habe deshalb bei den Meldebehörden in Bremen und Bremerhaven überprüft, welche Datenübermittlungen es 1999 an politische Parteien gegeben hat und welche rechtlichen Prüfungen dem vorgeschaltet waren. Bei dieser Überprüfung ergaben sich folgende Mängel.

- Von der Bremer Meldebehörde waren an mehrere politische Parteien, SPD, F.D.P., DVU, Bündnis 90/Die Grünen, Meldedaten (Adreßdaten wahlberechtigter Bürger, die der Weitergabe ihrer Daten an politische Parteien nicht widersprochen hatten) auf auswertbaren Disketten, z. T. sortiert nach bestimmten städtischen Regionen bzw. Postleitzahl-Bereichen übermittelt worden. Auch die Anrede war enthalten. In Einzelfällen sind diese Daten an Empfänger außerhalb Bremens weitergegeben worden.

  Besondere Bedenken wurden von den Bürgern der Datenübermittlung an die DVU entgegengebracht. Tatsächlich betraf der Umfang alle wahlberechtigten Bürger im Alter von 18 bis 35 Jahren sowie ab dem 60. Lebensjahr aufwärts, die der Datenweitergabe an politische Parteien nicht widersprochen hatten. Befürchtungen wurden auch geäußert wegen der Art des verwendeten Datenträgers (Diskette) und der Weitergabe der Daten durch die Landesgliederung der DVU an die Münchener Parteizentrale, die möglicherweise die Rechnerleistungen der Frey-Firmen in Anspruch nahm.

Das Bremische Meldegesetz läßt eine regionale Sortierung der Angaben aus dem Melderegister ebenso wenig zu wie die Mitteilung der Anrede. Dies mag bedauern, wer die Verteilung durch ehrenamtliche Helfer oder Parteimitglieder organisiert. Auch liegt mit dem Vornamen in aller Regel auch die Anredeform offen. Gleichwohl sind diese Kriterien von den geltenden Bestimmungen nicht zugelassen. Eine bestimmte Art von Datenträgern für die Meldedatenübermittlung wird vom Meldegesetz nicht vorgeschrieben mit der Folge, daß heute meist elektronisch verwertbare Datenträger wie z.B. Disketten verwendet werden.

- Von der Bremerhavener Meldebehörde wurden insgesamt zweimal Meldedaten an die DVU übermittelt. Bei der ersten Datenübermittlung, die per Liste erfolgte, waren mehr Daten von Wahlberechtigten weitergegeben worden als von der Partei angefordert. Beim zweiten Übermittlungsvorgang waren unterteilt in zwei Gruppierungen (18 bis 30-jährige sowie 31-jährige aufwärts bis unendlich) sogar die Daten aller Bremerhavener Wahlberechtigten, die der Weitergabe nicht widersprochen hatten, an die DVU übermittelt worden. Die Datenübermittlung erfolgte auf Diskette. Außerdem wurden in beiden Fällen mehr Daten als im Katalog des Meldegesetzes vorgesehen weitergegeben (z.B. Namensbestandteile). Auch die Bremerhavener Meldedaten wurden von der örtlichen Gliederung der DVU an die Münchener Parteizentrale weitergereicht.

Das Bremische Meldegesetz (§ 33 Abs. 1) läßt die Übermittlung der Daten aller Wahlberechtigten, die der Weitergabe ihrer Daten nicht widersprochen haben, wegen der ausdrücklichen Festlegung des Auswahlkriteriums „Lebensalter der Betroffenen“ nicht zu. Es dürfen nur die Daten bestimmter Altersgruppen (z.B. Jungwähler, Senioren) übermittelt werden. Eine Aufteilung der Wahlberechtigten in mehrere Auswertungsgruppen mit der Möglichkeit, diese Gruppen wieder zu einem Ganzen zusammenzufügen, bedeutet im Ergebnis, daß der gesamte Datenbestand, d.h. alle Wahlberechtigten ohne Widerspruchsmerkmal übermittelt wird. Dies verstößt gegen das Bremische Meldegesetz. Besonders pikant ist in diesem Zusammenhang, daß die Meldebehörde in Bremen sich geweigert hatte, die Adressen aller Wahlberechtigten ohne Widerspruchsvermerk an die DVU zu übermitteln. Erst nachdem die Bremer Meldebehörde sich mehrfach an den Senator für Inneres gewandt hatte und

die DVU beim Verwaltungsgericht Bremen schon eine einstweilige Anordnung zur Herausgabe der von ihr gewünschten Adreßdaten aus dem Melderegister beantragt hatte, haben sich beide Seiten auf den oben geschilderten Kompromiß geeinigt. Die Bremerhavener Meldebehörde indes hatte den bei ihr von der DVU angeforderten Gesamtdatenbestand ohne zu Zögern übermittelt. Eine Abstimmung zwischen den Behörden in Bremen und Bremerhaven hatte es nicht gegeben. Dieses Beispiel zeigt sehr eindringlich, wie notwendig landeseinheitliche Ausführungsbestimmungen bzw. Verwaltungsvorschriften sind.

Über die festgestellten Mängel habe ich den Senator für Inneres, Kultur und Sport sowie den Datenschutzausschuß der Bremischen Bürgerschaft unterrichtet. Zugleich habe ich meine Vorschläge zur Änderung der Gesetzesbestimmung formuliert: Der Katalog der an die Parteien übermittelbaren Daten müßte präziser definiert werden. Es sollte sichergestellt werden, daß nur bremische Parteiorganisationen Wählerdaten für Zwecke der Wahlwerbung erhalten und weiterverarbeiten dürfen. Auch sollte der für die Übermittlung zu verwendende Datenträger bereits im Gesetz vorgeschrieben werden, Papierlisten und Adreßaufkleber sollten den Vorzug erhalten. Bei elektronischen oder optischen Datenträgern ist eine beliebige Umsortierbarkeit der Daten und ihre Verknüpfung mit weiteren Daten möglich. Eine Bindung an den Übermittlungszweck „Wahlwerbung“ kann hier nicht sichergestellt werden.

Dem Datenschutzausschuß habe ich darüber informiert, daß die Konferenz der Datenschutzbeauftragten einen Beschluß gefaßt hat, in dem sie darauf hinweist, daß das informationelle Selbstbestimmungsrecht der Betroffenen sich besser wahren läßt, wenn die in vielen Meldegesetzen enthaltene Widerspruchslösung durch eine Einwilligungslösung ersetzt würde. Viele Bürgerbeschwerden wären dann gegenstandslos.

6.3.3. Neues DV-Verfahren für das Einwohnermeldewesen in Bremerhaven

Die rasante Entwicklung der Informationstechnologie in den letzten Jahren und die Notwendigkeit für die Bremerhavener Stadtverwaltung, ihre Datenverarbeitungs- und Kommunikationstechnik den neuen technischen Möglichkeiten anzupassen, haben zu der Entscheidung geführt, die automatisierten Großverfahren der Verwaltungspolizei (Einwohnermeldewesen, Kfz-Zulassung, Führerscheinwesen, Ausländerwesen, Ordnungswidrigkeiten) abzulösen und durch neue, rechtlich, organisatorisch und technisch aktuellere DV-Verfahren zu ersetzen.

Das abzulösende DV-Verfahren Einwohnermeldewesen war eine Eigenentwicklung der Stadt. Die auf dem Rechner installierten Verfahren hinkten seit langem der rechtlichen, organisatorischen und technischen Entwicklung hinterher. Sie hätten nur mit hohem Aufwand auf einen aktuellen Stand gebracht werden können.

Geplant ist, im März 2000 für die Meldebehörde Bremerhavens ein neues Client–Server–Verfahren auf Windows–Basis mit mindestens gleicher Funktionalität wie bisher von einem privaten Softwareanbieter einzuführen (Meso 96 – Meldebehördensoftware) und das alte Großrechnerverfahren "Einwohnermeldewesen" dann einzustellen.

Ich werde über den Übernahmeprozeß regelmäßig informiert. Zur Testinstallation Anfang 2000 soll ich eingeladen werden, um dann aus datenschutzrechtlicher Sicht zu einzelnen Punkten des Meso 96-

Verfahrens Stellung nehmen zu können. Hinsichtlich der Sicherheit des Client-Server-Verfahrens habe ich wegen der Vielzahl ähnlicher Verfahren ein Einsatz- und Administrationskonzept für den zentralen Server (Rechner) sowie besondere anwendungsorientierte Sicherheitsmaßnahmen für die einzelnen Clients (Arbeitsplätze) der Meldebehörde verlangt. Ferner wurden von mir ein Sicherheitskonzept für die geplante Fernwartung und die Einbindung des Meso 96-Verfahrens in das Verwaltungsnetz des Magistrats samt evtl. Internet- und E-Mail-Anschluß verlangt.

6.4. Statistik und Wahlen

6.4.1. Volkszählung 2001 - aktueller Stand der Debatte

Die letzte geplante große Volkszählung 1983 hat ja bekanntlich zu erheblichen Bürgerprotesten Anlaß gegeben. Ich widme mich daher besonders aufmerksam allen neuen Bestrebungen in dieser Sache. In meinem letzten Jahresbericht (vgl. 21. JB, Ziff. 9.5) hatte ich die Überlegungen zur nächsten Volkszählung im Jahre 2001 dargestellt. Diese Zählung soll in der gesamten Europäischen Union durchgeführt werden. Geplant ist auch ein statistischer Methodenwechsel, d.h. nicht mehr alle Einwohner sollen direkt befragt werden, sondern es sollen vorhandene öffentliche Register und Datenbestände sowie laufende amtliche Statistiken genutzt werden. Zwei Lösungsmodelle wurden diskutiert.

Im Berichtsjahr wurde beschlossen, Test- und Qualitätsuntersuchungen für die beiden Modellvarianten (Bundesmodell, umfassenderes Landesmodell) durchzuführen. Nach dem Ergebnis dieser Untersuchungen soll dann über die konkrete Ausgestaltung der neuen Volkszählung und damit über ein konkretes Gesetzesvorhaben entschieden werden. Die Durchführung der Testuntersuchungen soll auf der Basis eines spezifischen Gesetzes erfolgen, das bisher allerdings noch nicht erlassen ist.

Die von der EU (Eurostat – Statistisches Amt der Europäischen Union) im Jahre 2001 erwarteten Zensusdaten sollen deshalb aus der laufenden Bevölkerungsstatistik, einem zeitnahen Mikrozensus sowie Statistiken der Bundesanstalt für Arbeit bereitgestellt werden. Der bisher bestehende Zeitdruck für die Vorbereitung und Durchführung eines gemeinschaftsweiten Zensus 2001 wäre damit entfallen.

Im Zusammenhang mit der geplanten neuen Volkszählung steht auch ein Gesetzesvorhaben des Bundes mit Folgewirkungen für das Land, mit dem das Melderechtsrahmengesetz (MRRG) erneut geändert werden soll (Entwurf eines 2. Gesetzes zur Änderung des MRRG – Stand 28.9.1999). Mit den geplanten Änderungen soll u.a. die Qualität der kommunalen Melderegister verbessert werden, die Melderegister sollen also zensustauglich gemacht werden.

Hierzu sieht der Gesetzentwurf u.a. die Schaffung einer Befugnisnorm für die Meldebehörden zur Überprüfung der Meldedaten von solchen Einwohnern vor, bei denen aufgrund ihres gruppentypischen Meldeverhaltens davon ausgegangen werden müsse, daß die im Melderegister gespeicherten Daten in größerem Umfang unrichtig geworden sind (Gruppenüberprüfung von Amts wegen z. B. bei Inhabern von Nebenwohnungen, jüngeren mobilen Einwohnern, Ausländern). Des weiteren sollen die öffentlichen Stellen, denen Meldedaten zur Erfüllung ihrer Aufgaben übermittelt wurden, verpflichtet werden, ohne Rücksicht auf etwaige Geheimhaltungsbestimmungen ihrerseits festgestellte Unstimmigkeiten oder Abweichungen bei den Daten den Meldebehörden mitzuteilen.

Gegen beide Neuerungen werden erhebliche Datenschutzbedenken geltend gemacht: Inhabern von Nebenwohnungen, mobilen jüngeren Einwohnern und Ausländern generell ein nachlässiges Meldeverhalten zu unterstellen, ist durch Fakten nicht belegt. Im übrigen ist auch unklar, wie die Gruppenüberprüfungen seitens der Meldebehörden durchgeführt werden sollen (Ortsbegehungen, Einsatz der Schutzpolizei als Außendienst der Meldebehörde?). Evtl. bestehende Defizite hinsichtlich des Meldeverhaltens dieser Einwohner könnten durch andere (mildere) Maßnahmen wie z.B. eine verbesserte Aufklärung dieser Einwohner, Unterstützungsangebote der Verwaltung oder dgl. gemindert werden. Die Verpflichtung anderer Behörden, denen Meldedaten übermittelt werden, zur Rückmeldung evtl. unstimmiger Daten an die Meldebehörde ohne Rücksicht auf bestehende Geheimhaltungs- und Verschwiegenheitsverpflichtungen ist im Hinblick auf das öffentliche Interesse an einem richtigen und vollständigen Melderegister nicht gerechtfertigt. Wesentliche Datenschutzprinzipien wie z. B. die informationelle Aufgabenteilung, Zweckbindung der Daten und Verhältnismäßigkeitsprinzip würden dabei ignoriert.

Ende Januar 2000 haben die beiden Regierungsfraktionen einen überarbeiteten Entwurf eines Zweiten Gesetzes zur Änderung des Melderechtsrahmengesetzes (MRRG) in den Bundestag eingebracht. Soweit datenschutzrechtlichen Einwände fortbestehen, unterstütze ich die Bemühungen, diese Probleme im weiteren Gesetzgebungsverfahren zu bereinigen.

6.4.2. Auslegung des Wählerverzeichnisses

Die Wählerverzeichnisse werden in Bremen von den Meldebehörden aus dem Meldebestand erstellt. In dem Meldebestand sind jedoch eine Vielzahl von Personen enthalten, für die zu deren Schutz vor Belästigungen oder Bedrohungen ein Sperrvermerk eingetragen ist. Dieser Sperrvermerk bewirkt, daß keine Privatpersonen über diese Personen Auskunft erhalten. Diese Sperrvermerke werden jedoch nicht bei der Erstellung der Wählerverzeichnisse berücksichtigt, so daß Privatpersonen während der Auslegungsfrist der Wählerverzeichnisse auch Kenntnis von den Daten von Personen mit Sperrvermerk erhalten.

Der Senator für Inneres hat bereits mehrfach zugesagt (vgl. 17. JB, Ziff. 9.4.2 oder 20. JB, Ziff. 12.10), diese Regelungslücke im Wahlgesetz zu schließen. Leider ist bisher keine konkrete Umsetzung erfolgt.

6.5. Personenstandswesen

6.5.1. Keine ausreichenden Regelungen durch den Bund

Häufig schon habe ich in den vergangenen Jahren eine Änderung und Ergänzung des Personenstandsgesetzes (PStG) um wichtige Datenschutzanliegen angemahnt (vgl. zuletzt den 19. JB, Ziff. 9.4.). Bis heute ist in dieser Sache nichts geschehen. Obgleich der Bundesgesetzgeber in den letzten Jahren einige Veränderungen am Personenstandsgesetz vorgenommen hat, indem z. B. der Umfang der vom Standesbeamten zu erhebenden Daten und die Mitteilungspflichten erweitert wurden, versäumte er es, auch den datenschutzrechtlichen Notwendigkeiten Rechnung zu tragen.
Aus meiner Sicht sind insbesondere präzisere Bestimmungen, mit denen die Einhaltung des Adoptionsgeheimnisses gewährleistet wird, dringend erforderlich. Mit den geltenden Regelungen des

Personenstandsgesetzes ist die Einhaltung des Offenbarungs- und Ausforschungsverbotes nach § 1758 BGB nicht ausreichend sichergestellt.

Weiterhin müßte bereits im Personenstandsgesetz festgelegt werden, daß die Herausgabe personenbezogener Daten durch die Standesämter zum Zwecke der Veröffentlichung nur mit Einwilligung der Betroffenen zulässig ist. Gesetzlich definiert werden müßte dabei auch, in welchen Fällen, in welchem Umfang und unter welchen Voraussetzungen eine Bekanntgabe von Daten möglich ist.

An einer Unterstützung durch den Senator für Inneres mangelt es nicht, hatte doch der Senat in seiner Stellungnahme zu meinem 19. JB bereits erklärt, er werde meine Anregungen in seine Stellungnahme gegenüber dem Bundesminister für Justiz einbeziehen (vgl. Bürgerschafts-Drs. 14/779, S. 4). Der Bund ist damit weiterhin in der Pflicht.

6.5.2. Datenzugang für Zwecke der Forschung

Den datenschutzrechtlichen Anforderungen besser angepaßt werden sollten auch die Bestimmungen des Personenstandsgesetzes, die die Einsicht in die Personenstandsbücher, deren Durchsicht und die Erteilung von Personenstandsurkunden regeln (derzeit § 61 PStG). Immer wieder erhalte ich gerade zur datenschutzrechtlichen Auslegung des § 61 PStG Anfragen von Wissenschaftlern, Ahnenforschern oder Medienvertretern, die sich bei mir darüber beklagen, von den Standesämtern keine Auskünfte zu erhalten, obwohl die Person, nach der sie sich dort erkundigten, längst verstorben ist. Durch die Weigerung der Standesämter, ihnen Auskunft zu erteilen, seien sie nicht in der Lage, ihre Forschungsaktivitäten fortzusetzen bzw. abschließend durchzuführen. Die Standesämter begründen ihre Entscheidung zumeist damit, daß die restriktive Rechtssituation nichts anderes zuließe. Auskünfte dürften an Personen, die nicht Ehegatten, Vorfahren oder Abkömmlinge sind, nur erteilt werden, wenn hierfür ein rechtliches Interesse bestehe. Auch berechtigte Interessen hinsichtlich bedeutsamer Informationen über Personen, die während der Zeit des Dritten Reichs lebten, wurden auf diesem Wege z. B. nicht erfüllt.

Aus meiner Sicht erscheinen hier andere Lösungsmöglichkeiten denkbar, die den Datenschutzanliegen der Betroffenen entsprechen, die aber durch entsprechende gesetzgeberische Veränderungen festgelegt werden müßten. Der vom Bundesminister des Innern im März 1996 vorgelegte Vorentwurf zur Änderung des Personenstandsgesetzes hatte in diesem Punkte bereits einige bedeutsame Verbesserungen enthalten, die bei der Verabschiedung der bisherigen Gesetzesänderungen jedoch keine Berücksichtigung fanden. Der Bundesgesetzgeber ist aufgefordert, auch den § 61 PStG neu zu regeln.

6.6. Ausländische Bürger und Gäste

6.6.1. Kommt die Chipkarte für Asylbewerber?

Bereits 1995 (vgl. 17. JB, Ziff. 9.24.) habe ich über die Vorstellungen einer Bund-Länder-Arbeitsgruppe beim Bundesministerium des Innern zum Einsatz einer Chip-Karte im Asylverfahren berichtet. Diese Arbeitsgruppe kam zu dem Ergebnis, daß die Überlegungen für eine Asyl-Card in einer Machbarkeitsstudie untersucht werden sollten. Mit der Durchführung der Studie wurde eine

private Firma beauftragt, die Studie wurde im Juni 1998 dem Bundesministerium des Innern vorgelegt. Mir wurde diese Studie erst im März 1999 zugänglich gemacht.

Obwohl die Verfasser der Studie eine Reihe von Datenschutz- und Datensicherungskriterien der Datenschutzbeauftragten aufgegriffen haben, sind bei der Mehrheit der Datenschutzbeauftragten grundsätzliche Datenschutzbedenken gegen die Asyl-Card geblieben. An dieser Stelle will ich einige Kritikpunkte zusammenfassen:

- Auf der Chipkarte können eine Vielzahl von Daten gespeichert werden. Da mehrere Stellen, wie z. B. Ausländerbehörde, Bundesamt für die Anerkennung ausländischer Flüchtlinge, Sozialbehörde und Arbeitsämter, Daten auf der Asyl-Card speichern und ändern können, ist fraglich, wer für die Richtigkeit und die Gewährleistung der Datenschutzrechte des Betroffenen verantwortlich ist.
- Da der Zugriffsschutz auf die in der Asyl-Card zur Speicherung vorgesehenen Daten aufgrund des breiten Nutzerkreises erwartungsgemäß als sehr niedrig bewertet werden kann, ist das unberechtigte Auslesen durch Dritte, auch private Dritte, nicht hinreichend sicher ausgeschlossen. Gerade angesichts der in der Karte gespeicherten sensiblen Sozialdaten ist ein höheres Schutzniveau anzustreben.
- Es ist nicht auszuschließen, daß der Betroffene nicht mehr konkret nach den Angaben gefragt wird, die im Einzelfall erforderlich sind. Vielmehr wird ihm die Karte abverlangt und Einblick in alle auf ihr gespeicherten Daten genommen.
- Ist die Karte erst einmal im Gebrauch, ist auch nicht auszuschließen, daß Private vor Abwicklung von Geschäften die Herausgabe der Karte verlangen, um Einsicht in die auf ihr gespeicherten Daten zu nehmen. Dies ist insbesondere deshalb nicht ausgeschlossen, weil dem Betroffenen auch das für seine Karte gültige Paßwort mitgeteilt wird.

Das in der Studie vorgesehene Systemdesign birgt gewisse Sicherheitsrisiken. Trotzdem kommt die Studie zu dem Ergebnis, daß die Einführung einer Asyl-Card technisch machbar ist. Da die Einführung der Asyl-Card auf der Basis des derzeit gültigen Asyl- und Ausländerrechts nicht möglich ist, haben die Innenminister am 18./19. November 1999 beschlossen, einen Probelauf auf der Grundlage einer freiwilligen Beteiligung der Betroffenen zu prüfen. Ergebnisse hierzu liegen mir für Bremen bisher nicht vor. Einem solchen Versuchslauf haben die Datenschutzbeauftragten des Bundes und vieler Länder widersprochen, weil eine Zustimmung eines Betroffenen nur dann wirksam erteilt ist, wenn er hinreichend über die Datenverarbeitung und die Nutzung der Daten aufgeklärt worden ist. Dies ist naturgemäß bei Asylbewerbern wegen der Sprachprobleme und der Herkunft aus einem anderen Rechts- und Kulturkreis schwierig.

Angesichts der Tatsache, daß in den Jahren 1992 bis 1994 eine ausführliche Debatte über das Asylverfahren geführt wurde, die zu grundlegenden rechtlichen und technischen Änderungen geführt hat, ist zu prüfen, ob mit der Einführung einer Asyl-Card überhaupt der richtige Weg beschritten würde. Es ist festzuhalten, daß aufgrund der geltenden rechtlichen Bestimmungen bereits jetzt die Abnahme von Fingerabdrücken obligatorisch ist. Dieses erkennungsdienstliche Material wird per Computer verformelt und in das zentrale Fingerabdrucknachweissystem AFIS beim Bundeskriminalamt eingestellt, wo diese Daten jederzeit abrufbar sind. Mit diesen Daten kann also

jederzeit eine eindeutige Identitätsüberprüfung durchgeführt werden. Die technische Entwicklung auf dem Gebiet der Datenverarbeitung ist so rasant, daß man es sich heutzutage nicht mehr leisten kann, an einem Projekt über Jahre festzuhalten, ohne parallel nach Alternativen zu suchen, die auch andere moderne technische Entwicklungen berücksichtigen.

6.6.2. Stand des elektronischen Einbürgerungsverfahrens

Der Senator für Inneres hat 1998 ein elektronisches Einbürgerungsverfahren eingeführt. Ich habe mir das technische Verfahren angesehen und erläutern lassen. Es gibt bisher keine Verfahrensbeschreibung und keine Festlegungen über die Nutzung dieses Verfahrens. Zu dem Verfahren liegt - trotz Zusage im Frühjahr 1999 - noch immer kein Datenschutzkonzept vor. Es bedarf aber z. B. eindeutiger Festlegungen, welche Daten wie lange aufbewahrt werden und wann sie gelöscht bzw. zu sperren sind.

Der Senator für Inneres, Kultur und Sport erklärte dazu, die aktuelle Novelle zum Staatsangehörigkeitsrecht habe zu einer Vielzahl von Neuanträgen auf Einbürgerung geführt. Dadurch seien die Arbeiten an dem Datenschutzkonzept zurückgeworfen worden. Gerade die Vielzahl von neuen Einbürgerungsverfahren, die vorhersehbar waren, hätten aus meiner Sicht ein fertiges Konzept erfordert. Es dürfte bekannt sein, daß nach § 8 BrDSG (Dateibeschreibung und Geräteverzeichnis) die speichernden Stellen verpflichtet sind, in einer Beschreibung gewisse datenschutzrechtliche Standards festzuhalten. In einer innumerativen Aufzählung gibt § 8 BrDSG den speichernden Stellen auf, was sie zu erledigen haben. Bei einer ordnungsgemäßen Einführung eines DV-Verfahrens dürften die von § 8 BrDSG abverlangten Informationen quasi als "Abfallprodukt" anfallen, denn über die meisten Fragen muß sich die speichernde Stelle ohnehin vor Inbetriebnahme eines Verfahrens Klarheit verschaffen. Im Januar 2000 habe ich erneut an die Erstellung eines Datenschutzkonzeptes erinnert.

6.6.3. Neues DV-Verfahren bei der Ausländerbehörde Bremen ohne Datenschutzkonzept

In der Ausländerbehörde Bremen wurde im letzten Jahr ein vernetztes DV-Verfahren „Ausländer“ installiert, welches zunächst nur auf die Daten im Ausländerzentralregister zugreifen sollte und sonst als Formularserver und Schreibsystem eingesetzt werden sollte. Dazu hat mir das Stadtamt bisher trotz Erinnerung kein Einsatz- und Datenschutzkonzept vorgelegt. Im übrigen gelten meine Ausführungen zu § 8 BrDSG im vorgehenden Abschnitt (Elektronisches Einbürgerungsverfahren).

Kurz vor Redaktionsschluß habe ich darüber hinaus erfahren, daß ein umfassendes Datenverarbeitungsverfahren ausgewählt wurde, daß die Ausländerverwaltung umfassend unterstützen soll, ohne daß ich hierüber vorher unterrichtet worden bin. Sollte diese Information zutreffen, würde dies einen Verstoß gegen § 27 Abs. 4 BrDSG darstellen, danach bin ich rechtzeitig über Planungen zum Aufbau automatisierter Informationssysteme, die personenbezogene Daten verarbeiten sollen, zu unterrichten.

7. Justiz

7.1. DV-Entwicklung bei JUDIT

Im Berichtszeitraum habe ich mich bei JUDIT über die geplanten Änderungen im DV-Bereich informiert. So werden durch die Einrichtung eines "JUDIT-Synergiezentrums" und die fehlende Y2K-Fähigkeit (Jahr-2000-Fähigkeit) einiger bisher bei der ID Bremen eingesetzter DV-Verfahren Änderungen in den Bereichen Vernetzung sowie Hardware- und Software-Einsatz erforderlich. Im Synergiezentrum werden die Server der bremischen Justizanwendungen weitgehend zusammengefaßt und die Bereiche Administration und Datensicherung zentralisiert sowie das JUDIT-Datennetz betrieben.

Für das "JUDIT-Synergiezentrum" wurde mir der Grobentwurf eines Datenschutzkonzeptes vorgelegt, in dem u.a. die Regelungen für die Anbindung externer Stellen (z. B. Bundeszentralregister, Verkehrszentralregister, ID Bremen, DVZ Bremerhaven, zentrales staatsanwaltschaftliches Verfahrensregister, E-Mail) noch fehlen. In diesem Konzept ist auch der Zugriff der Fachverfahrensbetreuer auf die PC der Mitarbeiter und -innen vorgesehen. Hierzu habe ich nähere Informationen angefordert, die ich wie weitere Unterlagen zum Grobkonzept noch nicht erhalten habe.

7.2. JUDIT-Datennetz

Das Rechenzentrum ist im OLG/StA-Gebäude untergebracht. Über das vom Synergiezentrum betriebene JUDIT-Datennetz sollen die Justizstandorte Bremen und Bremerhaven miteinander verbunden werden, wobei einige der Dienststellen in Bremen und Bremerhaven sowohl miteinander als auch mit dem Synergiezentrum in einem LAN (Local Area Network) verbunden sind. Die Inhouse-Datennetze und LAN-Strecken werden von JUDIT erstellt und betreut. Außerhalb gelegene Behörden oder Gebäudekomplexe (zusammenhängende oder benachbarte Gebäude werden über LWL-Leitungen verknüpft) werden über eine WAN-Strecke (World Area Network) an das Synergiezentrum angebunden. Für die WAN-Verbindungen wird das BreKom-Netz genutzt. Deshalb ist die BreKom mit dem Betrieb und dem Netzwerkmanagement beauftragt. Die eingesetzten Übertragungsverfahren codieren die Daten auf den WAN-Strecken. Sobald geeignete technische Lösungen zur verschlüsselten Datenübertragung vorliegen, sollen diese eingesetzt werden.

7.3. Elektronisches Grundbuch

Im vorletzten Jahresbericht (vgl. 20. JB, Ziff. 13.3) habe ich über die Einführung des elektronischen Grundbuches berichtet. Im Berichtszeitraum wurden die für die Software-Anwendung erforderlichen Voraussetzungen geschaffen. Jetzt sind LAN- und WAN-Vernetzung sowie die Beschaffung der Hardwarekomponenten abgeschlossen.

Für die Erfassung der vorhandenen Grundbuchdaten wurde in Bremen eine Scan-Strecke eingerichtet, in der alle Grundbuchdaten zentral eingescannt (elektronisch erfaßt) werden. Die Speicherung erfolgt zentral auf FM-Worm-Platten in nicht codierter Form (NCI-Format). Neueingaben oder Änderungen werden in codierter Form (CI-Format) gespeichert. Eine Trennung der Datenbestände auf den Datenträgern nach Gerichten ist bei Neuanlagen möglich. Eine differenzierte Rechtevergabe entsprechend der Aufgabenzuständigkeit innerhalb einer Grundbuchabteilung sieht die Software nicht vor. Jeder Berechtigte der Grundbuchabteilung hat Lese- und Schreibzugriff auf alle Daten der Grundbuchabteilung. Der online-Zugriff für Externe (z.B. Notare) ist noch nicht realisiert. Es

wird geprüft, die ID Bremen mit der Realisierung zu beauftragen. Vorgesehen ist hierbei die Protokollierung aller Abrufe für eine detaillierte Rechnungstellung.

Ich habe darauf hingewiesen, daß u.a. folgende Punkte in das noch zu erstellende Datenschutzkonzept aufzunehmen sind: Protokollierung interner Lese- und Schreibzugriffe, Zugriff, Auswertung und Löschung auf die Protokolldateien, Regelungen zur digitalen Signatur (personalisierter Schlüssel oder Schlüssel des Prozesses) und Löschung bzw. Sperrung von Datensätzen auf den FM-WORM-Datenträgern bei unzulässiger Speicherung.

7.4. DV-Entwicklung in der Justizvollzugsanstalt

In der ersten Stufe werden alle vorhandenen Kupferleitungen durch LWL ersetzt und in der zweiten Stufe (im Jahr 2000) sollen alle Büroarbeitsräume mittels LWL vernetzt werden. Der Netzzugang wird bei Aufgabenerforderlichkeit freigeschaltet. Im "JUDIT-Synergiezentrum" werden die Datenbestände der Justizvollzugsanstalten auf einem Server vorgehalten. Die Netzzentrale der JVA mit Anbindung an den Server und das JUDIT-Datennetz befinden sich auf dem Gelände der JVA Oslebshausen. Die zentralen Netzkomponenten sind für Gefangene nicht zugänglich.

Die Daten waren bisher auf zwei UNIX-Anlagen getrennt gespeichert, wobei die Datenbestände der Justizvollzugsanstalten Oslebshausen und Blockland auf einer Anlage und die Datenhaltung der JVA Bremerhaven in einer UNIX-Anlage in der Justizvollzugsanstalt Bremerhaven erfolgte. Die UNIX-Anlagen werden ab 01.01.2000 nicht mehr eingesetzt, da sie durch die Herstellerfirma nicht mehr gewartet werden. Angeschlossen an die UNIX-Anlagen waren i.d.R. Terminals. Die Serveranbindung erfolgt nun durch PC, auf denen das Betriebssystem WNT und Office 97 (Tabellenkalkulation und Datenbank nur bei Bedarf) implementiert werden. Die Diskettenlaufwerke der PC sollen gesperrt werden; für den Zugriff auf die CD-ROM-Laufwerke soll nur Leserecht erteilt werden.

Bis zum 31.12.1999 waren die Verfahren ‚JUWIL' (ADV unterstützte Beschaffung und Lagerhaltung der Bewirtschaftungsgüter) und ‚Entgelt' (Lohnabrechnung der Insassen) bei der ID Bremen im Einsatz. Da diese Verfahren nicht Y2K-fähig sind und die neuen Verfahren auf Servern der JUDIT implementiert sind, ist die Verbindung zur ID Bremen zum 31.12.1999 beendet worden. Ab 01.12.1999 werden die Verfahren 'BASIS-VG', 'BASIS-AV' (Arbeitsverwaltung Entgelte) und BASIS-Zalo (Verwaltung der Gelder der Gefangenen) eingesetzt.

Die PC des ärztlichen Dienstes sollen ein eigenes Netz bilden und vom übrigen Netz abgeschottet werden. Ihm soll lediglich ein Zugriff auf die Stammdaten der Gefangenen ermöglicht werden. Zugriff auf die medizinischen Daten sollen nur der Arzt und die befugten Mitarbeiterinnen des ärztlichen Dienstes erhalten. Die Vollzugsbediensteten im übrigen haben keinen Zugriff. Das in BASIS vorhandene Modul ‚BASIS-Ärzte' soll für die elektronische Gefangenenkrankenakte zum Einsatz kommen.

Ich habe die Speicherung des Gesamtdatenbestandes auf einem Server, die Anbindung von PC sowie die Einbindung des Netzes des ärztlichen Dienstes gegenüber JUDIT angesprochen und auf die Festschreibung von Maßnahmen zur Gewährleistung des bisherigen Datenschutzniveaus hingewiesen. Das bisherige Datenschutzkonzept wird im Laufe des Jahres angepaßt und ein

Berechtigungskonzept für die Vergabe von Zugriffsberechtigungen erstellt. Ich werde die Umsetzung der Planungen datenschutzrechtlich begleiten.

7.5. E-Mail-Server bei JUDIT

Im November 1999 bin ich von JUDIT kurzfristig über Planungen zur kompletten Anbindung der Justiz-Dienststellen an das BVN unterrichtet wurden. Vorgesehen war die Beschaffung von 13 E-Mail-Servern, wobei ein sog. Head-Server die Routing-Funktion innerhalb von JUDIT wahrnehmen soll. Die Anbindung der E-Mail-Server an das BVN soll über einen zentralen Router erfolgen, um einen dienststellenübergreifenden Zugriff zu verhindern.

JUDIT war sich bewußt, daß nicht alle in Kurzform aufgeführten Punkte den vorgeschriebenen Richtlinien eines Datenschutzkonzeptes entsprechen, beantragte aber dennoch bei der SKP die Aufnahme der Behörden im Geschäftsbereich des Senators für Justiz und Verfassung in den E-Mail-Verbund. Die SKP wies JUDIT darauf hin, daß vor Inbetriebnahme der E-mail-Server erst ein mit dem LfD abgestimmtes Datenschutz- und –sicherungskonzept vorliegen müsse.

Mir war eine Stellungnahme binnen weniger Tage zu einem solch komplexen Bereich nicht möglich (vgl. auch Ziff. 3.4). Ich wollte aber der Beschaffung, die aus haushaltsrechtlichen Gründen unbedingt noch in 1999 erfolgen sollte, nicht im Wege stehen. Inwieweit eine auch von § 27 Abs. 4 Nr. 1 BrDSG verlangte rechtzeitige Unterrichtung über die Planungen möglich gewesen wäre, vermag ich nicht zu beurteilen. Bei meiner Entscheidung, die Beschaffung nicht zu verzögern, stand im Vordergrund, daß ich davon ausging, daß es gelingen wird, den Einsatz der E-Mail-Server datenschutzgerecht auszugestalten. Ich habe daher auf die Erstellung eines Datenschutzkonzeptes hingewiesen.

7.6. Zentrales Staatsanwaltschaftliches Verfahrensregister (ZStV)

Durch Änderung der Strafprozeßordnung (StPO) im Jahre 1997 wurden die Voraussetzungen zur Schaffung eines zentralen staatsanwaltschaftlichen Informationssystems geschaffen. Die Staatsanwaltschaften aller Länder sollen Daten über Einleitung und Ausgang strafrechtlicher Ermittlungsverfahren an das Zentrale Staatsanwaltschaftliche Verfahrensregister (ZStV) melden. Das ZStV wird – wie auch das Bundeszentralregister – von der Bundesgeneralstaatsanwaltschaft in Berlin geführt. Eine umfassendere Darstellung der Aufgaben und der Datenverarbeitung beim ZStV sowie der daran zu knüpfenden Datenschutzvorkehrung befindet sich in meinem 17. JB, Ziff. 10.2. Ein Bericht des ZStV zum Stand der Verfahrensentwicklung und Verfahrenseinführung vom März 1999 weist begrüßenswerterweise aus, daß die datenschutzrechtliche Forderung nach Verschlüsselung des Datenverkehrs mit dem ZStV grundsätzlich akzeptiert wird. Da allerdings die erforderlichen Hard- und Softwarekomponenten noch nicht vorliegen, soll der Echtbetrieb für eine Übergangszeit zunächst ohne Verschlüsselung stattfinden. Weiter diskutiert werden soll, in welchem Umfang neben den Staatsanwaltschaften auch andere Behörden, wie Polizei und Nachrichtendienste, mittels automatisierten Abrufverfahren Informationen aus dem ZStV abfragen können. Wann das ZStV in vollem Umfange betriebsbereit sein wird, ist noch nicht abzusehen.

7.7. Verschiedene Themen

Weiter habe ich mich gegenüber den Datenschutzbeauftragten des Bundes und der Länder oder dem Senator für Justiz und Verfassung an der Diskussion folgender Themen beteiligt:

- Datenschutzrechtliche Probleme bei der Durchführung des Täter-Opfer-Ausgleichs bei Erwachsenen
- Gesetzgebung zur Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften (vgl. Beschluß unter Ziff. 18.8.)
- Umfang von Auskunftsersuchen durch Staatsanwaltschaften und Gerichte bei der Schufa, hier werden häufig alle bei der Schufa gespeicherten Daten abverlangt, obwohl es lediglich um eine einzelne Information geht. Oder aber die Schufa ist gar nicht in der Lage, die in Rede stehende Anfrage zu beantworten, gleichwohl werden oft sämtliche Daten der zur Person gespeicherten Daten bei der Schufa abverlangt.

7.8. Zum Auskunftsanspruch des Grundstücksmaklers

Vom Niedersächsischen Landesbeauftragten für den Datenschutz wurde mir eine Bürgerbeschwerde zur weiteren Bearbeitung übersandt. Ein Ehepaar hatte im Bremer Randgebiet ein Hausgrundstück erworben. Ein Bremer Immobilienmakler behauptete Ansprüche gegen dieses Ehepaar aus diesem Hauskauf. Das Ehepaar war nicht auskunftsbereit. Der Makler beauftragte daraufhin einen in Bremen ansäßigen Notar und Rechtsanwalt mit der Informationsbeschaffung über den Grundstückskauf. Dieser besorgte als Notar Grundbuchauszug und Grundakte, inwieweit er selbst oder durch einen Korrespondenzanwalt dann diese Daten zur Vorbereitung einer Klage verwertete, blieb unklar. Im Zuge meiner Prüfung bin ich zu dem Ergebnis gekommen, daß er als Notar diese Auskünfte nicht verlangen durfte. Die ebenfalls mit der Frage konfrontierte Hanseatische Rechtsanwaltskammer hatte auch Bedenken an der Rechtmäßigkeit des Auskunftsersuchens des Notars; der Notar hat einen objektiven Fehler zugestanden und ein Büroversehen dafür verantwortlich gemacht. Im Ergebnis ist festzuhalten, daß in einem solchen Fall einem Makler und damit auch seinem Rechtsanwalt Auskunft aus Grundbuch und Grundakte darüber zu geben ist, ob einer seiner Klienten das Grundstück erworben hat; darüber hinaus auch über die Höhe des Kaufpreises, wenn es darum geht, sich über die Entstehung und Höhe eines Provisionsanspruchs zu vergewissern.

7.9. DNA-Analyse von Körperzellen nur mit richterlicher Anordnung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat aufgrund der Entwicklung in einigen Ländern darauf hingewiesen, daß eine Untersuchung von DNA-Material zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren nach den Vorschriften der StPO nur auf Anordnung des Richters erfolgen darf (vgl. Ziff. 18.12.). Dies habe ich auch dem Senator für Justiz und Verfassung mitgeteilt. Ich konnte feststellen, daß kein Dissens besteht, denn der Senator für Justiz und Verfassung erklärte dazu in einem Schreiben, daß in seinem Geschäftsbereich die Auffassung vertreten werde, daß die molekulargenetische Untersuchung von Körperzellen für Zwecke der Identitätsfeststellung in künftigen Strafverfahren ausschließlich auf der Grundlage einer richterlichen Anordnung nach § 81g Abs. 3 i. V. m. § 81f StPO bzw. § 2 Abs. 2 DNA-IFG i. V. m. § 81f StPO erfolgen dürfe. Die Gegenmeinung, wonach die fehlende richterliche Anordnung durch die Einwilligung des Betroffenen kompensiert werden könne, vermöge nicht zu überzeugen. Der

Generalstaatsanwalt Bremen teile seine Auffassung. Mit dem Leitenden Oberstaatsanwalt Bremen sei abgesprochen, daß auch bei Vorliegen einer Einverständniserklärung des Betroffenen ein richterlicher Beschluß erwirkt werden solle. Es bleibt abzuwarten, wie die Rechtsprechung zum Richtervorbehalt des § 81f StPO sich entwickeln wird.

8. Gesundheit und Krankenversicherung

8.1. Bremer Krebsregister

In meinem 20 JB. unter Ziff. 14.1. und in meinem 21. JB. unter Ziff.11.1. hatte ich über die Besonderheiten des im Oktober 1997 in Kraft getretenen Bremischen Krebsregistergesetzes und über die Probleme bei der Einrichtung des Registers berichtet. Der nachfolgend geschilderte Sachverhalt ist bereits im Datenschutzausschuß behandelt worden (vgl. Ziff. 4.1.).

Zwei Besonderheiten haben mich dazu veranlaßt, sowohl die Vorbereitung des Gesetzes als auch die Installation des Registers mit besonderer Aufmerksamkeit zu begleiten:

- Die Vertrauensstelle, die die Meldungen der Ärzte und Kliniken entgegennimmt, übermittelt zwar unverzüglich den medizinischen Datensatz an die Registerstelle, speichert aber die Identitätsdaten auf Dauer zwecks Ausschluß von Doppelmeldungen zur Reidentifizierung der gemeldeten Patienten für wissenschaftliche Untersuchungen und für Auskünfte an Betroffene. Als Risikoausgleich gibt das bremische Gesetz der Vertrauensstelle vor, sicherzustellen, daß sie die bei ihr gespeicherten Identitätsdaten von Krebspatienten nicht zu anderen als zu den gesetzlich definierten Zwecken nutzen kann und daß diese Daten nicht unbefugt eingesehen und genutzt werden können, § 4 Abs.1 Satz 2 i.V.m. § 6 Abs.2 BremKRG.
- Zweck der Aufteilung des Registers in Vertrauens- und Registerstelle ist es, die Identifizierung der einzelnen Krebspatienten anhand der über sie gespeicherten medizinischen Daten zu verhindern. Dies - so ausdrücklich das Gesetz - ist durch einen dem Stand der Technik angemessenen Schutz zu gewährleisten. Das Gesetz sieht kleinräumige Untersuchungen zu Krebsrisiken vor. Dazu sind neben den medizinischen Daten auch Daten, die zum Wohnsitz des gemeldeten Patienten gehören, erforderlich. Deshalb zählen diese Angaben zu der Kategorie von Daten, die an die Registerstelle übermittelt werden sollen. Im Ausgleich hierzu wiederum verlangt das Gesetz in seinem § 6 Abs. 1 Nr. 4 BremKRG ausdrücklich, es dürfe nicht möglich sein, anhand dieser Angaben die Anschrift und damit die Identität der Betroffenen festzustellen.

Ich habe bei Vertrauens- und Registerstelle vor Ort Datenschutzprüfungen durchgeführt. Ziel meiner von technischen Prüfungen begleiteten Erörterungen war die Durchsetzung der oben genannten zentralen gesetzlichen Vorgaben, und zwar sowohl in den Festlegungen der Datenschutzkonzepte beider Stellen als auch bei der technischen Installation der EDV-Systeme.

8.1.1. EDV-Sicherheitsstruktur in der Vertrauensstelle des Bremer Krebsregisters

Nach § 6 Abs.2 BremKRG hat die Vertrauensstelle sicherzustellen, daß sie die durch sie gespeicherten Identitätsdaten nur zu den in § 4 Abs.1 BremKRG aufgeführten Zwecken nutzen kann. Die Vertrauensstelle definierte hierfür in einem Datenschutzkonzept (Erster Entwurf: Mai 1998, mit mir abgestimmte Fassung: Dezember 1998) umfassende technische Vorkehrungen. Über deren Zielsetzung und Art bestand grundsätzlich Einigkeit, Probleme warf aber die Durchführung auf. So waren bei einer Prüfung im September 1999 einige Systemeinstellungen auf den Ebenen der Hardware, des Betriebssystems und der Protokollierung noch nicht umgesetzt. Bei der Nachprüfung im Dezember 1999 konnte ich aber feststellen, daß die Einstellungen geändert waren und mit dem Datenschutzkonzept übereinstimmten. Wesentliche Punkte waren:

- Hardware: Abschaltung serieller Schnittstellen über das BIOS
- Betriebssystem: Mitarbeiterinnen der Vertrauensstelle können auf MS-Office, auf ein gemeinsames Netzverzeichnis und auf Home-directories zugreifen. Die Registratur ist mit Hilfe von Berechtigungen so geschützt, daß nur der Administrator im Zusammenwirken mit einer Nutzerin die Konfigurationsdateien ändern kann. Über eine Domäne ist eine zentrale Sicherheitsstruktur realisiert.
- Protokollierung: Transaktionen des Datenexports und ausgehender Datenträger werden im gebotenen Umfang automatisch protokolliert, ebenso der Aufruf des Registerprogramms TRUST-KR. Mitarbeiterinnen können das Protokoll nur lesen, nicht ändern.

8.1.2. EDV-Sicherheitsstruktur in der Registerstelle des Bremer Krebsregisters

Die Vertrauensstelle übermittelt der Registerstelle die medizinischen Daten der ihr gemeldeten Patienten zusammen mit den von ihr jeweils vergebenen Registernummern, dies aber ohne Nennung von Namen, Geburtsdaten und Anschriften. Der Registerstelle darf die Deanonymisierung, d.h. die Verknüpfung der medizinischen Daten mit den betroffenen Patienten, nicht möglich sein, so ausdrücklich §6 Abs. 1 Nr. 4 BremKRG. Ihr wäre dies aber möglich, könnte sie zu den gesetzlichen Registerdaten und zu den gesetzlich vorgesehenen Auswertungen weitere Daten als Zusatzinformationen und/oder Zusatzprogramme in ihr EDV-System einspielen. Im Verlauf eines vom Juni 1998 bis zum November 1999 dauernden Erörterungsprozesses gelang es, mit der Registerstelle über diese Zielsetzung und die zu deren Realisierung gebotenen und in ihrer Wechselwirkung geeigneten Vorkehrungen Einvernehmen zu erzielen:

- Hardware: Deaktivierung der seriellen Schnittstellen, Sperrung externer Laufwerke (CD-ROM, Diskette).
- Betriebssystem: Anwendung der Administratorkennung, die vollen Zugriff auf das Betriebssystem ermöglicht, nur gemeinsam mit Anwendern (geteiltes Passwort).
- Datenbank/Rechtestruktur: Individueller Zugang zu den Registerdaten mit eingeschränkten Rechten, Trennung von Administrations- und Nutzungsebene, Installation einer entsprechend leistungsfähigen Datenbank.
- Protokollierung der Logins und aufgerufener Programme über die Ebene des Betriebssystems, Protokollierung auf Datenbankebene, Protokollierung von Datenexporten per Diskette durch ein manuelles Verfahren.
- Physikalische Löschung von Daten, falls wie etwa auf nachträglichen Widerspruch hin deren Löschung geboten ist.

Die im September 1999 anläßlich eines Prüfbesuchs in der Registerstelle festgestellten Defizite bei der Protokollierung, der Transparenz der Systemadministration und der physikalischen Löschung waren bei einer Nachprüfung im Dezember 1999 behoben. Lediglich die Datenbankprotokollierung war noch nicht realisiert. Dies soll bis Ende Januar 2000 nachgeholt werden. Ich habe die Registerstelle gebeten, mir bis Mitte Februar 2000 eine Fassung ihres Datenschutzkonzepts

vorzulegen, in der die miteinander abgestimmten Sicherungsvorkehrungen vollständig dokumentiert werden.

Die Vertrauensstelle übermittelt die für kleinräumige Untersuchungen erheblichen Wohnsitzdaten bislang noch nicht an die Registerstelle, da die technischen Einzelheiten noch nicht geklärt sind. Es besteht aber Übereinstimmung mit der Vertrauensstelle, daß diese Daten zwar ausreichend differenziert sein müssen. Sie dürfen aber der Registerstelle nicht die Identifizierung einzelner Betroffener ermöglichen. Dies wird es erforderlich machen, daß die Vertrauensstelle ein Verfahren zur Codierung, in diesem Zusammenhang "Verschmutzung" genannt, einsetzt.

Die in meinem 21. JB unter Ziff. 11.1.2 dargestellte Diskussion darüber, ob Vertrauens- oder Registerstelle im Falle sich inhaltlich widersprechender Meldungen zu einem Patienten zwecks Klärung mit den Meldern Verbindung aufnehmen sollen, ist inzwischen datenschutzgerecht abgeschlossen worden: Es kann nicht Aufgabe der Registerstelle sein, da ihr die Identität der betroffenen Patienten nicht bekannt ist und auch nicht bekannt werden darf. Man ist sich einig, daß es sich um eine Aufgabe der Vertrauensstelle handelt.

Die Vertrauensstelle hat die medizinischen Daten der gemeldeten Patienten nach der Übermittlung an die Registerstelle umgehend, spätestens aber vor Ablauf von drei Monaten, in ihren Dateien zu löschen. Andernfalls würde die Aufteilung des Registers in Vertrauens- und Registerstelle unterlaufen. Dies wurde in der Anlaufzeit des Registers nicht ausreichend beachtet, da die Registerstelle Schwierigkeiten mit dem Einlesen der ihr übermittelten Datensätze in ihr EDV-System hatte. Auf meine Intervention hin erklärte die Vertrauensstelle, sie werde künftig die gesetzliche Vorgabe beachten. Ich konnte mich davon bei einer Prüfung mittels einer Stichprobe überzeugen.

Der erreichte Stand wurde bereits im Datenschutzaussschuß behandelt. Dabei erklärte das Gesundheitsressort auch, daß es intensiv darauf hinwirken werde, daß nur das vorgesehene Formular für die Meldung zum Register von Ärzten und Kliniken verwendet werde und nicht Arztbriefe und Entlassungsberichte übermittelt würden, die weit mehr Daten enthalten, als für die Meldung erforderlich.

Darüber hinaus steht nach Informationen aus dem Gesundheitsressort eine umfassende Überarbeitung des Bremischen Krebsregistergesetzes an. Anlaß ist das Auslaufen des Krebsregistergesetzes des Bundes zum 31.12.99, berücksichtigt werden sollen die im Verlauf der Einrichtung des Bremischen Krebsregisters gesammelten Erfahrungen. Mit dem Datenschutzausschuß der Bremischen Bürgerschaft bin ich darin einig, daß der im geltenden Recht festgeschriebene und inzwischen auch technisch und organisatorisch umgesetzte Datenschutzstandard erhalten bleiben muß.

8.2. Bremer Brustkrebs-Screening-Programm

Im September 1999 erhielt die Stadtgemeinde Bremen auf ein bundesweites Ausschreibungsverfahren hin, das unter Regie des Bundesausschusses für Ärzte und Krankenkassen steht, den Zuschlag für ein Modellprojekt zur Früherkennung von Brustkrebs. Alle Bremerinnen im Alter von 50 bis 70 Jahren sollen eingeladen werden, sich in einem eigens hierfür gegründeten „Mamma-Zentrum“ einer Untersuchung mittels eines in dem unversitätsnahen Institut MeVis

entwickelten digitalen Verfahrens zu unterziehen. Zwecks wissenschaftlicher Auswertung des Projekts wird eine Beteiligungsquote von mindestens 70% angestrebt. Auch sollten im Rahmen des Projekts Datenabgleiche mit dem Bremer Krebsregister stattfinden.

Dieses Projekt setzt die Verarbeitung der Identitätsdaten von 70.000 Bremerinnen voraus und strebt die Verarbeitung medizinischer Daten von mindestens 50.000 Bremerinnen an und dies in einem gänzlich neu aufzubauenden organisatorischen Zusammenhang, ein anspruchsvolles Unterfangen. Deshalb wandte ich mich bereits Ende 1998, als ich von dem Projekt erfahren hatte, dann wieder, veranlasst durch die Presseberichterstattung, im September 1999 an die beteiligten Stellen, d.h. an den Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales, an MeVis, an die kassenärztliche Vereinigung, an das Zentralkrankenhaus St.-Jürgen-Straße und an das Bremer Institut für Präventionsforschung und Sozialmedizin (BIPS). Ich machte auf die datenschutzrechtlichen Anforderungen aufmerksam und bat darum, das Datenschutzkonzept rechtzeitig zu erarbeiten und mit mir abzustimmen, damit vor Anlaufen des Projekts die gebotenen technischen Sicherungsvorkehrungen getroffen werden können. Dabei ließ ich mich durch die im Zusammenhang mit der Einrichtung des Bremer Krebsregisters gemachten Erfahrungen leiten, daß Konzeption und Installation einer auf die Spezifika eines derartigen neuen Projekts ausgerichteten Hard- und Software Zeit kostet.

Im Zusammenhang mit dem Projekt stehen auch folgende Anforderungen:

- Bei der Beschaffung der Adressdaten der anzusprechenden Bremerinnen durch Registerauskunft der Meldestellen ist das Bremische Meldegesetz zu beachten.
- Die in das Projekt einbezogenen Frauen sind um eine schriftliche Einwilligung in die Verarbeitung ihrer Daten zu bitten. Zuvor sind sie auf die Zwecke der Speicherung und vorgesehene Übermittlungen ihrer Daten sowie darauf hinzuweisen, daß ihre Beteiligung freiwillig ist.
- Jeder auf die Person der betroffenen Frauen bezogene Abgleich von Daten aus dem Projekt mit Daten aus dem Krebsregister bedarf der Einwilligung der einzelnen betroffenen Frauen.

Bisher hat keine der genannten Stellen mit mir Kontakt aufgenommen, um die anstehenden Datenschutzfragen zu klären. Ich gehe aber davon aus, daß man den Datenschutz schon deshalb ernst nehmen wird, weil man für das Gelingen des Projekts auf das Vertrauen der Bremerinnen angewiesen sein wird.

8.3. Sozialpsychiatrischer Dienst - Datenschutzverordnung

Entsprechend dem Auftrag des § 33 Abs. 3 des Gesetzes über den Öffentlichen Gesundheitsdienst im Lande Bremen, das bereits 1995 in Kraft getreten ist, hat der Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales in Zusammenarbeit mit den Gesundheitsämtern Bremen und Bremerhaven und in Abstimmung mit mir die Verordnung über die Verarbeitung personenbezogener Daten in Behörden und Einrichtungen des Öffentlichen Gesundheitsdienstes (Brem.GBl. 2000, S. 2) in Kraft gesetzt. Damit wird über Umfang und Dauer der Speicherung von Patientendaten im öffentlichen Gesundheitsdienst Rechtssicherheit geschaffen. Insbesondere aber hat die Verordnung Klarheit darüber geschaffen, daß die Sozialpsychiatrischen Dienste bei der Datenverarbeitung dem Rechnung

zu tragen haben, daß ihre Ärzte zum einen Angebote freiwilliger Beratung, Behandlung und Hilfe bereithalten, zum anderen aber auch als Gutachter in Verfahren zur zwangsweisen Unterbringung psychisch Kranker tätig werden. Wie bereits durch das Gesetz vorgezeichnet, sind die im erstgenannten Zusammenhang erhobenen Daten getrennt von den im zweitgenannten Zusammenhang erhobenen Daten zu speichern. Die Daten dürfen nur unter besonderen im Gesetz genannten Umständen zusammengeführt werden. Dadurch werden das Vertrauen der Patienten in die Wahrung der ärztlichen Schweigepflicht der Sozialpsychiatrischen Dienste geschützt und indirekt deren Funktionsfähigkeit gestärkt. Es ist zu erwarten, daß diese nunmehr auf dieser Grundlage die Verarbeitung der Daten ihrer Patienten auf EDV umstellen. Ich werde mich daher in Kürze an die Gesundheitsämter wenden. Ich gehe davon aus, daß ich bei der Erarbeitung von Datenschutzkonzepten beteiligt werde.

8.4. Verkauf der Arztpraxis - Wahrung der Schweigepflicht

Der Bundesgerichtshof (BGH NJW 92, 737) hatte in einer Entscheidung zum Umfang der Schweigepflicht beim Verkauf von Arztpraxen erkannt, daß der abgebende Arzt durch eine Übergabe der ärztlichen Unterlagen ohne vorherige Einwilligung seines Patienten seine Schweigepflicht verletze. Deshalb habe ich mich für eine Einwilligungslösung stark gemacht (vgl. 20. JB, Ziff. 14.3 und 21. JB, Ziff. 11.8). Die Ärzte- und die Zahnärztekammer Bremen beschlossen im Rahmen der Neufassung ihrer Berufsordnungen, die vorsehen, daß der Praxisnachfolger seinerseits die ihm übergebenen Unterlagen unter Verschluß halten und sie nur mit Einwilligung des Patienten einsehen oder weitergeben darf.

Der Senator für Gesundheit hat diese Regelung im Widerspruchsverfahren genehmigt (zur Begründung vgl. die Stellungnahme des Senats zum 21. JB, Bürgerschaft-Drs. 15/75, S. 7). Dies bedauere ich sehr. Somit kann passieren, daß ein behandelnder Arzt, den ein Patient vor wenigen Jahren im Streit verlassen hat, als Praxisnachfolger erneut über Unterlagen zu diesem Patienten verfügt. Auch ist zu befürchten, daß der Patient in vielen Fällen lange Zeit nichts davon erfahren wird, daß seine Unterlagen im Besitz eines ihm unbekannten Arztes sind.

8.5. Wahrung der ärztlichen Schweigepflicht bei Kooperation zwischen Krankenhäusern

Zunehmend kooperieren Krankenhäuser zwecks Kostensenkung und Qualitätsverbesserung miteinander. Dies betrifft Funktionsdienste wie Reinigung, Küche und Technik, aber auch Pflegedienste und Ärzte. Auf diese Weise arbeiten zunehmend Ärzte einer Klinik (Klinik A) auf der Grundlage von Personalüberlassungsverträgen auch in einer anderen Klinik (Klinik B). In einem Fall, über den ich bereits im letzten Jahresbericht (vgl. 21. JB, Ziff. 11.6) berichtete, hatte die Klinik B die aus der Kooperation entstandene Kenntnis über den Patienten ohne sein Wissen genutzt und hatte seine über ihn in der Klinik A archivierte Krankenakte angefordert und in einem durch den Patienten gegen sie geführten Arzthaftpflichtprozeß verwendet. Ich habe den Fall zum Anlaß genommen, darauf hinzuweisen, daß generell darauf zu achten ist, daß die Verantwortung des einzelnen Krankenhauses für die Einhaltung der ärztlichen Schweigepflicht und die Sperrung archivierter Unterlagen ehemaliger Patienten durch Kooperationsverträge nicht aufgehoben wird. Vor diesem Hintergrund ist es zu begrüßen, daß die beiden beteiligten Kliniken aus dem dargestellten Einzelfall die Konsequenz

gezogen haben, ihre Kooperationsvereinbarung zu ergänzen. Sie haben klargestellt, daß die in der Klinik A tätigen Ärzte der Klinik B die Daten der dort von ihnen behandelten Patienten nur zur Erfüllung ihrer Aufgaben in der Klinik A nutzen dürfen. Jede darüber hinausgehende Verarbeitung, insbesondere die Entsperrung und Übermittlung von in der Klinik A archivierten Daten bedürfen der Zustimmung des zuständigen leitenden Arztes der Klinik A und des Einverständnisses des betroffenen Patienten. Ich habe gegenüber dem Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales angeregt, vergleichbare Regelungen auch in andere Kooperationsverträge unter Beteiligung kommunaler Kliniken der Stadtgemeinde Bremen aufzunehmen.

8.6. Recht des Patienten auf Einsicht in seine Krankenunterlagen - Charta der Patientenrechte und Richtlinie für Krankenhäuser der Stadtgemeinde Bremen

Basis für eine ärztliche Heilbehandlung ist das Vertrauen, das der Patient in seinen Arzt setzt. Zum Schutz dieses Vertrauensverhältnisses sichert die Rechtsordnung die ärztliche Schweigepflicht. Die Schweigepflicht gilt aber nicht gegenüber dem behandelten Patienten. Der Patient kann ein Interesse daran haben, Einsicht in die Dokumentation zu nehmen, die der Arzt über seine Behandlung anlegen muß. Die Rechtsprechung, Krankenhausgesetze der Länder (im Lande Bremen das Krankenhausdatenschutzgesetz) und die ärztlichen Berufsordnungen erkennen seit geraumer Zeit übereinstimmend das Einsichtsrecht der Patienten an. Allerdings bleibt bemerkenswert, wie oft noch immer Ärzte sich schwer tun, ihre damit korrespondierenden Pflichten zu erfüllen. Dies gilt wohl nicht so sehr, wenn zur Vorbereitung oder im Rahmen eines gerichtlichen Verfahrens ein Rechtsanwalt mit Vollmacht seines Mandanten Einsicht verlangt. Jedoch stoßen Patienten, die selbst ihre Rechte in Anspruch nehmen wollen, weiterhin häufig auf ärztliches Unverständnis.

Hiermit im Zusammenhang steht folgendes: Auf der Grundlage eines Gutachtens des Instituts für Gesundheits- und Medizinrecht der Universität Bremen und auf Initiative der Gesundheitsminister der Länder in Abstimmung mit den wichtigsten organisierten Beteiligten am Gesundheitswesen ist ein Dokument mit dem Namen „Charta der Patientenrechte“ (Charta I) vorgestellt worden. Leider schließen sowohl diese Charta selbst, die letztlich auf Wunsch der Bundesärztekammer auf einen Gemeinsamen Standpunkt herabgestuft wurde, als auch ein „abgespecktes“ Konkurrenzpapier, das eben diese Bundesärztekammer unter der Bezeichnung „Charta der Patientenrechte“ der Öffentlichkeit vorstellte (Charta II), das Einsichtsrecht des behandelten Patienten in subjektive Aufzeichnungen und Bewertungen des Arztes aus. Immerhin wurde auf Intervention der erst spät zu den Beratungen hinzugezogenen Datenschutzbeauftragten in das erstgenannte gemeinsame Dokument der Hinweis aufgenommen, daß aus datenschutzrechtlicher Sicht auch dieser Teil der ärztlichen Aufzeichnungen zu offenbaren sei. Die Datenschutzbeauftragten legten auf diesen Zusatz insbesondere deshalb solchen Wert, weil der Standpunkt der anderen Beteiligten dazu führt, daß psychiatrisch oder psychotherapeutisch behandelten Patienten das Einsichtsrecht in seinem Kern vorenthalten bleibt; denn welche ärztliche Äußerungen in diesem Zusammenhang sind eigentlich nicht subjektiver Art? Zwar mögen auch bei Psychiatriepatienten Blutdruck und Temperatur gemessen werden, um diese objektiven Werte aber wird es dem Einsicht begehrenden Patienten nur selten gehen.

Beide Dokumente zu den Patientenrechten beschneiden im Vergleich zur Rechtsprechung, erst recht im Vergleich zur Datenschutzgesetzgebung die Rechte der Patienten. Immerhin aber erreichten die Gutachter der Universität Bremen im Verlauf eines durch sie organisierten fachlichen Diskussionsprozesses über die Umsetzung der Charta I im Lande Bremen, daß die Beteiligten, darunter auch die Vertreter von Ärztekammer, kassenärztlicher Vereinigung und des Senators für Gesundheit, den pauschalen Ausschluß von Unterlagen mit subjektiven oder bewertenden ärztlichen Aussagen doch weitgehend relativierten. So soll die Unterscheidung bei der Dokumentation von Verdachtsdiagnosen und von Behandlungen im Krankenhaus keine Rolle spielen. Lediglich in der Psychiatrie und bei psychotherapeutischer Behandlung könnten in relevantem Umfang der obengenannte therapeutische Vorbehalt oder schutzwürdige Interessen des Arztes der Einsichtnahme entgegenstehen. Es bleibt abzuwarten, ob und inwieweit diese schriftlich dokumentierten Beratungsergebnisse in Zukunft das ärztliche Verhalten gegenüber Einsicht verlangenden Patienten beeinflussen werden.

Wie schwer dies angesichts des zähen Widerstandes des ärztlichen Berufsstandes gegen eine ihren Patienten zugute kommenden Transparenz ihrer Dokumentation sein wird, zeigen Verlauf und bisheriges Ergebnis der Diskussion, die ich zeitgleich mit dem Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales über dessen „Richtlinie zur Einsichtnahme in Krankenunterlagen der Stadtgemeinde Bremen“ zu führen hatte. Diese beschränkte die Einsicht gleichfalls auf objektive Feststellungen. Auch mein Hinweis, daß § 5 des Bremischen Krankenhausdatenschutzgesetzes diese Einschränkung nicht vorsehe, fruchtete zunächst nicht. Die Auffassung der Datenschutzbeauftragten stützt auch der Beschluß des Bundesverfassungsgerichts vom 16.09.98 (BVerfGE, RDV 1999, S. 216), der die Rechtsprechung des Bundesgerichtshofs aus den Achtzigerjahren aufgreift. Das Gericht stellt fest, daß das im Recht auf Selbstbestimmung in der personalen Würde des Patienten begründete Einsichtsrecht sich grundsätzlich auf die gesamte ärztliche Dokumentation bezieht. Nur wegen entgegenstehender gleichfalls grundrechtlich fundierter Interessen des Arztes oder Dritter sowie wegen therapeutischer Vorbehalte, d.h. der begründeten Befürchtung, daß der Patient durch die Einsichtnahme gesundheitlichen Schaden nehmen könne, könne das Einsichtsrecht eingeschränkt werden. Der Arzt dürfe nicht – auch nicht nach einer psychiatrischen Behandlung – pauschal die Einsicht in nicht objektivierbare Befunde verweigern, sondern müsse die entgegenstehenden Gründe näher kennzeichnen. Auf meinen entsprechenden Hinweis hin wurde zunächst die Richtlinie überarbeitet und der Rechtsprechung angepaßt.

8.7. Elektronischer Arztbrief - Vernetzte Praxen - Integrierte Versorgung - Elektronische Patientenakte

Im Land Bremen wird eine Reihe von Projekten vorangetrieben, die den digitalisierten Austausch medizinischer Daten zwischen Ärzten, Kliniken und/oder Pflegeeinrichtungen zum Inhalt haben. Als Beispiele seien genannt:

- Der Elektronische Arztbrief: Eine Reihe von Kliniken und niedergelassenen Ärzten wollen Informationen über ihre Patienten digitalisiert austauschen. Als Einstiegsprojekt hat man den für den nachbehandelnden Arzt bestimmten Entlassungsbericht der Klinik ausgewählt.

- Der Gesundheits- und Soziallotse für Bremerhaven: Angestrebt wird die Vernetzung der Einrichtungen der gesundheitlichen Versorgung und der Pflege untereinander.
- Die Teleradiologie: Die Radiologischen Abteilungen der Bremer Kliniken und sonstige radiologische Institute sollen miteinander vernetzt werden.
- Das ICUNET: Die intensivmedizinischen Abteilungen von Krankenhäusern im Lande Bremen sollen miteinander vernetzt werden.

All diese Projekte werden im Ergebnis die Voraussetzung für die Entwicklung der elektronischen bzw. digitalisierten Patientenakte schaffen. Darunter ist zu verstehen, daß die Dokumentationen der an der gesundheitlichen Versorgung (möglicherweise auch an der Pflege) beteiligten Ärzte und anderen Fachkräfte (auch kurz Health Professionals genannt) digitalisiert und miteinander vernetzt werden. Das Netz könnte es ermöglichen, daß ein Health Professional in der Lage sein wird, jede der in das Netz eingestellten Dokumentationen abzurufen. In dieser Konsequenz würde jeder Health Professional mit der Einstellung von Daten seiner Patienten in ein Netz gegen seine berufliche Schweigepflicht verstoßen, die ausweislich der ärztlichen Berufsordnungen auch den Austausch von Patientendaten mit Fachkollegen einschränkt. In das Netz müssen durch technischen Vorkehrungen „Regelstäbe“ eingebaut werden, die die Kommunikation mit den gesetzlichen Vorgaben synchronisieren.

Zum Schutz der Persönlichkeitsrechte der betroffenen Patienten, konkretisiert durch die ärztliche Schweigepflicht und das Datenschutzrecht, ist insbesondere zu beachten:

- Den Zugriff auf in ein Netz eingestellte ärztliche/pflegerische Dokumentationen dürfen nur Health Professionals haben.
- Will ein Health Professional Patientendaten bei einem anderen abrufen bzw. an einen anderen übermitteln, so muß der betroffene Patient zuvor ihm gegenüber eingewilligt haben, vgl. § 140a Abs.2 SGB V i.d.F. der Gesundheitsreform 2000.
  Beide Vorgaben können am sichersten durch die Verwendung von Chipkarten realisiert werden: die Legitimation durch das Einlesen der Health Professional Card und die Einwilligung durch das Einlesen der Patientenkarte.
- Die Dokumentationen sind weiterhin dezentral zu führen. Die Speicherung von Patientendaten in einer zentralen Datenbank ist nicht erforderlich und erzeugt höhere Risiken.
- Die Daten sind auf dem Transportwege wirksam zu verschlüsseln. Dies gilt insbesondere für den Fall, daß das Internet benutzt wird.
- In den Fällen, in denen der Empfänger/Abrufer den Patientenbezug nicht oder nur in Ausnahmefällen benötigt, sind die Daten derart zu codieren, daß er nur mit Hilfe des Absenders oder eines Treuhänders den Patientenbezug herstellen kann, vgl. hierzu die für § 294 SGB V vorgeschlagenen Regelungen in der ursprünglich vom Bundestag verabschiedeten, aber vom Bundesrat abgelehnten Fassung der Gesundheitsreform 2000.

Bisherige Erörterungen mit Projektverantwortlichen und dem Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales berechtigen zu der Hoffnung, daß zu den oben skizzierten Anforderungen kein Dissens besteht.

8.8. Gesundheitsreform 2000 - eine vorerst vertane Chance für Datenschutz durch Technik

Im Meinungsstreit um die Gesundheitsreform 2000, d.h. die Novellierung des SGB V durch die Regierungskoalition in Berlin, standen im Herbst 1999 Schlagworte wie gedeckeltes Budget und Positivliste im Vordergrund. Mit der Ablehnung des durch den Bundestag beschlossenen Gesetzes im Bundesrat und das Inkrafttreten der "abgespeckten" Gesundheitsreform bleibt aber vorerst auch ein Vorhaben unrealisiert, das Datenschutz durch Technik, heute "privacy enhancing technology" (pet) genannt, zum Schutz der Gesundheitsdaten der gesetzlich Krankenversicherten realisiert hätte und darüber hinaus Signalwirkung für den Persönlichkeitsschutz in anderen gesellschaftlichen Bereichen hätte entfalten können.

Worum ging es? Seit Verabschiedung des Gesundheitsreformgesetzes in 1988, weiter vorangetrieben durch das Gesundheitsstrukturgesetz von 1993, ist es gesetzliches Ziel und Auftrag, den gesetzlichen Krankenkassen zum Zweck von Kostensenkung und Qualitätsverbesserung neue Kontrollverfahren und –instrumente an die Hand zu geben, die sich auf eine verbesserte Datenbasis stützen. Die zur Auswertung verwendete Datenbasis der Krankenkassen bezog sich nicht nur auf die Leistungserbringer, sondern bestand auch aus versicherten- bzw. patientenbezogenen Daten, wie Befunde, Diagnosen, ärztliche und ärztlich verordnete Leistungen. Aus Sicht der Datenschutzbeauftragten galt es, den oft beschworenen „gläsernen Patienten“ zu verhindern. Die Datenschutzbeauftragten versuchten mit Hilfe der reichlich unklaren Regelungen des SGB V zur Zweckbindung, versichertenbezogenen Abgleichen und Auswertungen seitens der Kassen Grenzen zu setzen. Leider oft vergeblich. Dabei hatte der Gesetzgeber selbst durch die von ihm vorangetriebene automatisierte Datenverarbeitung bei Leistungserbringern und Kassen Datenschutzrisiken hervorgerufen. Deshalb begrüßten sie es, als in 1993 der Gesetzgeber in § 295 Abs.2 SGB V anordnete, daß die Kassen die für die Abrechnung erforderlichen Daten über die Leistungen niedergelassener Ärzte und Zahnärzte nur fallbezogen, nicht aber versichertenbezogen erhalten dürften. Diese Regelung machte es sich zunutze, daß insoweit die Kassenärztlichen bzw. Kassenzahnärztlichen Vereinigungen zwischengeschaltet waren, d.h. öffentlichrechtliche Körperschaften, denen ihrerseits das Gesetz Kontrollaufgaben gegenüber den Ärzten übertragen hatte. Dies hatte zur Folge, daß die Kassen selbst fallbezogen keine quartalsübergreifenden Auswertungen mehr vornehmen konnten und seither bestrebt sind, ihre Datenbasis und deren Auswertung zu komplettieren. Dies wiederum rief wiederholt den Widerstand der Datenschutzbeauftragten hervor. Dabei ging es nicht um ärztliche Standesinteressen, sondern um die Daten und damit um die Persönlichkeitsrechte der gesetzlich krankenversicherten Patienten (vgl. dazu ausführlich der 18. JB unter Z. 15.1).

Über meine erfolgreichen Interventionen in diesem Zusammenhang berichtete ich bereits (vgl. 17. JB, Ziff. 13.1.2 und 18. JB, Ziff. 15.2.4.). Weitere Beispiele sind:

- Angesichts der Installation von Datenbanksystemen, die beliebige Auswertungen der gespeicherten Versichertendaten erlauben, versuchten die Datenschutzbeauftragten, die hierfür gesetzlich zuständigen Spitzenverbände der Krankenversicherung zu veranlassen, ihren Mitgliedskassen aufzugeben und Hilfestellung dabei zu leisten, technische Vorkehrungen zur Begrenzung der Auswertungen auf das gesetzlich zulässige Maß zu entwickeln und umzusetzen – bislang ohne greifbaren Erfolg (vgl. 20. JB, Ziff. 16.3).

- Die heutigen EDV-Systeme führen dazu, daß die Sachbearbeiter einer Krankenkasse im ganzen Bundesgebiet auf die Daten aller bei dieser Versicherten zugreifen können. Die Datenschutzbeauftragten von Bund und Ländern bemühen sich seit Jahren zu erreichen, daß der Versicherte selbst entscheiden kann, ob seine Daten organisationsweit verfügbar sein sollen oder nicht (vgl. die im 18. JB, Ziff. 20.7 abgedruckte Entschließung).

- Der Bundesverband der Betriebskrankenkassen entwickelte ein Projekt, bei dessen Realisierung Versichertendaten bundesweit vernetzt und für beliebige Auswertungen verfügbar wären. Nachdem die Datenschutzbeauftragten bundesweit Bedenken erhoben und ihre Beteiligung eingefordert hatten, scheint das Projekt derzeit nicht weiterverfolgt zu werden.

Die Bundesregierung legte im Sommer 1999 den Entwurf zur Gesundheitsreform 2000 mit neuen Instrumentarien zur Kontrolle der Ärzte und anderen Leistungserbringer mit Hilfe der Verarbeitung versichertenbezogener Daten vor. Die Datenschutzbeauftragten intervenierten (siehe Entschließung vom 25.08.99 unter Ziff. 18.7.). Die Bundesregierung ging auf das von Datenschutzseite vorgeschlagene Konzept ein, den Kassen zwar die für erforderlich erachteten Daten zur Verfügung zu stellen, dies aber generell für alle mit den Kassen abgerechneten Leistungen und zwar nicht versichertenbezogen. Damit war die langjährig verfestigte, für den durch die Datenschutzbeauftragten vertretenen Schutz der Persönlichkeitsrechte der Versicherten wenig effektive Konstellation aufgehoben. Zwischen dem Bundesministerium für Gesundheit und den Datenschutzbeauftragten wurde ein gesetzlicher Rahmen für die Pseudonymisierung der Daten abgestimmt, innerhalb dessen die Leistungserbringer den Krankenkassen zu den Zwecken von Abrechnung sowie Kontrolle von Wirtschaftlichkeit und Qualität ihres Handelns sämtliche Daten zu übermitteln haben. Datenannahmestellen, deren Einschaltung ohnehin geplant war, sollten die ihnen von den Leistungserbringern übermittelten Daten vor der Weiterleitung an die jeweilige Kasse so aufbereiten, daß diese zwar die gewollten Auswertungen vornehmen, aber nicht die Identifizierung einzelner Versicherter ermöglichen (vgl. die Entschließung vom 08.10.99 unter Ziff. 19.11.). Lediglich in einem besonderen Verfahren sollten die einzelnen Versicherten reidentifiziert werden können, damit den Kassen ein versichertenbezogener Datensatz zur Verfügung gestellt werden kann, der die Nutzung ausschließlich in gesetzlich definierten Ausnahmefällen ermöglicht. Das technische Instrumentarium für dieses Verfahren steht inzwischen bei vergleichsweise geringem Aufwand zur Verfügung. Der Bundestag verabschiedete am 04.11.99 diese innovative Regelung (BR-Drs. 609/99). Leider fiel sie am 26.11.99 der Ablehnung des Gesamtkonzepts der Gesundheitsreform 2000 im Bundesrat zum Opfer. Im Vermittlungsausschuß wurde der Vorschlag des Bundesministeriums und einzelner Datenschutzbeauftragter, die Regelung in Gestalt eines Gesetzes zur Verbesserung des Datenschutzes und der Datengrundlage der gesetzlichen Krankenkassen zu verabschieden, leider

nicht aufgegriffen. Im anschließend vom Bundestag verabschiedeten Gesetz zur Gesundheitsreform 2000 fehlt sie. Die bislang geltenden Vorschriften zur Datengrundlage der Krankenkassen gelten weiter und damit bleiben die oben dargestellten Konflikte weiterhin ungelöst. Überdies sind neue Konflikte vorprogrammiert. So sehen die §§ 136a-137e des SGB V nunmehr ein differenziertes Instrumentarium zur Qualitätssicherung in der Medizin vor. Unter den im unverändert gebliebenen § 284 SGB V aufgeführten Zwecken, für die Krankenkassen versichertenbezogene Daten verarbeiten dürfen, fehlt nun aber weiterhin die Sicherung oder Verbesserung der Qualität. Wäre der ursprünglich verabschiedete Entwurf Gesetz geworden, dürften Versichertendaten auch zu diesem Zweck verarbeitet werden, allerdings lediglich in pseudonymisierter Form. Nun ist zu befürchten, daß entgegen der sowohl aus Sicht der Krankenkassen als auch aus Sicht des Datenschutzes unbefriedigenden Gesetzeslage Qualitätssicherung mit versichertenbezogenen Daten betrieben wird und die Datenschutzbeauftragten in Erfüllung ihrer gesetzlichen Aufgaben Gefahr laufen, als Qualitätsgegner diffamiert zu werden. Ich kann nur hoffen, daß der Gesetzgeber sein letztes Wort noch nicht gesprochen hat, sondern daß die Pseudonymisierung der Daten Krankenversicherter bei nächster Gelegenheit erneut auf der Tagesordnung von Bundestag und Bundesrat stehen wird. Öffentlichen Verlautbarungen des Ministeriums sind solche Absichten zu entnehmen.

9. Jugend, Soziales und Arbeit

9.1. Kindergarten-Informationssystem (KIS)

KIS dient der automatisierten Verarbeitung der Sozialdaten von Eltern mit Kindern in Kindertagesheimen (KTH). Es wurde im Herbst 1997 in einigen KTH der Stadtgemeinde Bremen mit einem Modul für das Aufnahmeverfahren installiert. Im Jahre 2000 soll es, zusätzlich mit einem Modul für die Beitragsberechnung ausgerüstet und in allen städtischen KTH in Betrieb genommen werden. Bereits in vorangegangenen Jahren hatte ich berichtet (vgl zuletzt 21. JB, Ziff. 12.3.). Nach Präzisierung einiger Details lag im April 1999 ein mit mir abschließend abgestimmtes Datenschutzkonzept vor. Dessen technische Umsetzung prüfte ich im August 1999 exemplarisch in einem städtischen KTH. Ich mußte feststellen, daß wesentliche rechtlich gebotene technische Vorkehrungen wie etwa die Einschränkung der Zugriffe der Nutzer auf erforderliche Systemressourcen, die Protokollierungen und die Sicher-heitseinstellungen des KTH-Verzeichnisses im Rahmen des Betriebssystems nicht umgesetzt worden waren. Dies teilte ich dem Ressort mit. Mir wurde umgehende Nachbesserung zugesichert. Im November 1999 nahm ich in zwei städtischen KTH eine exemplarische Nachprüfung vor; diesmal mit dem Ergebnis, daß die gebotenen und zugesagten Sicherungsvorkehrungen weitgehend umgesetzt worden waren. Dazu gehören insbesondere

- die Definition der zulässigen Datenkataloge und die entsprechende Festlegung der Datenfelder im Anwendungsprogramm KIS,
- eine angemessene Konfiguration des Betriebssystems WINDOWS-NT und
- ein sicheres Backup-Verfahren.

Das Ressort hat versichert, daß diese Sicherheitseinstellungen in allen KTH der Stadtgemeinde Bremen implementiert werden, bevor in ihnen KIS genutzt wird.

KIS wird aber auch bereits derzeit in KTH freier Träger in der Stadtgemeinde Bremen genutzt. Freie Träger, die in ihren KTH KIS installieren, müssen das gleiche Datenschutzniveau gewährleisten. Ich

habe das Ressort für Jugend unter Hinweis darauf, daß es an der Entscheidung der freien Träger für den Einsatz von KIS beteiligt gewesen ist und daß überdies § 61 Abs.4 SGB VIII ihm die Verantwortung für die Wahrung des Sozialgeheimnisses bei den freien Trägern überträgt, gebeten, mich darüber zu unterrichten, ob diese ihre KIS-Systeme mit vergleichbaren Sicherungsvorkehrungen ausgestattet haben oder ob daran gedacht ist, sie entsprechend nachzurüsten. Sollte ich keine befriedigende Antwort erhalten, werde ich mich direkt an die freien Träger wenden.

9.2. Ressortinternes Informationssystem - Elektronische Fallakte

Der Senator für Gesundheit, Jugend und Soziales plant, seine Abteilungen und Ämter miteinander zu vernetzen. Im Berichtsjahr übersandte mir das Ressort Unterlagen über ein Netzkonzept. Darin wurden ein Datenschutz- und ein Datensicherungskonzept angekündigt. Vorsorglich machte ich darauf aufmerksam, daß darin auch folgende Festlegungen zu treffen seien:

- Differenzierung der Zugriffsberechtigungen je nach interner Aufgabenverteilung,
- Kontrolle und Protokollierung der Zugriffe durch die zentrale Netzwerkadministration,
- ggf. Schutz vor unerlaubten Zugriffen aus dem Internet und
- ggf. Rahmenbedingungen für externe Online-Abrufe.

Den Unterlagen konnte ich entnehmen, daß geplant ist, eine Art Data-Warehouse zu realisieren., d.h. eine aufbereitete, strukturierte Sammlung von Daten aus allen Bereichen des Ressorts zur Entscheidungsunterstützung und zum Controlling. Auf meinen Hinweis, daß wegen der damit geplanten umfassenden Verfügbarkeit und Nutzbarkeit in diesem Zusammenhang jedenfalls keine Sozialdaten zur Verfügung gestellt werden dürften, erhielt ich zur Antwort, daran sei nicht gedacht, sofern ein Data-Warehouse eingerichtet werde, sollten nur anonymisierte Daten zur Verfügung gestellt werden.

Weiter scheinen die Vorbereitungen für die Einführung der Elektronischen Fallakte in der Jugendhilfe vorangetrieben worden zu sein, für die die interne Vernetzung gleichfalls die technische Grundlage bietet. Auch hierzu erhielt ich im Berichtsjahr Unterlagen. Bei den Vorbereitungen eines entsprechenden Projekts hatte mich das Amt für Jugend und Familie in Bremerhaven beteiligt. Beim Vergleich der Unterlagen zu beiden Vorhaben war auffällig, daß die hier in Aussicht genommene Standard-Software die Speicherung von Klientendaten lediglich in vorstrukturierten Datenfeldern vorsieht. Deren erste Durchsicht ließ erkennen, daß es sich dabei um die Daten handeln dürfte, die für die Entscheidung über die Gewährung kostenrelevanter Hilfen erheblich sind, d.h. um Verwaltungsdaten im eigentlichen Sinne. Gegen deren Verarbeitung in einem amtsinternen Netz bestehen keine grundsätzlichen Bedenken, vorausgesetzt, sie stehen lediglich für die Zugriffe der Mitarbeiter zur Verfügung, die sie zur Erfüllung ihrer Aufgaben benötigen. Auch müssen sie vor unbefugten Zugriffen geschützt sein. Dagegen ließen die Unterlagen aus Bremen erkennen, daß man hier zwar dieselbe Software einsetzen will, jedoch sollen alle Daten aus der fachlichen Sachbearbeitung im pädagogischen Bereich digitalisiert gespeichert und in das Netz eingestellt werden. Dies gab Anlaß zu der Befürchtung, daß berufliche Schweigepflichten und der besondere Vertrauensschutz, den § 65 SGB VIII den Klientendaten einräumt, die einem Mitarbeiter eines öffentlichen Trägers der Jugendhilfe zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind, gefährdet werden könnten. Auf meinen im September 1999 gemachten Vorschlag,

darüber zu sprechen, reagierte das Ressort nicht. Auch die Zusage vom Juni 1999, mich weiterhin über den Sachstand zu informieren, wurde bislang nicht eingelöst. Daran habe ich das Ressort jetzt erinnert und um Unterrichtung gebeten.

9.3. Informationsverbund illegale Beschäftigung

Im 21. JB berichtete ich unter Ziff.13.1 ausführlich über das Vorhaben des Senats, beim Senator für Arbeit einen Informationsverbund zur Bekämpfung illegaler Beschäftigung in Gestalt einer zentralen Datei einzurichten. Mit deren Hilfe sollen alle mit dieser Aufgabe beauftragten öffentlichen Stellen instandgesetzt werden, Daten, darunter auch auf Arbeitgeber und Beschäftigte bezogene Daten, untereinander auszutauschen. Ich hatte in diesem Zusammenhang auf bundesrechtliche Regelungen hingewiesen, die die Verfolgungs-, Kontroll- und Koordinierungsaufgaben, die Zuständigkeiten, die Mitteilungspflichten, die Übermittlungsbefugnisse und die Auskunftsrechte einer Vielzahl im einzelnen genannter öffentlicher Stellen (Arbeitsämter und andere Sozialversicherungsträger, Finanzbehörden, Staatsanwaltschaften, Ordnungsbehörden, Gewerbeaufsichtsämter) im einzelnen regeln. Die Fragen wurden auch in der letzten Legislaturperiode im Datenschutzausschuß eingehend diskutiert.

Inzwischen hat der Senator für Arbeit den in Frage kommenden Auftraggebern Entwürfe für die Vereinbarungen vorgelegt. Bei den konkreten Verhandlungen traten bei den Verantwortlichen Bedenken gegen das Vorhaben auf. Von denen wurden insbesondere folgende Gesichtspunkte eingebracht:

- Die unterschiedlichen Rechtsgrundlagen würden unterschiedliche Lösungen erfordern. Mitteilungspflichten erlaubten andere Regelungen als Auskunftsbefugnisse. Voraussetzungen, Inhalte und Adressaten der vorgeschriebenen Übermittlungen seien je nach Rechtsgrundlage unterschiedlich. Besondere Amtsgeheimnisse wie das Sozial- und das Steuergeheimnis seien zu beachten.

- Einige potenzielle Auftraggeber haben grundsätzliche rechtliche Bedenken gegen die Einschaltung einer zentralen Datenannahme- und Verteilstelle geäußert und meinten, sie dürften nur direkt an die im Gesetz genannten Adressaten übermitteln. Andere befürchteten, ihren gesetzlichen Verpflichtungen nicht schon durch die Einstellung von Daten in die Zentraldatei, sondern nur durch Übermittlung direkt an die im Gesetz genannten Adressaten nachkommen zu können.

- Es wurde bezweifelt, ob die Zwischenschaltung einer zentralen Stelle erforderlich und zweckmäßig sei, bzw. es wird befürchtet, daß dies zu zeitlichen Verzögerungen, Übermittlungsfehlern und Mehrarbeit führe.

Die Bau-Berufsgossenschaft Hannover lehnt die Beteiligung an dem Vorhaben aus rechtlichen Gründen ab. In den anderen Fällen ist mir ein abschließender Stand der bilateralen Verhandlungen nicht bekannt.

Ich habe darauf hinweisen müssen, daß nicht ich, sondern die Auftraggeber, d. h. auch Stellen des Bundes, über deren Beteiligung zu entscheiden haben. Diese müssen darüber hinaus zuständigkeitshalber die Abstimmung mit dem Bundesbeauftragten für den Datenschutz einleiten. Die

Verhandlungen und Abstimmungen haben sich durch den Berichtszeitraum hingezogen und sind noch nicht abgeschlossen.

10. Bildung und Wissenschaft

10.1. PISA-Studie

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) führt im Rahmen ihres Indikatorenprogramms zu den Bildungssystemen der Mitgliedsstaaten (INES – Indicator of Educational Systems) eine internationale Schulleistungsstudie (PISA – Programme for International Student Assessment) durch, an der sich auch die Bundesrepublik Deutschland beteiligt. Die Kultusminister der Bundesländer haben neben der Beteiligung auch beschlossen, die PISA – Studie national zu ergänzen und Leistungsvergleiche zwischen den Bundesländern durchzuführen.

Ziel der internationalen Schulvergleichsstudie PISA ist es, die Schulleistungen von 15-jährigen Schülern und Schülerinnen sowie von Schülern der 9. Klasse in den Bereichen Lesen, Mathematik, Naturwissenschaften sowie in fächerübergreifenden Kompetenzen (die für methodisches Vorgehen, selbsttätiges Lernen und kooperatives Arbeiten notwendig sind) zu beschreiben und nach Gründen für gefundene Unterschiede zu suchen.

PISA soll sich über mehrere Projektzyklen erstrecken. Derzeit läuft der erste Zyklus, in dem der Bereich Lesen im Vordergrund stehen soll. Verantwortlich für die Durchführung der Studie in der Bundesrepublik Deutschland ist ein Konsortium mehrerer Universitäten und Forschungseinrichtungen unter Federführung des Max-Planck-Instituts für Bildungsforschung, Berlin. Die Feldarbeit und die Datenverarbeitung hat das Data Processing Center der International Association for the Evaluation of Educational Achievement (IEA – DPC), Hamburg übernommen.

Im Frühjahr 1999 fand der sog. PISA – Feldtest (Pretest) statt, in dem die Instrumente und Prozeduren wie z.B. Testfragen und Fragebögen, Begleitschreiben, Erhebungs- und Aufbereitungsverfahren erprobt werden sollten. Auch bremische Schulen (Schüler, Eltern der Stichprobenschüler, Schulleiter) waren hier beteiligt. Nach Auswertung des Feldtests und Überarbeitung der Instrumente und Prozeduren soll nach den Osterferien 2000 mit der PISA – Haupterhebung begonnen werden.

Ich wurde Ende 1998 erstmalig vom Senator für Bildung, Wissenschaft, Kunst und Sport in allgemeiner Form über das Vorhaben informiert und um datenschutzrechtliche Beurteilung gebeten. Ohne damals schon nähere Einzelheiten des Projekts zu kennen, habe ich in allgemeiner Form über die im Bundesland Bremen zu beachtenden Datenschutzerfordernisse informiert und auf die § 21 BrDSG und § 13 BrSchulDSG sowie auf mein Merkblatt zum Datenschutz bei Forschungsprojekten hingewiesen.

Im April 1999 habe ich nach Eingang weiterer Informationen seitens des Bildungsressorts und von Stellungnahmen meiner Kollegen aus den anderen Bundesländern endgültig zum PISA – Pretest im Lande Bremen Stellung genommen. Zentrale Punkte in den Stellungnahmen waren die Freiwilligkeit der Teilnahme, die informierte Einwilligung der Befragungspersonen, die Gestaltung der Anschreiben, die Sicherung der zugesicherten Anonymität und die (anonyme) Weiterverarbeitung der erhobenen Daten.

Als Ergebnis ist festzustellen, daß die datenschutzrechtlichen Anforderungen vom Projekt weitgehend berücksichtigt werden, so daß einer Durchführung der PISA – Haupterhebung im Frühjahr 2000 aus Datenschutzsicht keine Hindernisse im Wege stehen.

10.2. Datenerhebung zum Thema "Jugendkriminalität und Gewalt in der Schule"

Auch im vergangenen Jahr war ich wieder mit zahlreichen Untersuchungen, Erhebungen und Forschungsvorhaben befaßt, die an Schulen in Bremen und Bremerhaven durchgeführt werden sollten. Bei der Prüfung der mir vorgelegten Vorhaben mußte ich mehrfach auf die Beachtung wichtiger datenschutzrechtlicher Anforderungen hinweisen.

Besonders erwähnt werden soll an dieser Stelle eine Befragungsaktion an der Heinrich-Heine-Schule in Bremerhaven, bei der Schüler und Lehrer umfangreiche und auch sehr sensible persönliche Bereiche betreffende Fragen zum Thema „Jugendkriminalität und Gewalt in der Schule“ beantworten sollten. Ursache dieser Befragungsaktion war die zunehmende Kriminalitäts- und Gewaltbereitschaft von Schülern, für deren Bekämpfung an Schulen es noch der Erarbeitung geeigneter Konzepte bedarf. So wie mir die Befragungsaktion vor ihrer Durchführung seitens der Schule dargestellt worden war, sollte die Erhebung im Rahmen eines wissenschaftlichen Forschungsvorhabens der Universität Bielefeld durchgeführt werden, deren Mitarbeiter selbst an der Schule die Befragungsaktion vornehmen sollten. Nach der Auswertung der erhobenen Daten an der Universität Bielefeld sollten die Ergebnisse der Befragungsaktion an der Schule im Rahmen einer schulinternen Lehrerfortbildung genutzt werden.

Den Wunsch vieler Schulen, Kriminalität und Gewalt unter ihren Schülern mit geeigneten Mitteln zu begegnen, halte auch ich für begrüßenswert. Doch wenn zur Feststellung von Sachverhalten bei Schülern und Lehrern personenbezogene Daten erhoben werden sollen, dann dürfen die datenschutzrechtlichen Anforderungen für derartige Erhebungsaktionen nicht außer acht gelassen werden. Der bremische Gesetzgeber hat die Durchführung von Erhebungen, Untersuchungen und Forschungsvorhaben an Schulen an strenge rechtliche Voraussetzungen geknüpft, die sich im wesentlichen aus dem Gesetz zum Datenschutz im Schulwesen (BrSchulDSG) und dem Bremischen Datenschutzgesetz (BrDSG) ergeben. In den Bestimmungen dieser Gesetze, speziell des § 13 BrSchulDSG und des § 21 BrDSG, ist weitgehend festgelegt, was in datenschutzrechtlicher Hinsicht bei der Durchführung solcher Vorhaben an Schulen zu beachten ist.

Bei der Durchführung der Datenerhebung zum Thema „Jugendkriminalität und Gewalt in der Schule“ an der Heinrich-Heine-Schule wurden die datenschutzrechtlichen Vorgaben in gröblicher Weise ignoriert.

So ist trotz meiner Empfehlung nicht darauf geachtet worden, die erforderlichen individuellen Einwilligungserklärungen der Erziehungsberechtigten einzuholen. Die Schule begründete dieses damit, daß vom Schulpsychologen und einer an der Schule ebenfalls tätigen Sozialarbeiterin im Rahmen ihrer Tätigkeit zu Beginn der Schullaufbahn der Schüler eine generelle schriftliche Einverständniserklärung für die Teilnahme an Befragungen bzw. psychologischen Testverfahren eingeholt werde, so daß die Schule keine weitere Erklärung der Erziehungsberechtigten mehr für erforderlich hielt. Die zu Beginn der Schullaufbahnen eingeholten generellen

Einverständniserklärungen reichten in datenschutzrechtlicher Hinsicht aber keinesfalls aus. Eine informierte Einwilligung, wie sie das Gesetz verlangt, kann vom Betroffenen bzw. dessen Erziehungsberechtigten nur erteilt werden, wenn er vor der Durchführung des jeweils beabsichtigten Erhebungsvorhabens über dieses ausreichend informiert wird.

Zu bemängeln war auch, daß die Erhebung nicht wie ursprünglich vorgesehen von Mitarbeitern der Universität Bielefeld, sondern von an der Schule tätigen Mitarbeitern, dem Schulpsychologen und einer Sozialarbeiterin, durchgeführt wurde. Für die Schüler stellte sich die Befragungsaktion als Pflicht im Rahmen des Unterrichts dar, eine Trennung zwischen freiwilliger Teilnahme und schulischem Pflichtprogramm war nicht gewährleistet.

Zum Auftrag der Schule gehört es nicht, Forschungsvorhaben durchzuführen. Nach dem Bremischen Schuldatenschutzgesetz (§ 1) ist der Schule die Verarbeitung personenbezogener Daten ihrer Schüler, Eltern, Lehrer oder sonstiger Mitarbeiter nur insoweit gestattet, als diese zur Erfüllung des Unterrichts- und Erziehungsauftrags und zur Wahrnehmung der gesetzlichen Mitwirkungsrechte erforderlich ist.

Darüber hinaus verlangen sowohl die Bestimmungen des Bremischen Schulverwaltungsgesetzes als auch die des Gesetzes zum Datenschutz im Schulwesen eine klare Trennung zwischen der Tätigkeit der Schule und derjenigen des Schulpsychologen (funktionelle Trennung). Die Tätigkeiten dürfen nicht miteinander vermischt werden. Die notwendige Trennung war bei der Datenerhebung an der Heinrich-Heine-Schule nicht gewährleistet.

Deutliche Kritik rief bei mir außerdem hervor, daß die Schule mich nur sehr zögerlich über den Fortgang des Vorhabens informiert hat. Die von mir benötigten Auskünfte habe ich erst ca. neun Monate, nachdem die Erhebung stattgefunden hatte, erhalten. Die in § 27 Abs. 3 BrDSG enthaltene Verpflichtung zur Unterstützung und zur Auskunft gegenüber dem Landesbeauftragten für den Datenschutz wurde mißachtet.

Über die von mir festgestellten Mängel informierte ich neben der Schule auch den zuständigen Stadtrat der Stadt Bremerhaven. Ich halte es für dringend erforderlich, daß dieser die Bremerhavener Schulen noch einmal ausführlich über die korrekte Durchführung von Datenerhebungen, Untersuchungen und Forschungsvorhaben an Schulen und die dabei anzuwendenden funktionellen Trennungsgebote unterrichtet.

10.3. Internet-Nutzung der Schulen

Viele bremische Schulen beschäftigen sich mit der Nutzung des Internets und haben bereits eigene Homepages eingerichtet. Schon bei flüchtiger Betrachtung derartiger Internet-Präsentationen fallen der große Wildwuchs und die offenkundige Unkenntnis datenschutzrechtlicher Erfordernisse auf. Leider hat der Senator für Bildung und Wissenschaft bisher keine landesweiten Empfehlungen für eine datenschutzgerechte Nutzung dieses neuartigen Mediums erlassen. Bei allem Verständnis für die Technikbegeisterung und die allgemeine Förderung des Mediums („Schulen ans Netz“, „Internet-Zugang für alle Schulen“) muß doch auf die datenschutzrechtlichen Rahmenbedingungen hingewiesen werden, die bei Nutzung dieses Mediums zu beachten sind. Ich habe in einem ersten Anlauf ein Anforderungspapier erarbeitet, das ich mit den Schulbehörden und den Schulen im Lande

Bremen diskutieren und abstimmen will, um zu einer datenschutzgerechten Nutzung des Mediums durch Schulen zu gelangen. Folgende Punkte erscheinen mir dabei wesentlich:

Die Internet-Nutzung durch Schulen berührt verschiedene datenschutzrechtliche Regelungen, auch wenn dieses Medium teilweise unterrichtlich genutzt werden sollte. Konkret handelt es sich hierbei um das Telekommunikationsgesetz (TKG), das Gesetz über die Nutzung von Telediensten (Teledienstegesetz - TDG), das Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz - TDDSG), den Mediendienstestaatsvertrag (MDStV) sowie bei öffentlichen Schulen im Bundesland Bremen um das Bremische Gesetz zum Datenschutz im Schulwesen (BrSchulDSG) und daneben um das Bremische Datenschutzgesetz (BrDSG).

Wegen der erheblichen Datenschutz- und Datensicherheitsrisiken bei Nutzung des allgemein zugänglichen Internet müssen seitens der Schulen besondere technisch-organisatorische Sicherheitsmaßnahmen (§§ 19, 20 BrSchulDSG, § 7 BrDSG) ergriffen werden. Diese bestimmen sich je nach Art des Rechneranschlusses und der Internet-Nutzung. Die Nutzung des Internets im Unterricht ist hier eingeschlossen.

Es empfiehlt sich, verantwortliche Personen für die Beschaffung, Betreuung und Administration der gesamten DV- und TK-Technik der Schule sowie für die Beratung und Kontrolle in Datenschutzrechtsfragen zu bestimmen. Die Betreuung und Pflege des Internet-Angebots der Schule ist ebenfalls verantwortlich sowie fachkundig zu regeln.

Die Rechner der Schulverwaltung (evtl. eingebunden in ein Netz der Gesamtverwaltung) und die Rechner der unterrichtlichen Nutzung samt Internet sind gemäß § 19 BrSchulDSG strikt zu trennen (kein Netzverbund, keine gemischte Nutzung, kein Geräteaustausch, kein Datenträgeraustausch).

Die Gestaltung der Homepage einer Schule und das Einstellen von Präsentations- und Angebotsseiten der Schule ins Internet erfolgt in Verantwortung der jeweiligen Schule (speichernde Stelle im Sinne des Datenschutzrechts). Sie muß dabei u.a. folgende spezifische Anforderungen berücksichtigen:

- Es besteht nach § 6 TDG, § 6 MDStV eine Pflicht zur Anbieterkennzeichnung. Die Schule muß also sich und die verantwortliche Leitungsperson namentlich mit schulischer Anschrift benennen.
- Links, d.h. Verweise auf Homepages von Privatpersonen, Betrieben, Vereinen, Organisationen o.dgl. sollten regelmäßig überprüft werden. Es sollte ausgeschlossen werden, daß auf Homepages mit rechtswidrigem Inhalt verwiesen wird (vgl. § 8 MDStV).
- Der Anbieter (Schule) darf die Erbringung von Diensten nicht von einer Einwilligung des Nutzers in die Verarbeitung und Nutzung seiner Daten für andere Zwecke, z.B. Werbung abhängig machen (§ 3 Abs. 3 TDDSG, § 12 Abs. 4 MDStV).
- Nutzungsprofile, z.B. wie oft hat ein bestimmter Nutzer die Homepage der Schule aufgerufen, sind nur bei Verwendung von Pseudonymen zulässig (§ 4 Abs. 4 TDDSG, § 13 Abs. 4 MDStV). Das Setzen sog. Cookies durch die Schule sollte unterbleiben (nur mit ausdrücklicher Einwilligung des jeweiligen Nutzers überhaupt zulässig!).

- Jeder Nutzer ist grundsätzlich berechtigt, jederzeit die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten unentgeltlich beim Anbieter (Schule) einzusehen (§ 7 TDDSG, §16 Abs. 1 MDStV).

Sachdarstellungen ohne Personenbezug sind im Rahmen einer Selbstdarstellung und Präsentation der Schule im Internet aus datenschutzrechtlicher Sicht unproblematisch. Gleiches gilt für die Darstellung interner Gliederungs- und Organisationspläne, für Telefonverzeichnisse sowie sonstige Informationen ohne Personenbezug. Für Stundenpläne und Vertretungspläne sowie Adreßlisten der schulischen Gremien gelten wegen des Personenbezugs besondere Zulässigkeitsregeln.

Gästebücher, innerhalb derer Dritte Mitteilungen für allgemeinen Zugriff ablegen können, sollten besonders kritisch auf ihre Erforderlichkeit geprüft werden. Dem meist nur geringen Nutzen für die Aufgabenerfüllung der Schule oder die Attraktivität des Internet-Angebotes stehen neben dem laufenden Betreuungsaufwand und möglichen Haftungsfolgen auch Gefährdungen für das informationelle Selbstbestimmungsrecht der Gäste gegenüber. Auf die Risiken, die mit der Nutzung dieser Möglichkeit verbunden sind, sollte aufmerksam gemacht werden. Die Verarbeitung hierbei gewonnener Nutzerdaten durch die Schule fällt unter die Regelungen des TDDSG.

Sofern die Schule die Möglichkeit der Kontaktaufnahme per E-mail anbietet, sollten die elektronischen Briefe verschlüsselt verschickt werden können. Hierzu sollte die Schule auf ihrer Homepage einen (öffentlichen) Schlüssel bekanntgeben, der von den Absendern einer Nachricht benutzt werden kann. Als Verschlüsselungsverfahren wird PGP (Pretty Good Privacy) empfohlen. Die Schule sollte sich im übrigen der Gefahren bewußt sein, die mit der Benutzung dieses Dienstes verbunden sind. Außerdem müßten die Schulen interne Regelungen für die Entgegennahme und Behandlung von E-Mails schaffen (vgl. Ziff. 3.4. in diesem Bericht).

Für die Zulässigkeit der Darstellung und Präsentation von Lehrerdaten im Internet (Lehrer, Lehrmeister, Referendare) durch öffentliche Schulen im Lande Bremen gelten die §§ 1 und 2 Abs. 7 BrSchulDSG i.V. mit § 22 BrDSG mit Verweis auf §§ 93 ff. Bremisches Beamtengesetz.

Nach § 1 Abs. 1 BrSchulDSG dürfen öffentliche Schulen Lehrerdaten nur verarbeiten, soweit es zur Erfüllung ihres Unterrichts- und Erziehungsauftrages und zur Wahrnehmung gesetzlicher Mitwirkungsrechte erforderlich ist (Zweckbindungsgebot und Erforderlichkeitsprinzip). Die Zulässigkeit der Datenverarbeitung über Lehrer selbst richtet sich gemäß § 2 Abs. 7 BrSchulDSG nach den Regelungen des § 22 BrDSG. Danach dürfen öffentliche Stellen personenbezogene Daten über Bewerber, Bedienstete und ehemalige Bedienstete nur nach Maßgabe der §§ 93 ff. Bremisches Beamtengesetz verarbeiten, wobei die Verarbeitung dieser Daten in automatisierten Verfahren (z.B. Internet-Präsentation) der Zustimmung der obersten Dienstbehörde bedarf (§ 22 Abs. 2 BrDSG).

Als Verarbeitungszwecke werden in § 93 Bremisches Beamtengesetz genannt: Begründung, Beendigung oder Abwicklung des Dienstverhältnisses, Durchführung organisatorischer , personeller und sozialer Maßnahmen, insbesondere auch Personalplanung und Personaleinsatz. Dem Erforderlichkeitsprinzip werden hier zusätzlich noch die schutzwürdigen Belange der Betroffenen gegenübergestellt. Gemäß § 93g Bremisches Beamtengesetz dürfen Personal(akten)daten in Dateien nur für die genannten Zwecke verarbeitet werden. Ihre Übermittlung ist nur nach Maßgabe des § 93e

Bremisches Beamtengesetz zulässig. Ein automatisierter Datenabruf (Internet- und Intranet-Abruf) durch andere Behörden (und damit besonders auch private Stellen!) ist unzulässig, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist. Nach § 93g Bremisches Beamtengesetz ist dem Beamten bei erstmaliger Speicherung die Art der über ihn gespeicherten Daten mitzuteilen, bei wesentlichen Änderungen ist er zu benachrichtigen. Auskünfte an Dritte (z. B. die Bereitstellung von Lehrerdaten im Internet) dürfen nach § 93e Abs. 2 Bremisches Beamtengesetz nur mit Einwilligung des Beamten erteilt werden, es sei denn, es liegen bestimmte Ausnahmen vor (Beeinträchtigung des Gemeinwohls, der Schutz berechtigter höherrangiger Interessen des Dritten). Inhalt und Empfänger der Auskunft sind dem Beamten schriftlich mitzuteilen.

Für die Präsentation von **Lehrerdaten im Internet** bedeutet dies:

- Die Präsentation von Lehrerdaten im Internet einschl. evtl. Texten, Beschreibungen, Bildern oder Photos ist nur mit ausdrücklicher schriftlicher Einwilligung der Betroffenen zulässig. Hierbei gelten das Zweckbindungsgebot (rein schulischer Zweck) und das Erforderlichkeitsprinzip (nur die zur Zweckerfüllung notwendigen Daten). Die schutzwürdigen Belange der Betroffenen sind trotz Einwilligung zu berücksichtigen. Die Internet-Präsentation ist auch bei Einwilligung auf rein schulische Daten beschränkt.
- Bei Repräsentanten der Schule (z.B. Schulleiter, Vertreter) und bei für die Außendarstellung der Schule wichtigen Funktionsträgern sind das Zweckbindungsgebot und das Erforderlichkeitsprinzip anders einzuschätzen, als bei den übrigen Lehrern. Das prinzipielle Einwilligungserfordernis könnte hier durch das Ausnahmekriterium „Schutz berechtigter höherrangiger Interessen der Öffentlichkeit“ ersetzt werden. Zulässig für eine Präsentation im Internet wären danach dann der Name, die dienstliche Funktion, die dienstliche Anschrift und Angaben zur dienstlichen Erreichbarkeit wie z. B. dienstliche Telefonnummer oder Faxnummer.
- Die oberste Dienstbehörde muß der Präsentation von Lehrerdaten im Internet zustimmen. Bei der erstmaligen Speicherung der Daten (Einstellung ins Internet) ist den Betroffenen die Art der Daten mitzuteilen, bei wesentlichen Datenänderungen sind sie zu benachrichtigen. Im übrigen haben die Betroffenen die nach dem BrDSG üblichen Rechte (z. B. Auskunft, Sperrung, Löschung, Berichtigung).

Für die Zulässigkeit der Darstellung und Präsentation von **Daten des übrigen Schulpersonals** wie z. B. Hausmeister, Sekretärinnen, sonstige Mitarbeiter gelten analoge Regelungen (§ 22 BrDSG mit Verweis auf §§ 93 ff. Bremisches Beamtengesetz). Die Einstellung von Daten, Texten, Bildern oder Photos ist nur mit ausdrücklicher schriftlicher Einwilligung zulässig. Sie ist im Einwilligungsfall beschränkt auf die rein dienstlichen Funktionen. Dieses Personal hat für die Außenrepräsentation der Schule keine Bedeutung, sondern eine rein interne Funktionen. Dies bedeutet, daß immer eine Einwilligung erforderlich ist. Es gilt im übrigen das zuvor Gesagte.

Für die Zulässigkeit der Darstellung und Präsentation von Schüler- und Elterndaten im Internet gilt das BrSchulDSG. Auch hier gelten das Zweckbindungsgebot und das Erforderlichkeitsprinzip des § 1 Abs. 1 BrSchulDSG: Erfüllung des Unterrichts- und Erziehungsauftrages der Schule sowie Wahrnehmung der gesetzlichen Mitwirkungsrechte. Bestimmte Schülerdaten, z. B. die Bewertung von Leistungskontrollen, persönliche Notizen des Lehrers über Schüler, Klassenbucheintragungen gelten

dabei nicht als Daten im Sinne des BrSchulDSG, für sie gelten aber das Verarbeitungsverbot des § 3 Abs. 2 BrSchulDSG (keine Verarbeitung auf privatem Rechner oder auf Rechnern außerhalb der Schule), die Übermittlungsbestimmungen des BrSchulDSG (§§ 5 bis 10) und die besondere Sorgfaltsverpflichtung nach § 1 Abs. 5 BrSchulDSG.

Für die Darstellung und Präsentation von **Schüler- und Elterndaten** im Internet durch öffentliche Schulen im Lande Bremen bedeutet dies:

- Die Darstellung und Präsentation von Schüler- und Elterndaten einschließlich etwaiger Texte, Beschreibungen, Bilder bzw. Photos im Internet (Datenübermittlung!) ist nicht zulässig, auch nicht mit Einwilligung der Schüler bzw. ihrer Erziehungsberechtigten. Die Übermittlung ist zur Erreichung des schulischen Zwecks nicht erforderlich. Die Übermittlungstatbestände der §§ 5 bis 10 BrSchulDSG liegen nicht vor. Eine fehlende Einwilligung kann wegen des fehlenden schulischen Zwecks auch nicht vom Schulleiter ersetzt werden (§ 4 Abs. 2 und 3 BrSchulDSG).
- Lediglich Name, Funktion und schulische Erreichbarkeit der Elternvertretung der Schule (nicht Klassenvertretung!) dürften gemäß § 2 Abs. 6 BrSchulDSG wegen ihrer Funktionsträgerschaft ins Internet eingestellt werden; empfehlenswert ist hier aber auch die Einwilligung der Betroffenen. Die Schülervertretung der Schule darf nicht (auch nicht bei Einwilligung) in das Internet eingestellt werden; das BrSchulDSG enthält zur Übermittlung von Schülerdaten durch die Schulen eine abschließende Regelung. Es wäre allenfalls zulässig, wenn die Gesamtvertretung der Schülerschaft mit Einwilligung der Betroffenen sich im Internet präsentiert.

Die Nutzung des Internets durch Schüler sollte nur im Rahmen einer Nutzungsordnung zugelassen werden, z. B. nur für Unterrichtszwecke, nur zu bestimmten Zeiten und für bestimmte speziell konfigurierte Geräte. Mißbräuche und Verstöße müßten mit Nutzungsausschluß geahndet werden. Aufstellung und Ausstattung dieser Geräte müßten der Nutzung entsprechend sein. Klarnamen von Schülern (nicht Klassen oder Jahrgangsstufen) sind zu vermeiden (z. B. als E-Mail-Adresse).

Diese Grundsätze habe ich erst gegen Berichtsende zur Diskussion gestellt (vgl. hierzu auch Ziff. 1.9.), so daß ich Rückäußerungen erst in der kommenden Zeit erwarte.

11. Bau, Verkehr und Umwelt

11.1. Neues Wohngeldverfahren in Bremen und Bremerhaven

Für Bremen und Bremerhaven ist durch die ID Bremen das Verfahren für die Wohngeldbearbeitung ‚BREWOG' entwickelt und im Berichtszeitraum für den Echtbetrieb freigegeben worden. Bei dem Verfahren handelt es sich um eine Client-Server Lösung. Der Server für die zentrale Datenhaltung befindet sich in der ID Bremen. Zugriff auf die Daten erhalten das Amt für Wohnung und Städtebau in Bremen und das Amt für Bauförderung in Bremerhaven über angeschlossene PC. Für die Verbindung der Ämter mit der ID Bremen steht in jedem Amt ein Kommunikationsserver zur Verfügung. Für die Datenübertragung zwischen Magistrat und ID Bremen stehen Datenleitungen der BreKom und der NordKom zur Verfügung, die nur für diese Übermittlungen genutzt werden. Die Erstellung der Bescheide und der Bundes- und Landesstatistiken erfolgt durch ID Bremen.

Bereits vor Inbetriebnahme des Verfahrens habe ich verschiedene Unterlagen zur Stellungnahme erhalten; darunter ein Datenschutz- und Datensicherungskonzept, ein Rollenkonzept, ein Datenmodell

und Tabellenkalkulationen sowie Dienstanweisungen für Bremen und Bremerhaven. Die von mir anhand der Unterlagen angesprochenen Themen, wie z.B. die Aufbewahrung von Protokolldaten und die Aufbewahrungsdauer der Falldaten, wurden in einem Gespräch nach einer Vorführung des Testsystems diskutiert und in die Papiere eingearbeitet. Die Dienstanweisung für Bremerhaven ist bereits mit mir abgestimmt; bei der Dienstanweisung für Bremen steht ein Abschluß kurz bevor.

Zur Zeit erfolgt eine Umstellung der Client-Software auf WindowsNT 4.0. Die sich dadurch ergebenden Änderungen sollen in die Dienstanweisung eingearbeitet werden. Auch Gesetzesänderungen müssen noch in das Verfahren eingearbeitet und das Benutzerhandbuch redaktionell überarbeitet werden.

11.2. Neues DV-Programm für die Erteilung von Berechtigungsscheinen in Bremerhaven

Im Amt für Bauförderung in Bremerhaven ist eine ACCESS-Eigenentwicklung für die softwaregestützte Erteilung von Berechtigungsscheinen bereitgestellt worden. Alle Arbeitsplätze sind im Rahmen einer eigenständigen Containerverwaltung (d. h. die Daten können innerhalb der Organisationsstruktur des Amtes administriert werden) in das Magistratsnetz eingebunden und die zuständigen Sachbearbeiter haben über angeschlossene Clients Zugriff auf die dort gespeicherten Daten. Das Programm wurde mir vorgeführt und ein Datenschutz- sowie Datensicherungskonzept zur Stellungnahme vorgelegt. Verschiedene technische Komponenten waren nicht hinreichend sicher installiert. In der Antwort auf meine Stellungnahme wurde meinen Anregungen Rechnung getragen. Die Sperre von CD-ROM- und Diskettenlaufwerk für die Sachbearbeitungs-PC, der Einsatz von ACCESS-Runtime-Versionen, die Begrenzung der Anmeldeversuche auf drei Anmeldungen und die Festlegung der Löschfrist für archivierte Daten auf 5 Jahre wurden schriftlich zugesagt. Im Konzeptentwurf fehlte auch die Festlegung der Löschzeitpunkte für das Datensicherungsarchiv. Die Einarbeitung der genannten Punkte in die Konzepte, die Erstellung einer Dienstanweisung sowie die Dateibeschreibung sind noch nicht abgeschlossen.

11.3. Datenerhebung beim Antrag auf Fahrerlaubnis

Nach Inkrafttreten des novellierten Straßenverkehrsgesetzes (StVG) und der Fahrerlaubnisverordnung im Jahre 1998 (vgl. 19. JB, Ziff. 14.1) habe ich geprüft, ob die Formulare, die beim Antrag auf Fahrerlaubnis zu verwenden sind, den neuen Vorschriften angepaßt worden sind. Gegen den Umfang der Datenerhebung hatte ich mit Ausnahme der Frage nach der Staatsangehörigkeit keine Einwände. Die Frage ist nicht zulässig, insbesondere weil dieses Datum nicht im abschließenden Katalog des § 50 StVG enthalten ist. Des weiteren habe ich vorgeschlagen, die neuen Rechtsgrundlagen in den von der Behörde herausgegebenen Hinweisen zur Datenerhebung durch die Fahrerlaubnisbehörde und zur Datenübermittlung an das Kraftfahrtbundesamt konkret anzugeben. Denn gemäß § 3 Abs. 2 BrDSG ist der Betroffene auf die Erhebungsvorschrift des § 10 Abs. 4 BrDSG hinzuweisen. Meine Änderungsvorschläge sind inzwischen umgesetzt worden.

11.4. Datenschutzbestimmungen im Bremischen Naturschutzgesetz

Bereits im Jahre 1992 hat mich der damalige Senator für Umweltschutz und Stadtentwicklung darüber unterrichtet, daß er im Rahmen der Novellierung des Bremischen Naturschutzgesetzes (BremNatSchG) bereichsspezifische Datenschutzregelungen vorbereite. Nunmehr sind diese

Regelungen im Ersten Gesetz zur Änderung des BremNatSchG vom 01. Juni 1999 (BremGBl. S. 90) in der Vorschrift des § 48a enthalten.

Nach § 48a Abs. 2 BremNatSchG dürfen die Naturschutzbehörden zur Wahrnehmung ihrer Aufgaben nach diesem Gesetz, dem Bundesnaturschutzgesetz und den aufgrund dieser Gesetze erlassenen Rechtsverordnungen die erforderlichen personenbezogenen Daten erheben und speichern. Es handelt sich dabei vorwiegend um Namen und Anschriften folgender Personengruppen:

- Diejenigen, die bei der Aufstellung des Landschaftsprogramms und der Aufstellung von Landschaftsplänen Bedenken und Anregungen vorgebracht haben,
- Eigentümer und sonstige Nutzungsberechtigte von Grundstücken, auf denen sich besonders geschützte Biotope befinden oder die sich im Geltungsbereich eines Landschaftsplanes, einer landschaftsplanerischen Festsetzung in einem Bebauungsplan u.a. befinden,
- Verursacher von beantragten oder angezeigten Eingriffen im Rahmen eines Verfahrens,
- Grundstückseigentümer und Nutzungsberechtigte von Grundstücken, auf denen die Durchführung von Ausgleichs- und Ersatzmaßnahmen angeordnet ist,
- Mitglieder der unabhängigen Beiräte und ihrer Vertreter sowie Naturschutzwarte zur Unterstützung der Überwachung der Verbote und Gebote nach diesem Gesetz sowie
- Personen, die im Auftrag der Naturschutzbehörden oder der Verursacher von Eingriffen Bestands-erhebungen (Kartierungen) durchführen.

Des weiteren regelt Abs. 3 dieser Vorschrift, daß an Behörden, deren Belange berührt werden, diese Daten auch ohne Kenntnis der Betroffenen nur dann durch Auskunft aus dem Grundbuch, dem Liegenschaftskataster oder dem Altlastenkataster mitgeteilt werden dürfen, soweit es für die genannten gesetzlichen Aufgaben erforderlich ist.

Die Daten können nach § 48a Abs. 4 BremNatSchG an die Behörden, deren Belange berüht werden, übermittelt werden, soweit dies zur Abgabe eigener Stellungnahmen der empfangenden Stelle in den Verfahren zur Aufstellung des Landschaftsprogramms, des Landschaftsplanes oder zum Erlass einer Rechtsverordnung oder zur rechtmäßigen Wahrnehmung von Aufgaben der empfangenden Stelle im Zusammenhang mit eingreifenden Vorhaben erforderlich ist.

Nach § 48a Abs. 1 BremNatSchG gelten im übrigen die Bestimmungen des Bremischen Datenschutzgesetzes. Ich habe zu verschiedenen Gesetzentwürfen mehrfach Stellung genommen; meine Anregungen wurden weitgehend berücksichtigt.

12. Finanzen

12.1. CHIPSMOBIL

Aufgrund des Senatsbeschlusses vom 16.12.97 zur Erneuerung des bremischen Haushalts- Kassen- und Rechnungswesens (HKR) initiierte der Senator für Finanzen das Projekt CHIPSMOBIL (**C**ontolling, **H**aushalt, **I**ntegration, **P**lanung, **S**tandard, **M**odular, **O**nline, **B**uchführung, **I**nformatik, **L**ogistik).

Im Verlauf der ersten Projektphase wurde ein Anforderungsprofil für die erforderliche Software erstellt. Diese Projektphase begleitet ein Fachausschuß. Hier beteiligte ich mich insbesondere an der Beschreibung technischer Datenschutzanforderungen und an der Klärung von Fragen bei der Verarbeitung personenbezogener Daten in einzelnen Kernprozessen.

Durch den Einsatz eines diesem Anforderungsprofil entsprechenden HKR-Verfahrens wird eine hohe Transparenz finanztechnischer Abläufe entstehen. Hauptziel meiner Beratung war es deshalb,

- die Erhebung von personenbezogenen Daten (Mitarbeiter- und Klientendaten) auf ihre Erforderlichkeit für die definierten Ziele des Verfahrens zu prüfen und
- die Zweckbindung dieser Daten technisch sicherzustellen, d.h. insbesondere die Möglichkeit zentraler personenbezogene Auswertungen auszuschließen.

Gemäß dem Anforderungsprofil der vom Senator für Finanzen erstellten Ausschreibung des Verfahrens präsentierten vier Firmen ihre Angebote. Die Präsentationen wurden von mir aufgrund der vorgestellten Datenschutzfeatures nach folgenden Kriterien bewertet:

- Zugangsorganisation auf den Ebenen Betriebssystem, HKR und Datenbank
- Berechtigungskonzept unter den Gesichtspunkten Differenzierungsgrad, Transparenz der Berechtigungsstruktur und Bildung komplexer Strukturen durch Hierarchisierung und Verknüpfung
- Bei den Systemrechten die differenzierte Zuweisungsmöglichkeit von Systemadministratorrechten
- Protokollierungsfunktionen

Meine Einschätzung aller Produkte nach den o.g. Kriterien ergab qualitative Unterschiede in den Ausgestaltungsmöglichkeiten und im Umfang der zur Verfügung gestellten Funktionen. Der Senator für Finanzen entschied sich für eine HKR-Software. Sie enthält nach Darstellung des Herstellers die eben beschriebenen Datenschutzfeatures. Eine als von mir besonders kritisch bewertete Öffnung der Datenbank unterhalb der Berechtigungsstruktur für Reporttools soll bei diesem Produkt nicht möglich sein.

Im weiteren Verfahren ist es nun erforderlich, die Implementierung der durch das ausgewählte neue HKR-Verfahren bereitgestellten Funktionen konzeptionell festzulegen und zu realisieren.

12.2. SEKT

Im letzten Jahresbericht (21. JB, Ziff. 17.4.) habe ich bereits von dem in der bremischen Verwaltung vorangetriebenen Projekt "sichere E-Mail-Kommunikation für den Austausch von Transaktionsdaten" (Abkürzung: SEKT) berichtet. Gegenstand dieser Anwendung ist die verschlüsselte und doppelt-signierte Übertragung von Daten zur Zahlbarmachung von Auszahlungen und zur Entgegennahme von Einnahmen im Verkehr zwischen den einzelnen Haushalts- und Rechnungsstellen in den bremischen Behörden und der Landeshauptkasse (jetzt Performa Nord).

Bei der Konzeption dieses Projektes hatten mich der Senator für Finanzen und das ehemalige TuI-Referat der Senatskommission für das Personalwesen frühzeitig beteiligt. Wie wichtig diese Beteiligung ist, wird besonders deutlich, weil dieses ehrgeizige Projekt auf Grund der hochkomplexen

Sicherheitstools immer noch nicht zur Zufriedenheit läuft. Offensichtlich treten die Schwierigkeiten insbesondere bei den Nutzern auf, die nicht in das eigentliche Verwaltungsnetz integriert sind.

12.3. Unvollständige Aufklärung der Schuldner der LHK

Die Gerichtskasse der Landeshauptkasse (jetzt Performa Nord) ist für die Einziehung von durch Gerichte festgesetzte Forderungen der Freien Hansestadt Bremen zuständig. Um diese Aufgabe zu erledigen, steht ihr ein umfassendes Instrumentarium zur Durchsetzung der Ansprüche zur Verfügung. Sie kann Pfändungs- und Überweisungsbeschlüsse erwirken, Abtretungserklärungen entgegennehmen, die eidesstattliche Versicherung zum Vermögen (gemäß § 807 ZPO) erwirken und Ratenzahlungen und Stundungen mit den Schuldnern vereinbaren. Um ihre Informationsbasis zu verbessern, hat sie u.a. die Möglichkeit unter bestimmten Voraussetzungen Daten von den Sozialleistungsträgern (Sozialämtern und Arbeitsämtern) zu erhalten, um von vornherein auf Zwangsmaßnahmen verzichten oder aber moderate Vereinbarungen treffen zu können. Ein Teil dieser Informationen erhält die Gerichtskasse durch freiwillige Angaben des Schuldners oder mit seiner Zustimmung von Dritten.

Anläßlich einer Prüfung stellte ich fest, daß die Aufklärung der Betroffenen, die einer Offenbarung ihrer Vermögens- und Einkommensverhältnisse zugestimmt haben, unvollständig und zweideutig war. So war für den Erklärenden nicht klar, in was er einwilligt, welche Folgen die Einwilligung hat und welche Alternativen er hat.

In Zusammenarbeit mit den zuständigen Mitarbeitern der Gerichtskasse wird derzeit ein Fragebogensatz und Informationspapier entworfen, die diese Defizite beseitigen. So wird in Zukunft für jeden Betroffenen klar sein, welche Daten die Gerichtskasse bei Dritten abrufen darf, wie lange seine Zustimmung wirkt und welche Folgen eine Offenbarungsverweigerung hat. Mein Hauptanliegen ist dabei, neben einer größtmöglichen Transparenz, auch zu erreichen, daß die Zustimmungserklärung nur solange Wirkung entfaltet, wie es für die Zwecke der Gerichtskasse erforderlich ist.

12.4. Fehlende Datenschutzregelungen in der Abgabenordnung

12.4.1. Abgabenordnung allgemein

Seit Jahren bemühen sich die Datenschutzbeauftragten in Bund und Ländern um eine Verbesserung des Datenschutzes in der Abgabenordnung (AO). Zielrichtung ist dabei, den Bürgern normenklar die vergleichbaren Rechte wie sie das allgemeinene Datenschutzrecht (z. B. Bundesdatenschutzgesetz) garantiert auch zu gewährleisten. Es gibt zwar eine starke Ausprägung des Steuergeheimnisses und eine relativ klare Ausgestaltung der Offenbarungsregelungen bis hin zur Hundesteuer, dennoch ist die Zweckbegrenzung innerhalb der Steuerverwaltung nicht eindeutig beschrieben. Insbesondere enthält die AO keine Regelungen über das Auskunfts- und Akteneinsichtsrecht der Steuerpflichtigen sowie über Aufkärungspflichten der Steuerverwaltung. Ebenso sind keine gesetzlichen Regelungen entwickelt worden, unter welchen Voraussetzungen Daten online verarbeitet werden dürfen. Hier ist der Bundesgesetzgeber gefordert. Die Datenschutzbeauftragten sind sich weitgehend über folgende noch zu erreichende Verbesserungen einig.

12.4.2. Steuerdatenabrufverordnung

§ 30 Abs. 6 AO ist die Ermächtigungsgrundlage für den Erlaß von Verordnungen, die den Abruf (online) von Steuerdaten durch andere Steuerbehörden und andere öffentliche Stellen regeln. Nach mehr als 6 Jahren befindet sich eine derartige Verordnung z. Zt. in der Endphase der Abstimmung in den Erlaßgremien. Dieser lange Zeitraum zeigt, wie unterentwickelt das Datenschutzrecht in der Steuerverwaltung ist. So war ich überrascht, daß die Steuerverwaltung online Abrufmöglichkeiten ohne Verschlüsselung der Daten vornehmen wollte. Ferner sollten die Zugriffsrechte nicht nur individuell sondern auch für Gruppen möglich sein; damit wäre eine Kontrolle der Abrufe unmöglich geworden. Da es beim Erlaß der Verordnung Schwierigkeiten gab, wollte die Steuerverwaltung diese Materie zunächst auf der Grundlage einer Allgemeinen Verwaltungsregelung gestalten.

12.4.3. Online- und Offline-Zugriffe der Steuerverwaltung auf DV-Finanzverwaltungssysteme

Die Entwürfe zum Steuerbereinigungsgesetz und jetzt -da die Änderung in der Beratung des Vermittlungsausschusses nicht konsensfähig war- zum Unternehmenssteuergesetz sahen eine Änderung des § 147 Abs. 6 AO dergestalt vor, daß die Steuerbehörden befugt werden - bei der Steuerprüfung vor Ort - die DV-Systeme der Steuerpflichtigen für ihre Zwecke zu nutzen und Online-Zugriffe auf die Daten der Steuerpflichtigen vom Finanzamt aus durchzuführen.

Gegen diese hier nur skizzenartig beschriebene Regelung haben sich nicht nur die Datenschützer sondern auch viele Verbände und Publikationen ausgesprochen. Nunmehr scheint sich eine Regelung abzuzeichnen, die folgende Festlegungen trifft:

- Nutzung der DV-Systeme der Steuerpflichtigen, nur soweit auf ihnen für die Steuerberechnung relevante Daten gespeichert sind.
- Der Steuerpflichtige selbst oder ein Beauftragter haben das Recht auf Anwesenheit.
- Datenträger dürfen nur mit Zustimmung und Kenntnis des Steuerpflichtigen entnommen werden.
- Online-Zugriffe (mit schriftlicher Einwilligung des Steuerpflichtigen) vom Finanzamt aus, sind nach dem neuen Entwurf nicht mehr vorgesehen.

12.4.4. Regelungen über den Schadensersatz

Es ist eine Vorschrift unerläßlich, die den Schadensersatz bei fehlerhafter Datenverarbeitung und -übermittlung regelt, da gerade im Bereich der Steuer durch Datenverarbeitungsfehler, für den Steuerpflichtigen Schaden entstehen kann.

12.4.5. Regelungen über die Berichtigung bzw. die Sperre von Daten

Ebenso ist eine Vorschrift erforderlich, die die Steuerverwaltung verpflichtet, unrichtige Daten zu berichtigen und nicht beweisbare Daten, die der Steuerpflichtige bestreitet, für eine weitere Nutzung durch die Steuerverwaltung zu sperren.

12.4.6. Erteilung von Teilauszügen aus den Steuerbescheiden

In der Vergangenheit hat sich immer wieder gezeigt, daß die bei vielen Stellen vorzulegenden Steuerbescheide (z. B.: zur Festsetzung des Kindergartenbeitrages, zur Berechnung des BAFÖG oder

zur Festsetzung des Wohngeldes) Daten des Betroffenen oder von Dritten (nichtunterhaltspflichtiger Ehepartner) enthalten, die für diese Berechnungsstellen nicht benötigt werden. Deshalb sollte die Möglichkeit eröffnet werden, daß entsprechend reduzierte Auszüge vom Steuerpflichtigen angefordert werden können.

12.4.7. Regelung über die Anonymisierung von Daten nach § 88a AO

Nach § 88a AO sind die Steuerbehörden befugt, Daten zu erheben, die lediglich Vergleichszwecken dienen. Diese Daten werden nicht konkret für ein Steuerverfahren benötigt und sollten deshalb nach Aufnahme in das Vergleichs- oder Auswertungprogramm unverzüglich anonymisiert werden.

12.4.8. Fazit

Diese vorgenannten Beispiele zeigen, wie notwendig eine datenschutzrechtliche Anpassung der AO ist, um normenklar und verfassungskonform den Datenschutz in der Steuerverwaltung zu gewährleisten.

12.5. Vollstreckung

Die zentrale Vollstreckungsstelle der Finanzämter in Bremen hat u. a. auch das Recht, Forderungen, die ein Steuerschuldner gegenüber Dritten hat, zu pfänden. Bei der Durchführung sind verschiedene Datenschutzprobleme aufgetaucht, auf die ich von Drittschuldnern hingewiesen wurde. So waren der Briefumschlag und die beigefügte Empfangsbekenntnis so ausgestaltet, daß von außen erkennbar war, daß es sich um eine Zwangsvollstreckungsmaßnahme handelte. Ich habe erreichen können, daß die Kennzeichnung der Zustellungsurkunde so gestaltet wurde, daß Außenstehende nicht mehr auf die Maßnahme schließen können.

13. Wirtschaft und Häfen

13.1. Neue Schlachte

Mit Förderung des Senator für Wirtschaft und Häfen wurde die „Neue Schlachte" erstellt. Wie diese Förderungsmaßnahme von den Bremern und Bürgern im Umland aufgenommen wurde, wollte die Behörde durch eine Telefonumfrage ermitteln. Ferner sollte der Bekanntheitsgrad und die Attraktivität der "Neuen Schlachte" festgestellt und Verbesserungsvorschläge aufgegriffen werden. Mit der Durchführung wurde ein Call-Center beauftragt.

Schon bei der Konzeption der Telefonumfrage hat mich der Senator für Wirtschaft und Häfen beteiligt. Dabei habe ich ihn auf die wesentlichen Punkte, die bei einer solchen Umfrage aus datenschutzrechtlicher Sicht zu beachten sind, hingewiesen: Die Datenerhebung wurde auf freiwilliger Grundlage gem. § 3 Abs. 1 Nr. 2 BrDSG durchgeführt. Der Fragenkatalog wurde durch den Auftraggeber eindeutig festgelegt und der Kreis der Befragten sollte mittels eines Zufallsgenerators ausgewählt werden. Es wurde auch festgelegt wie zu verfahren sei, falls einer der Interviewten Kontakt zur Behörde wünschen würde. Das Call-Center wurde -nach sorgfältiger Auswahl- durch schriftlichen Vertrag gemäß §9 BrDSG beauftragt. Es hat sich meiner Kontrolle unterworfen. An Hand des Fragenkataloges wurden vom Call-Center die Antworten der Bürgerinnen anonym erfaßt, aufbereitet und ausgewertet an den Senator für Wirtschaft und Häfen weitergeleitet. Die Ergebnisse der Telefonbefragung wurden in anonymer Form veröffentlicht.

Durch meine frühe Beteiligung konnte eine datenschutzrechtlich unbedenkliche Meinungsumfrage durchgeführt werden.

13.2. BrePos und der Anschluß privater Stellen

Beim Hansestadt Bremischen Hafenamt wurde auch im vergangenen Jahr an einer Fortentwicklung des Programms BrePOS (Bremen Port Operating System) gearbeitet. Dieses Programm beruht auf entsprechenden Vorschriften im Hafengesetz und der Hafenordnung und bündelt die mit der Verkehrslenkung, der Versorgung, der Sicherheit und der Abrechnung der verschiedenen Gebühren von Schiffen, Ladung und Containern im Hafen erforderlichen Daten. Meine Beteiligung war über die Jahre sichergestellt. Über BrePOS berichtete ich bereits (vgl. 14 JB, Ziff. 2.9).

Im Dezember 1999 wurde zwischen den für das Programm Verantwortlichen und mir festgelegt, daß die reinen Verkehrsdaten der Schiffe ohne Personenbezug auch an Lotsen, Festmacher und Schlepperfirmen weitergeben werden dürfen, damit sie bei der Abfertigung der Schiffe mit verläßlichen und aktuellen Daten ihre Aquisition vornehmen und ihre Arbeit erledigen können.

14. Bremerhaven

14.1. Rechnungsprüfungsamt Bremerhaven

14.1.1. Anforderung von Sozial- und Ausländerakten durch das Rechnungsprüfungsamt

Durch eine Eingabe und andere Hinweise wurde ich davon unterrichtet, daß das Rechnungsprüfungsamt Bremerhaven jeweils eine gezielte Akte der Ausländer- und der Sozialbehörden einer bestimmten Person angefordert hatte. Diese Anforderungen erfolgten auf der Grundlage der Rechnungsprüfungsordnung der Stadt Bremerhaven (§ 7).

Dabei fiel den Hinweisgebern auf, daß bei der gezielt angeforderten Ausländerakte keinerlei haushaltsrechtliche Vorschriften zu prüfen waren, so daß Anlaß zur Befürchtung bestand, daß eine Nutzung der Daten außerhalb der Zuständigkeit des Rechnungsprüfungsamtes nicht ausgeschlossen werden konnte. Noch eindeutiger war der Fall bei der Anforderung der Sozialakte. Für die Prüfung dieser Ausgaben ist der Bundesrechnungshof zuständig und es ist auch nicht bekannt, daß er diese Zuständigkeit auf das Rechnungsprüfungsamt abgetreten hat. Es war mithin nicht erkennbar, zu welchem Prüfzweck das Rechnungsprüfungsamt die beiden Akten benötigt. Für eine Wirtschaftlichkeitsuntersuchung des Verwaltungshandelns in der Ausländer- oder der Sozialbehörde - für die das Rechnungsprüfungsamt zuständig ist - erscheinen jedenfalls zwei einzelne Akten ungeeignet.

Da für die Aktenherausgabe der Magistrat zuständig ist, habe ich ihm meine Stellungnahme zugesandt und ihn gebeten, die Erforderlichkeitsprüfungen in eigener Zuständigkeit zu klären.

14.1.2. Änderungsvorschläge zur Rechnungsprüfungsordnung der Stadt Bremerhaven

Die Befugnisse des Rechnungsprüfungsamtes der Stadt Bremerhaven sind in der Rechnungsprüfungsordnung geregelt. Diese Befugnisse entsprechen im wesentlichen denen des Rechnungshofes der Freien Hansestadt Bremen und haben ihre Ermächtigung in der Landeshaushaltsordnung.

Nunmehr hat der Leiter des Rechnungsprüfungsamtes dem Magistrat einen Entwurf zur Änderung der Rechnungsprüfungsordnung vorgelegt. Ich habe aus datenschutzrechtlicher Sicht u. a. zu folgenden Punkten Stellung genommen.

- Online-Abrufe durch das Rechnungsprüfungsamt auf DV-Verfahren der Verwaltung:

  Der Entwurf sah ein schrankenloses und ungeregeltes Abrufrecht für das Rechnungsprüfungsamt auf elektronisch geführte Daten der Bremerhavener Verwaltung vor. Hier habe ich auf die eindeutige Vorschrift im Bremischen Datenschutzgesetz (§ 14) hingewiesen, die präzise festlegt, für welche Zwecke, in welchem Umfang, unter welchen Voraussetzungen und Sicherheitsvorkehrungen Abrufverfahren eingerichtet werden dürfen.

- Prüfungsrecht in Unternehmen, an denen die Stadt Bremerhaven beteiligt ist:

  Eine solche Vorschrift wäre eine wesentliche Erweiterung der Prüfrechte in den Unternehmen. Die entsprechende Vorschrift in der Landeshaushaltsordnung (§ 92) läßt keine Prüfung im Betrieb zu, sondern nur eine Prüfung, ob die Betätigung der öffentlichen Hand im Rahmen des öffentlichen Rechts als Aufgabe der Verwaltung wirtschaftlich zu rechtfertigen ist.

- Durchsuchungsrecht für das Rechnungsprüfungsamt in den Amtsstuben:
  Sehr erstaunt war ich hinsichtlich eines in dem Entwurf vorgesehenen Durchsuchungsrecht für das Rechnungsprüfungsamt. Dieses Recht sollte die Befugnis zur Durchsuchung von Schreibtischen, Schränken und sonstigen Behältnissen durch das Rechnungsprüfungsamt eröffnen. Abgesehen davon, daß ein solches Recht in der Landeshaushaltsordnung nicht vorgesehen ist, habe ich auch Zweifel, ob dieses der Aufgabenstellung des Rechnungsprüfungsamtes entspricht, das insbesondere die Rechnung der Verwaltung, das Vermögen und die Schulden sowie die Wirtschaftlichkeit der Verwaltung zu prüfen hat. Dabei greift es auf die entsprechenden Belege und Bücher zurück, die von der Verwaltung vorzulegen sind.

Da ich bisher keinen Fortgang in der Sache feststellen konnte, gehe ich davon aus, daß die Novellierung insoweit nicht weiterverfolgt wird.

14.2. Stadtkämmerei Bremerhaven: Neues DV-Verfahren "Haushalts- und Kassenwesen"

Im Rahmen eines Projektes wird aus verschiedenen Gründen (z. B. 2000-Problem) die DV-Landschaft beim Magistrat der Stadt Bremerhaven in einzelnen Schritten von einer Host-Anwendung auf eine Clint-Server-Lösung umgestellt. Bei der Gestaltung dieses ehrgeizigen Projektes bin ich von Anfang an beteiligt worden. Die Umstellung betrifft auch das Haushalts- und Kassenwesen, das maßgeblich von der Stadtkämmerei betrieben wird. Ich habe bei dem Projekt CHIPSMOBIL in Bremen (vgl. Ziff. 15.1) in entsprechendem Zusammenhang darauf hingewirkt, eine Software auszuwählen, die die Zugriffsrechte klar abgrenzen und die Rechteverwaltung transparent gestalten kann sowie die Nutzung protokolliert. Das Projekt scheint sich insgesamt auf einem guten Weg zu befinden.

Von der eben beschriebenen Umstellung sind auch andere DV-Verfahren innerhalb der Ortspolizeibehörde betroffen. In Teilprojekten werden z. B. die folgenden Verfahren umgestellt:

- Einwohnermeldewesen,
- Kfz-Zulassung,
- Führerscheine
- Ausländerangelegenheiten und
- Ordnungswidrigkeiten.

Alle diese Teilprojekte habe ich neben anderen Verfahren datenschutzrechtlich begleitet, auch wenn es nicht immer möglich war, die Verwaltung in allen Verfahren mit gleich hoher Intensivität zu beraten.

In einigen Fällen war die neue, anwenderfreundliche Software im wesentlichen in die bisherigen Anwendungen zu implementieren. Dennoch gab es an verschiedenen Punkten Gestaltungsbedarf, insbesondere auf der Netzstrukturebene. Hinsichtlich der Administration, der Zugriffsrechte und der Protokollierung waren Festlegungen zu treffen. Einige dieser Anwendungen befinden sich noch in der Pilotphase, andere bereits im Echtbetrieb.

14.3. Verweisungen

Weitere Themen aus Bremerhaven betreffen, finden sich unter der Ziff. 5.1. (Erhebung und Führung von Personaldaten), Ziff. 6.3.2. (Meldedaten an politische Parteien), Ziff. 6.3.3 (DV-Verfahren Einwohnermeldewesen), Ziff. 10.2. (Jugendkriminalität an Schulen), Ziff. 11.1. (Neues Wohngeldverfahren), Ziff. 11.2. (Neues DV-Programm für die Erteilung von Berechtigungsscheinen) und für den nicht-öffentlichen Bereich unter Ziff. 16.7.6. (Auskunfteien) dieses Jahresberichts.

15. Handels- und Handwerkskammer

15.1. Datenabgleich über Ausbildungsverhältnisse mit den Arbeitsämtern

Die Bundesanstalt für Arbeit (Berufsberatung) hat mit dem Deutschen Industrie- und Handelstag bzw. dem Handwerkskammertag 1998 Vereinbarungen über den Abgleich von Daten über eingetragene Ausbildungsverhältnisse geschlossen. Durch eine Eingabe bin ich auf die beiden Vereinbarungen aufmerksam gemacht worden.

Meine Anfrage bei der Handwerkskammer und der Handelskammer Bremen hat ergeben, daß beide Kammern keine Rechtsgrundlagen für die geplanten Datenabgleiche erkennen können und sich daher an dem Datenaustausch nicht beteiligt haben. Auf Intervention des Bundesbeauftragten für den Datenschutz bei der Bundesanstalt für Arbeit wurde die Aktion bundesweit nicht weiterverfolgt. Beide Kammern brachten bei ihrer Antwort an mich zum Ausdruck, daß sie die Idee für geeignet halten und sie sich in einem rechtlich zulässigen Rahmen beteiligen würden. Soll das Projekt also weiterverfolgt werden, wäre zunächst der Bundesgesetzgeber aufgerufen, die Voraussetzungen für einen Datenaustausch zu schaffen.

16. Datenschutz in der Privatwirtschaft

16.1. Video-Überwachung in Großwohnanlagen

Ein Wohnungsunternehmen beabsichtigt, zur Verhinderung bzw. Verringerung von Sachbeschädigungen (z. B. Brände in Tiefgaragen, Beschmierungen und Zerstörungen in Eingangsbereichen) ihre Großwohnanlagen mit Videokameras zu überwachen. Sie hat mich unter

Datenschutzgesichtspunkten gebeten, die Zulässigkeit einer derartigen Videoüberwachung zu bewerten. Dazu hat sie mir ein digitales Videosystem vorgeführt, das von einem Sicherheitsdienst eingesetzt werden soll.

Die Demonstration hat deutlich gemacht, daß Überwachungsanlagen dieser Qualität in der Lage sind, Bilder und Ausschnitte von nicht gekannter und nicht erwarteter Güte und Präzision zu liefern. Das erschwert u. a. die Aufklärung der Betroffenen erheblich, denn ein bloßer Hinweis darauf, daß ein gewisser Bereich videoüberwacht wird, würde bei den Betroffenen keineswegs die Vorstellung entstehen lassen, daß mit derartiger Präzision und Erfassungstiefe gearbeitet werden kann, wie sie in der Vorführung vorgestellt worden ist.

Die Vorführung mit den vielfältigen technischen Möglichkeiten, wie z. B. die Alarmschaltung, die Voralarmschaltung, die digitale Bildbearbeitung, die Aufhellung dem bloßen Auge als dunkler Bereich nicht erkennbarer Ausschnitte, der um 360° rundum schwenkbare Überwachungsausschnitt oder der beeindruckende Zoombereich, haben deutlich gezeigt, wie intensiv die Überwachung eines Lebensbereiches werden kann.

Bedenkt man die Reaktionen der Bevölkerung auf die beabsichtigte Durchführung einer Volkszählung im Jahre 1983, so sind entsprechend heftige Reaktionen gegenüber dieser Technik nicht auszuschließen, wenn den Betroffenen bekannt wird, wie total und genau eine solche Videoüberwachungsanlage rund um die Uhr alle menschlichen Verhaltensweisen in ihrem Erfassungsbereich erheben und festhalten kann. Denn auch – wie im Falle der Volkszählung – geht es bei der Videoüberwachung um einen Eingriff in das grundrechtlich geschützte informationelle Selbstbestimmungsrecht der von der Videoüberwachung Betroffenen.

Wie sieht nun die Rechtslage aus? In dem Moment, in dem Bilder auf Dauer gespeichert und nach bestimmten Kriterien personenbezogen ausgewertet werden können, wie z. B. eine Serie von Kfz-Kennzeichen, Bilder von Hauseingängen mit Hausnummern und Bewohnern o. ä. wäre auf solche Sammlungen das Bundesdatenschutzgesetz (BDSG) anzuwenden. Diese Fragen sind unmittelbar verknüpft mit der Form und Dauer der Speicherung, der systematischen Sammlung von Bildern und den Möglichkeiten der Auswertung. Angesichts der vielfältigen und intensiven Möglichkeiten der Überwachung, die das vorgeführte System bietet, würde es den tatsächlichen Umständen aber nicht gerecht, wenn man auf alle Vorgänge die allgemeinen Bestimmungen des BDSG anwenden würde. Das BDSG ist bisher weder den neuen Bedingungen angepaßt worden, die die EU-Datenschutz-Richtlinie setzt, noch hat der Gesetzgeber bei Erlaß dieser Vorschriften jemals auch nur im entferntesten an die dramatische technische Weiterentwicklung im Videobereich und die Verknüpfung dieser Technik mit einem Computer sowie an die Möglichkeiten moderner Bildbe- und -verarbeitung gedacht.

Eine rechtliche Gestaltung des Einsatzes derartiger Videotechnik kann daher datenschutzrechtlich nur in einer bereichsspezifischen Regelung getroffen werden. Eine rudimentäre Regelung ist diesbezüglich mit § 6b BDSG-Novelle in Diskussion.

Weiter verbleibt die Verpflichtung des Wohnungsunternehmens, das allgemeine Persönlichkeitsrecht, insbesondere das Recht am eigenen Bild der betroffenen Dritten (z. B. Besucher) wie der Mieter zu

wahren (z. B. §§ 242, 823 und 1004 BGB und § 22 KunstUrhG). Diese Regelungen sind jedoch nicht so präzise, daß sie eine klare Einschätzung zulassen, ob der Einsatz der vorgeführten Technik rechtlich zulässig wäre. Es gibt zwar Rechtsprechung zur Anwendung einfacher Videotechnik mit analoger Aufzeichnung, nach der der Einsatz solcher Videotechnik zum Schutz des eigenen Grundstücks in seinen Grenzen akzeptiert wird. Ich habe aber Zweifel, ob diese unmittelbar auf das in der Vorführung verwendete Gerät mit seinen vielfältigen technischen Möglichkeiten übertragen werden kann. Zum einen geht der öffentlich gewidmete Raum nahtlos über in die im Eigentum des Wohnungsunternehmens stehenden Zuwegungen und Flächen. Anders als die nachbarlich durch Zäune und Pforten abgegrenzten Grundstücksflächen von Einfamilienhäusern stellen die vom Wohnungsunternehmen gehaltenen Flächen quasi öffentliche Flächen dar, weil sie jedermann zugänglich sind. Aber auch die bei der Vorführung verwendete Technik ist keinesfalls mit der von der Rechtsprechung bewerteten herkömmlich eingesetzten Videotechnik mit festen Brennweiten und analoger Aufzeichnung vergleichbar.

Der BGH formuliert in einem Urteil vom 25.04.1995 (Az.: VI ZR 272/94 (KG)), daß auch die Herstellung von Bildnissen einer Person, insbesondere die Filmaufzeichnung mittels Videogerät, in der Öffentlichkeit zugänglichen Bereichen auch ohne Verbreitungsabsicht einen unzulässigen Eingriff in das Persönlichkeitsrecht des Betroffenen darstellt. Im vom BGH entschiedenen Fall überwachte ein Hauseigentümer gezielt und regelmäßig ein bestimmtes Stück eines öffentlichen Weges über längere Zeiträume. Die Überwachung war darauf angelegt, Benutzer des Weges in einer Vielzahl von Fällen abzubilden und aufzuzeichnen. Dabei sei es um den Zugangsweg zu Wohngrundstücken, darunter demjenigen der Kläger, gegangen.

Der BGH weist in diesem Zusammenhang darauf hin, daß die Kläger der Videoaufnahme nicht ausweichen können, wenn sie sich auf dem Weg von oder zu ihrem Grundstück befinden. Die Kläger können weder beeinflussen, wann sie bei solchen Gelegenheiten aufgenommen werden, noch können sie feststellen, ob solche Aufzeichnungen gefertigt worden sind oder nicht. Sie müssten daher, wenn sie den Weg benutzen, ständig mit der der Überwachung dienenden Aufzeichnung ihres Bildes rechnen.

Der BGH stellt daher fest, daß derartige Maßnahmen eine **schwerwiegende** Beeinträchtigung des allgemeinen Persönlichkeitsrechts der Kläger bewirken. Denn diese müssen sich praktisch stets, wenn sie von ihrem Haus kommend oder zu ihrem Haus gehend den öffentlichen Zugangsweg benutzen, in einer jede ihrer Bewegung geradezu dokumentierenden Weise kontrolliert fühlen. Auf dem jeweiligen Videofilm ist nicht nur festgehalten, wann, wie oft und in welcher Begleitung sie den Weg begangen haben, sondern auch in welcher Stimmung, mit welchem Gesichtsausdruck etc. sie dies getan haben. Die hierin liegende Beeinträchtigung der Kläger werde nicht dadurch gemindert, daß die beklagte Partei die Videoaufzeichnung nach Überprüfung wieder lösche.

Diee BGH-Entscheidung macht deutlich, daß die Installation und Inbetriebnahme der vorgeführten Videoüberwachungsanlage mit erheblichen rechtlichen Risiken verbunden ist, solange der Gesetzgeber keine klaren Vorgaben gemacht hat, unter welchen Bedingungen und in welchem Umfange zum Schutze anderer Rechtsgüter in die allgemeinen Persönlichkeitsrechte Dritter eingegriffen werden darf. Angesichts dieser Rechtslage habe ich das Wohnungsunternehmen

gebeten, noch einmal zu überprüfen, ob eine derartige Videoüberwachungsanlage eingeführt werden soll, oder ob nicht andere, weniger gravierende Maßnahmen zum Schutze der Anlagen des Wohnungsunternehmens und zur Sicherheit der Bewohner getroffen werden können.

Sollte sie sich dennoch für den Einsatz einer solchen Videoüberwachungsanlage entscheiden, würden die rechtlichen Bedenken gegen den Einsatz einer solchen Anlage jedenfalls in dem Maße geringer, als die Überwachungsanlage durch technische Vorwahl so ausgestaltet würde, daß zwar Personen an sich und deren Handlungen über den Bildschirm wahrnehmbar wären, die einzelne Identität der Personen aber nicht individualisiert und personenbeziehbar erkannt werden kann. Ebenso sollte das System so voreingestellt sein, daß nach sehr kurzen Intervallen die gespeicherten Bildsequenzen, die keinen Grund zum Einschreiten der Sicherheitskräfte geben, überschrieben oder gelöscht werden. Bereits eine so eingestellte Anlage würde es dem Sicherheitsdienst ermöglichen, sein Personal zu erkannten Brennpunkten zu beordern. Soweit Bilder zu Beweiszwecken weiter gespeichert bleiben sollen, sind Regelungen zur Zweckbindung, zum Zugriffsschutz und Befugnisse der Herausgabe an Dritte festzulegen.

Außerdem konnte man durch den Standort der Probeinstallation hoch über den Dächern der Wohnanlage schräg nach unten in alle Fenster der umliegenden Wohnungen blicken und zwar auch der hochgelegenen Stockwerke. Ich habe daher darauf hingewiesen, daß eine Wohnraumüberwachung ebenso wenig in Betracht kommen kann, wie die Überwachung öffentlicher, nicht im Eigentum des Wohnungsunternehmens stehender Flächen. Ich habe aber auch deutlich gemacht, daß ich keine Bedenken habe, wenn nach Anbringung entsprechender Hinweisschilder die im Eigentum des Wohnungsbauunternehmens befindliche Tiefgarage videoüberwacht würde.

Inzwischen hat eine von dieser beabsichtigten Videoüberwachung betroffene Stadtteilgruppe darüber öffentlich diskutiert. Das Wohnungsunternehmen hat zudem erklärt, vor dem Einsatz des Videosystems ein Konzept vorzulegen und mit mir abzustimmen.

16.2. Mithören und Aufzeichnen von Telefongesprächen in Call-Centern

Ein Call-Center hat mich um rechtliche Beratung zur Frage der Zulässigkeit des Mithörens und Aufzeichnens von geschäftlichen Telefongesprächen mit Kunden gebeten. Den Angaben zufolge sollten per Zufall ausgewählte Telefongespräche aufgezeichnet werden. Diese sollten dann von den jeweiligen Mitarbeitern und ihren direkten Vorgesetzten angehört werden, um den Trainingsbedarf der Beschäftigten zu analysieren oder direkte Hilfestellungen zu besprechen. Außerdem sitzen in der Einarbeitungsphase erfahrene Mitarbeiter bei den neuen Mitarbeitern, um Gesprächsabläufe mitzuhören.

Ich habe dem Call-Center mitgeteilt, daß das Aufzeichnen von Telefongesprächen strafbar ist, soweit dieses unbefugt im Sinne des § 201 Abs. 1 Strafgesetzbuches (StGB) erfolgt. Danach wird das unbefugte Aufnehmen des nichtöffentlich gesprochenen Wortes eines anderen auf einem Tonträger mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe geahndet. Eine Befugnis zum Aufzeichen von Telefonaufzeichnungen durch das Call-Center besteht nur dann, wenn die jeweiligen Gesprächsteilnehmer, also die Kunden und die Beschäftigten, hierin eingewilligt haben oder eine gesetzliche Erlaubnis vorliegt.

Die Absicht des Call-Centers, im Zusammenhang mit der Veröffentlichung der Service-Telefonnummern etwaige Kunden auf die Aufzeichnung eingehender Kundengespräche hinzuweisen, kann nicht als wirksame Einwilligung durch den Kunden gewertet werden. Auch eine vertragliche Einwilligungserklärung der Beschäftigten könnte unwirksam sein, weil die Einwilligung offensichtlich aufgrund des Abhängigkeitsverhältnisses des Mitarbeiters zu seinem Arbeitgeber unter faktischem Zwang und demnach nicht ohne jeden Zweifel erteilt wird.

Da eine gesetzliche Erlaubnis für eine Gesprächsaufzeichnung nicht vorliegt, habe ich dem Call-Center erklärt, daß das Aufzeichnen der Telefongespräche unzulässig ist und gebeten, diese Praxis unverzüglich einzustellen. Dies ist mir inzwischen bestätigt worden.

Eine andere Rechtslage ergibt sich beim Mithören bzw. Abhören von Telefongesprächen. Gemäß § 201 Abs. 2 Satz 1 StGB wird zwar bestraft, wer unbefugt das nicht zu seiner Kenntnis bestimmte nichtöffentliche Wort eines anderen mit einem Abhörgerät aufzeichnet. Allerdings hat der Bundesgerichtshof in seinem Urteil vom 08.Oktober 1993 (2 StR 400/93) ausgeführt, zu den Abhörgeräten im Sinne des § 201 Abs. 2 Satz 1 StGB zählten übliche und von der Post zugelassene Mithöreinrichtungen nicht. Ein strafbares Abhören liegt demnach nicht vor, soweit es sich nur um derartige Mithöreinrichtungen handelt. Da in dem Call-Center offensichtlich nur die vorgenannten Mithöreinrichtungen eingesetzt werden, ist das Mithören von Telefongesprächen zwar möglich, es ist aber nur unter Beachtung der nachstehenden Voraussetzungen zulässig:

Es darf keine permanente Überwachung der Arbeitnehmer stattfinden und sie darf nicht heimlich erfolgen. Auch das Bundesarbeitsgericht hat mit Urteil vom 30.08.1995 (Az: 1 ABR 4/95) zu einem ähnlich gelagerten Fall entschieden, daß keine Bedenken gegen das Mithören von geschäftlichen Telefongesprächen in der Einarbeitungsphase der neuen Mitarbeiter bestehen, soweit dies zur Wahrung der berechtigten Interessen des Arbeitgebers sowie im Rahmen der Zweckbestimmung der Arbeitsvertragsverhältnisse erforderlich ist und kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Interessen der Kunden oder Arbeitnehmer beeinträchtigt werden.

Ich habe daher angeregt, das Verfahren bei dem Call-Center im Einzelnen festzulegen und betriebsintern zu veröffentlichen. Außerdem habe ich geraten, die Kunden darüber zu informieren, zumindest mit der Veröffentlichgung der Service-Nummern auf Werbeplakaten oder in Anzeigen.

Die betriebliche Datenschutzbeauftragte hat mir zwischenzeitlich mitgeteilt, daß entsprechend meinen Vorschlägen gehandelt wurde. Auch eine Delegation des Datenschutzausschusses der Bremischen Bürgerschaft hat sich aufgrund von Berichten in den Medien interessiert und dem Unternehmen einen Besuch abgestattet.

16.3. Vernichtung von Bewerbungsunterlagen

Im Berichtszeitraum sind zweimal Personalunterlagen in Müllcontainern geworfen worden, die somit jedermann zugänglich wurden. Die Unterlagen haben mir durch aufmerksame Bürger ausgehändigt.

In einem Fall handelte es sich um Unterlagen offensichtlich abgewiesener Bewerber, die u. a. Lebensläufe und beglaubigte Kopien von Zeugnissen der Betroffenen enthielten. Ich habe die Unterlagen den Betroffenen zugesandt mit dem Hinweis, daß ich den verantwortlichen Arbeitgeber

(einen Hotelbetrieb) auf die Missachtung der Vertraulichkeit von Personalunterlagen hingewiesen habe.

Ein anderer Fall betraf Personalunterlagen aus den Jahren 1988 bis 1993 (Lebensläufe, sonstige Bewerbungsunterlagen und von Beschäftigten unterzeichnete Erklärungen über erhaltene Trinkgelder usw.). Da die Anschriften der Betroffenen nicht vorhanden waren, habe ich die verantwortliche Arbeitgeberin (eine Friseurmeisterin) aufgefordert, die Unterlagen bei mir abzuholen, ordnungsgemäß zu entsorgen und mir die datenschutzgerechte Vernichtung der Unterlagen schriftlich zu bestätigen, was inzwischen geschehen ist.

16.4. Offenbarung von Paßwörtern durch einen Provider

Am Anfang des Jahres wurde ich durch mehrere Anrufe darauf aufmerksam, daß ein Bremer Internet-Provider, der ein besonders günstiges Angebot veröffentlicht hatte, mit den Daten der Interessenten nicht korrekt umging. Dieser Provider hatte die Bestellungen für seinen Dienst u. a. über das Internet entgegen genommen.

Dieses ist für sich gesehen nicht problematisch, wenn entsprechende Sicherheitsvorkehrungen getroffen werden. Die technische Gestaltung in diesem Fall war –auf Grund mangelnder DV-Kenntnisse- äußerst mangelhaft. So konnten andere Interessenten die Namen, Anschriften, Bankverbindungen und Paßworte der Interessenten auf dem Rechner des Providers auslesen.

Bei einer Prüfung vor Ort konnte ich nur noch feststellen, daß der Verantwortliche des Dienstes durch andere Nutzer bereits auf den Fehler aufmerksam gemacht worden war. Er hatte seinen Server bereits stillgelegt und einen anderen Betreiber mit Sitz in Süddeutschland mit diesem Dienst beauftragt. Ich habe ihn daraufhin aufgefordert, alle Online-Anmelder über das Sicherheitsleck zu informieren, da durch die offenbarten Paßworte natürlich weitere Gefahren für die Kunden auftreten können, da viele Nutzer nicht für jeden Dienst ein eigenes Passwort verwenden. Inwieweit späterhin durch das Sicherheitsleck Kunden, z. B. durch Mißbrauch der Kreditkartennummer, tatsächlich ein Schaden entstanden ist, habe ich nicht verfolgen können.

16.5. Datenverarbeitung im Verein

In jedem Jahr erreichen mich viele Nachfragen von Vereinen und Clubs. Es wird die Frage gestellt, wie der Datenschutz im Verein richtig gestaltet wird oder ob der Vereinsvorstand durch diese oder jene Mitteilung an Trainer oder Vereinsmitglieder nicht gegen den Datenschutz verstoßen habe. Es kommen sehr viele Fragestellungen verschiedenenster Natur. So will der eine Vereinsvorstand wissen, ob er die Daten der Mitglieder an eine Versicherung weitergeben darf, die gleichzeitig die Haftpflichtversicherung für die sportlichen Aktivitäten übernommen hat, aber auch den einzelnen Mitgliedern individuelle Versicherungsangebote unterbreiten will. Oder aber ein Wassersportverein fragt nach, ob er die zum Arbeitsdienst“ eingesetzten Vereinsmitgliederdaten veröffentlichen (Aushang, Vereinsblatt usw.) darf. Oder ein anderer will wissen, ob die Geburtstage im Vereinsblatt veröffentlicht werden dürfen.

Die meisten Fragen betreffen jedoch die ordnungsgemäße Sicherung der Vereinsmitgliederdaten und der Vereinsprotokolle. Da diese Unterlagen häufig in den häuslichen Bereichen der Vorstände

aufbewahrt werden, bekommt einer ordnungsgemäßen Datensicherung eine besondere Bedeutung zu. Da viele dieser Fragen auch bei anderen Kollegen immer wieder eine Rolle spielen, haben die Datenschutzbeauftragten im Internet einen Leitfaden veröffentlicht, der unter www.datenschutz.de abgerufen werden kann. Gegen Übersendung eines frankierten und rückadressierten Briefumschlages versende ich den Leitfaden aber auch auf Diskette an interessierte Vereine.

16.6. Ticket-Service kann Daten nicht löschen

Ein Ehepaar aus Bremen hatte telefonisch Eintrittskarten für ein Konzert in der Glocke bestellt. Bei dieser Bestellung wurden die persönlichen Daten wie Name, Adresse, Telefonnummer abgefragt und in einer Bestelldatei abgespeichert. Als das Ehepaar ein paar Tage später die Karten beim Ticket-Center abholte, mußte es sich mit einer Bestellnummer identifizieren, und die Karten wurden ausgedruckt. Auf die Frage, was denn jetzt mit den Daten passieren würde, wurde dem Ehepaar geantwortet, daß die Daten gespeichert blieben. Auf den Einwand, daß man nicht weiter in dieser Datei gespeichert werden möchte, wurde geantwortet, man könne diesen Datensatz gar nicht löschen. Das Ehepaar hat sich darauf hin an mich gewandt.

Ich habe mich mit dem Kartenvorverkaufsunternehmen in Verbindung gesetzt, das im wesentlichen die Angaben der Beschwerdeführer bestätigte. Allerdings wurde zugesichert, daß man sich im vorliegenden Fall um eine Einzellöschung der Daten der Beschwerdeführer kümmern wolle. Insgesamt aber sei es nicht möglich, routinemäßig Daten aus dem System zu löschen. Das System werde in vielen Großstädten der Bundesrepublik eingesetzt, der Softwareanbieter habe jedoch noch kein entsprechendes Löschprogramm entwickelt. Es sei allerdings nunmehr beabsichtigt, ein entsprechendes Programmmodul aufzulegen. Ich habe das Unternehmen auf § 35 BDSG hingewiesen, nach dem personenbezogene Daten, die für eigene Zwecke verarbeitet werden, zu löschen sind, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Deshalb ist das Unternehmen gehalten, nicht nur auf Wunsch eines Kunden, sondern per Gesetz generell verpflichtet, nach Abwicklung und vollständiger Bezahlung die Daten von Kunden zu löschen. Weiter habe ich den Hinweis auf Softwareprogramme anderer Sparten gegeben, die routinemäßige Löschfristen nach gewissen Zeitabläufen vorsehen. Im übrigen würde dadurch eine arbeitsaufwendige Einzelfalllösung, die jeweils manuell angestoßen werden muß, vermieden. Der Zeitablauf bestimmt sich nach den für das jeweilige Geschäft üblichen Usancen. Ist also z. B. in einem Geschäftsbereich zu erwarten, daß es zu einem regelmäßigen Geschäftskontakt kommt, könnte die Software vorsehen, daß der Datensatz für einen gewissen Zeitraum gespeichert bleibt, kommt es innerhalb eines solchen Zeitraumes zu keiner Anschlußbuchung, würde eine automatische Löschung erfolgen.

Nachdem das Softwareunternehmen das Bremer Unternehmen im Jahre 1999 mehrfach vertröstet hatte, habe ich mich direkt an die für das Softwaresystemhaus zuständige Datenschutzaufsichtsbehörde in Südhessen gewandt. Diese hat mir Anfang Januar mitgeteilt, auch das Softwaresystemhaus habe nunmehr erkannt, daß das System hinsichtlich der Löschungsmöglichkeiten von Kundendaten "nicht besonders bedienerfreundlich für den Nutzer" sei. Weiter heißt es, "wir haben uns – auch auf Ihre Anregung hin – entschlossen, dies zu verbessern". Immerhin stellt das Softwarehaus im zweiten Halbjahr 2000 die Realisierung in Aussicht.

16.7. Kreditwirtschaft, Handel, Auskunfteien

16.7.1. Bankgeheimnis beim Lastschriftverfahren

Ein Kreditinstitut hatte gegenüber einem Kaufhaus in der Bremer Innenstadt Name und Anschrift der Kunden herausgegeben, obwohl nach den Allgemeinen Geschäftsbedingungen des Kreditinstituts wie auch nach den Vorschriften des Lastschriftverfahrens die Datenweitergabe unzulässig waren. Das Kreditinstitut hat sich gegenüber der Kundin entschuldigt und wollte für den Schaden einstehen.

16.7.2. Gegen den Willen des Kunden den Magnetstreifen der Scheckkarte eingelesen

Ein anderer Bürger hatte bei einem Einkauf den Kaufbetrag mit einem komplett ausgefüllten Euroscheck beglichen. Auf Anforderung der Kassiererin händigte er dieser zur Überprüfung seine Scheckkarte aus. Die Kassiererin hat daraufhin gegen den Willen des Kunden den Magnetstreifen der Scheckkarte eingelesen.

Meine Nachforschungen haben ergeben, daß beim Auslesen des Magnetstreifens der Scheckkarte an den Kassen des Kaufhauses nur die Daten ausgelesen und gespeichert werden, die für die Abwicklung bei Scheckeinreichung erforderlich sind. Die Firma erhält also nur Informationen über die Bankleitzahl und die Kontonummer des Kontoinhabers. Diese Daten werden zusammen mit der Schecknummer, der Scheckkartennummer und dem ausgestellten Betrag zum Zweck der automatisierten Kassenabrechnung und dem Bankeinzug der Scheckbeträge benötigt. Die Eingabe der genannten Daten wäre ebenso manuell möglich, sie lassen sich nämlich auch von der Scheckkarte bzw. dem Scheck ablesen. Ich mußte daher dem Beschwerdeführer mitteilen, daß, soweit er dies nicht wolle, ihm in Zukunft nur die Möglichkeit bleibe, mit Bargeld zu zahlen.

16.7.3. BSAG: Pilotprojekt "Elektronisches Ticket"

Bei der Bremer Straßenbahn AG (BSAG) ist im Berichtszeitraum mit der Einführung des elektronischen Tickets ein Pilotprojekt begonnen worden. Ich habe mich zweimal bei der BSAG über den Projektverlauf informiert.

Grundlage für den Erwerb des elektronischen Fahrscheines ist der Besitz einer Geldkarte. Die Geldkarte mit ihrer herkömmlichen Bezahlfunktion ist die Basis; der Elektronische Fahrschein ist eine von der Kreditwirtschaft mitautorisierte Zusatzanwendung. Die Karte kann sowohl kontogebunden über das eigene Kreditinstitut als auch kontounabhängig (‚white Card') bei Kreditinstituten oder der BSAG erworben werden. Die Tickets können an stationären Terminals, die sich an bestimmten Haltestellen, im BSAG-Zentrum oder im Sparkassen-Foyer befinden oder in ausgewählten Linien direkt im Fahrzeug an mobilen Terminals erworben werden. Der Fahrpreis wird vom Guthaben der Geldkarte abgebucht und das Ticket auf der Karte in einem Fahrscheinverzeichnis gespeichert. Sofern das Verzeichnis, in dem bis zu zehn Fahrscheine gespeichert werden können, noch nicht vorhanden ist, wird es auf der Karte nachträglich erstellt. Bei älteren Geldkarten (Ausgabe vor 1999) wird nur der Betrag von der Geldkarte abgebucht und automatisch ein Fahrschein ausgedruckt, da die Anlage eines Fahrscheinverzeichnisses und somit die Speicherung des Tickets aufgrund der Kartenstruktur nicht möglich ist. Im Fahrscheinverzeichnis werden pro Fahrschein die Ticketart, der Preis, die Zonennummer, die Linie und der Verfallzeitpunkt gespeichert. Für die Tickets wird ein Verfallzeitpunkt

(abhängig von der Fahrkartenart) festgelegt. Nach Überschreiten des Verfallzeitpunktes wird ein abgelaufenes Ticket beim Kauf eines weiteren Tickets überschrieben.

Der Kartenbesitzer kann mit einem mobilen Kundenlesegerät die zu den letzten 15 Bezahlvorgängen und den letzten drei Ladevorgängen gespeicherten Daten im Teil "Bezahlfunktion der Geldkarte" einsehen. Darüber hinaus kann er die den gesamten Inhalt des Fahrscheinverzeichnisses lesen. Die Löschung gespeicherter Tickets ist für ihn nicht möglich, auch wenn diese bereits abgelaufen sein sollten. Für die Kontrolleure gibt es ein Kartenlesegerät, mit dem nur die im Fahrscheinverzeichnis gespeicherten Datensätze ausgelesen werden können.

In den stationären und mobilen Terminals werden die durch die Transaktion erhobenen Daten gespeichert und regelmäßig an die BSAG weitergeleitet. Bei Buchung des Bezahlvorganges wird die auf der Geldkarte gespeicherte Geldkartennummer ausgelesen und für Abrechnungszwecke mit der Evidenzzentrale an die BSAG weitergeleitet.

Am Pilotprojekt sind drei Firmen beteiligt, die für die Durchführung der Transaktion an den stationären und mobilen Terminals, die korrekte Datenübertragung von den Terminals an die Leitrechner (Server) bei der BSAG und für die Aufbereitung der Datei für die Einreichung bei der Evidenzzentrale verantwortlich sind.

Die Datenübermittlung in den stationären Terminals an die BSAG erfolgt regelmäßig über ISDN. In den mobilen Terminals erhobene Daten werden per Funk an die Herstellerserver bei der BSAG übertragen, sobald die Fahrzeuge in den Betriebshof einfahren. Laut Auskunft der BSAG werden die unverschlüsselt übertragenen Daten nach erfolgreicher Datenübernahme in den stationären und mobilen Terminals gelöscht. Auf jedem Herstellerserver werden die übermittelten Daten gespeichert und eine Bezahldatei für die Einreichung bei der Evidenzzentrale erzeugt. Die Bezahldatei wird der BSAG zur Verfügung gestellt und von ihr an die Evidenzzentrale weitergeleitet.

Das Pilotprojekt in Bremen ist deshalb von so herausragender Bedeutung, weil nicht nur die BSAG, sondern eine Vielzahl anderer Verkehrsbetriebe, nicht zuletzt die Deutsche Bahn AG, die Zusatzanwendung "Elektronisches Ticket" nach erfolgreichem Versuch einführen wollen. Ich koordiniere daher meine Aktivitäten zur Verbesserung des Datenschutzes mit den anderen Obersten Aufsichtsbehörden für den Datenschutz einerseits und mit dem Zentralen Kreditausschuß (ZKA) als Gesamtvertretung der im ZKA zusammengeschlossenen Dachverbände der Kreditwirtschaft andererseits. Bremen hat, wie schon bei der datenschutzrechtlichen Beurteilung der Geldkarte, die Federführung bei der datenschutzrechtlichen Einschätzung des auf dem Chip gespeicherten Fahrscheines übernommen.

Ende Februar wird es zu einem ersten Meinungsaustausch über von mir erarbeitete Vorschläge zur Verbesserung des Datenschutzes bei der BSAG kommen. Im Vordergrund stehen dabei

- ein überschaubarer Zeitraum, in dem der Fahrschein mit Daten der Bezahlfunktion der Geldkarte verknüpft ist,
- Möglichkeiten individueller Löschung abgelaufener Fahrscheine auf der Karte durch den Karteninhaber,

- keine kartenbezogenen Auswertungen aller Fahrscheindaten ohne Einwilligung des Betroffenen und
- Zugriffe bei jeweiligen Kontrollen nur auf die Fahrscheindaten im Verzeichnis, die für den jeweiligen Fahrtabschnitt erforderlich sind.

Bei einer frühzeitigen Beteiligung der Aufsichtsbehörden durch die Kreditwirtschaft im Stadium der Planung wären einige Punkte sicherlich leichter zu realisieren gewesen. Gleichwohl gehe ich davon aus, daß eine Nachbesserung ohne großen Aufwand möglich sein wird, da die Forderungen die Anwendung im Kernbereich nicht tangieren. Im ersten Halbjahr 2000 werden die in Bremen erzielten Ergebnisse auf Bundesebene diskutiert werden.

16.7.4. GeldKarte

Die AG Kreditwirtschaft ist ein Beratungsgremium. An ihr nehmen Vertreter der Datenschutzaufsichtsbehörden und des Zentralen Kreditausschusses (ZKA) - dem Zusammenschluß der drei großen Spitzenverbände des Kreditgewerbes BdB, BVR und DSGV - teil.

Im vergangenen Jahr standen für die Bremer Aufsichtsbehörde zwei Themen im Vordergrund der Beratungen in diesem Kreis, die abschließende Aufklärung und Einschätzung der Datenverarbeitungsvorgänge im Zusammenhang mit der Verwendung der Geldkarte und der ebenfalls mit der Geldkarte in Verbindung stehende elektronische Fahrausweis (vgl. Ziff. 16.7.3.). Bei beiden Themen hat Bremen die Federführung.

Nachdem , wie berichtet (vgl. 21. JB, Ziff. 18.1.), mir im vergangenen Berichtsjahr bei einem Besuch bei einer Evidenzzentrale Einblick in die zentralen Datenverarbeitungs- und Verteilvorgänge gegeben wurde, die im Zusammenhang mit dem Aufladen ,dem Bezahlen und der Abwicklung des Vorganges mit der Geldkarte stehen, hatte ich die Hoffnung gehegt, daß die Aufsichtsbehörden im letzen Jahr zügig zu einer einvernehmlichen Einschätzung der Datenverarbeitungsvorgänge kommen würden. Damit verbunden war aber, daß noch einige offene Fragen von seiten der Kreditwirtschaft beantwortet werden mußten. Dies ist auch im zweiten Halbjahr 1999 erfolgt, verbunden allerdings mit der Übersendung einer CD-ROM, auf der die gesamten Spezifikationen des GeldKarte-Verfahrens auf schätzungsweise über 1000 Seiten abgelegt sind. So konnte nicht mehr rechtzeitig zu der Herbstsitzung eine abschließende und umfassende datenschutzrechtliche Einschätzung aller damit im Zusammenhang stehenden Fragen vorgenommen werden.

Den Abschluß der Arbeiten habe ich aber noch im Berichtszeitraum erreichen können, es bedarf aber noch einer Abstimmung der Ergebnisse unter den Aufsichtsbehörden, wie auch mit der Kreditwirtschaft. Da dies erst auf unserer nächsten Sitzung im Frühjahr gelingen kann, möchte ich an dieser Stelle den Ergebnissen nicht vorgreifen und verzichte auf eine Darstellung einzelner Vorschläge. Insgesamt läßt sich aber schon die Prognose wagen, daß die Datenschutzaufsichtsbehörden unter den gegebenen Rahmenbedingungen der GeldKarte keine gravierenden Mängel des Gesamtsystems feststellen, wohl aber noch einige Anregungen zur Verbesserung des Datenschutzes vorschlagen werden.

Wenn man das Prinzip der möglichst weitgehenden Verwirklichung eines spurenlosen Bezahlvorganges vor Augen hat, wie es beim Bezahlen mit Bargeld der Fall ist, bleibt allerdings ein Mangel. Das größte Defizit der GeldKarte entsteht aus meiner Sicht nämlich dain, daß aufgrund von Vorgaben aus dem Bundesministerium der Finanzen gem. §§ 257 HGB, 147 AO die gesamten Einzeltransaktionen kartenbezogen über 10 Jahre gespeichert bleiben sollen. Hier muß noch die entscheidende juristische Auseinandersetzung mit Unterstützung des Bundesbeauftragten für den Datenschutz geführt werden.

16.7.5. Geldwäscheprävention der Kreditwirtschaft durch Research-Systeme

Ein Bremer Kreditinstitut hat sich an mich gewandt mit der Frage, in welchem Umfang unter Berücksichtigung datenschutzrechtlicher Aspekte Research-Systeme zur Abwehr von Geldwäsche eingesetzt werden dürfen.

Hintergrund ist die Neufassung der Verlautbarung des Bundesaufsichtsamtes für das Kreditwesen (BAKred) zum Geldwäschegesetz (GWG) vom 30.03.1998. Damit wird die Kreditwirtschaft verpflichtet, neue Wege in der Geldwäschebekämpfung zu beschreiten. Im Mittelpunkt der vom BAKred intendierten "intelligenten" Geldwäschebekämpfung steht die aktive Nachforschungspflicht (Research) der Kreditinstitute, u. a. durch Schaffung interner Organisationsanweisungen, um auf diejenigen Finanztransaktionen besondere Aufmerksamkeit zu lenken, die bereits in der Vergangenheit in dem jeweiligen Kreditinstitut unter Geldwäschegesichtspunkten auffällig geworden sind, wobei insbesondere die jeweillige Geschäftskundenstruktur des Kreditinstituts Berücksichtigung finden soll. Die Nachforschungspflicht begründet auch das sogenannte Monitoring, wonach die Kreditinstitute bei Transaktionen, die nach der Beurteilung des Kreditinstitutes die Schwelle zu einem anzeigepflichtigen Sachverhalt mangels eines hinreichenden Verdachts noch nicht überschritten haben, die Geschäftsbeziehung bis zur Ausräumung der Zweifel ggf. auch längerfristig überwacht werden sollen.

Die Kreditwirtschaft hat daraufhin Konzepte von Research-Systemen zur Geldwäschebekämpfung entwickelt. Ich habe mich über diese Frage intensiv mit anderen Datenschutzaufsichtsbehörden ausgetauscht, wobei festzustellen ist, daß die im Zentralen Kreditausschuß (ZKA) und im Bankenfachverband organisierten Kreditinstitute unterschiedliche Wege beschreiten. Die von beiden Verbänden vorgelegten Konzepte wurden intensiv beraten. Entscheidend dabei scheint mir, daß die vom Geldwäschegesetz– insbesondere von § 11 des GWG – vorgeschriebenen Rahmenbedingungen nicht verlassen werden. Wenn sich daher zeigen sollte, daß völlig neue Wege zu beschreiten sind, müssen dafür vorher auch die rechtlichen Voraussetzungen geschaffen werden. Wenn daher von den Datenschutzaufsichtsbehörden die Vorschläge der Kreditwirtschaft zum Teil als akzeptable Ansätze gesehen wurden, die den einzelnen Bankinstituten im Rahmen der Eigenverantwortlichkeit genügend Spielraum lassen hinsichtlich der Entscheidung, ob und in welchem Umfang Kundenaktivitäten überprüft werden sollen, so wurde von den Vertretern der Datenschutzaufsichtsbehörden auch darauf hingewiesen, daß eine umfassende und ständige technische Überwachung aller Kundenkonten durch einzelne Kreditinstitute (vergleichbar einer polizeilichen Rasterfahndung) durch das Konzept eines der Verbände nicht ausgeschlossen ist. Die Vertreter der Datenschutzaufsichtsbehörden haben daher deutlich gemacht, daß eine solche permanente, umfassende Überwachung unter Einbeziehung aller Kundenkonten unter datenschutzrechtlichen Gesichtspunkten nicht in Betracht kommen kann. Es

kommt daher darauf an, daß die einzelnen Kreditinstitute in Abhängigkeit zu den besonderen Usancen ihrer Kunden einen eingeschränkten Kriterienkatalog entwickeln, der eine Totalüberwachung sowohl in temporärer wie quantitativer Hinsicht ausschließt. Insbesondere bedarf es aber darüber hinaus durch das jeweilige Kreditinstitut einer persönlichen Interpretation der mit Research-Systemen gefilterten Daten, bevor eine Mitteilung an die Strafverfolgungsbehörden erfolgt.

Da derzeit verschiedene Research-Systeme mit unterschiedlichen Ansätzen erwogen werden, die auf ihre praktische Verwendbarkeit überprüft werden sollen, bin ich zusammen mit anderen Datenschutzaufsichtsbehörden übereingekommen, die weitere Entwicklung zu beobachten und die Problematik zu gegebener Zeit erneut zu erörtern.

16.7.6. Wirtschafts- und Handelsauskunfteien

Im Berichtszeitraum erhielt ich wieder eine Reihe von Eingaben von Petenten, die sich bei mir über die Verarbeitung ihrer Daten durch die in Bremen und Bremerhaven ansässigen Auskunfteien beklagten. Die Eingaben hatten unterschiedliche datenschutzrechtliche Fragestellungen und Probleme zum Gegenstand. So betrafen sie u. a. die nachträgliche Speicherung von Negativmerkmalen in den Datenbestand der Schufa, das Nachmeldeverfahren der Schufa, die Richtigkeit von Datenspeicherungen, das Vorliegen des für Datenübermittlungen durch Auskunfteien erforderlichen berechtigten Interesses, die Einhaltung der Löschungsfristen und den Umfang des Auskunftsanspruchs des Betroffenen. Erneut ging es in den Eingaben somit um Themen, über die ich in früheren Jahresberichten schon berichtet habe.

Besonders erwähnen möchte ich hier die **Eingabe eines Bremerhavener Bürgers**. Dieser beklagte sich bei mir über eine aus dem Jahre 1985 stammende Eintragung zu seiner Person bei der Auskunftei Creditreform. Aufgrund der Eintragung hatte sich ein Einzelhandelsunternehmen, das bei Creditreform zu seiner Person angefragt hatte, geweigert, dem Petenten einen Computer auf Rechnung zu verkaufen. Auch beschwerte sich der Bürger darüber, daß er über die Übermittlung seiner Daten nicht benachrichtigt worden war.

Wie mir der Petent weiter mitteilte und mir die Auskunftei dann auch bestätigte, war bei Creditreform über den Betroffenen zuletzt im Jahre 1985 eine Abfrage getätigt worden. Seit der damaligen Auskunftserteilung war bei der Auskunftei der von ihr recherchierte Datenbestand - zum größeren Teil mit einem Sperrvermerk versehen - gespeichert geblieben. Für die mit der Beauskunftung beschäftigten Auskunfteimitarbeiter standen immer noch die Adreßdaten des Betroffenen mit einigen internen Vermerken, u. a. dem Datum der letzten Recherche im Jahre 1985 und einem Hinweis, daß noch ein gesperrter Datensatz besteht, für die Auskunftserteilung bereit. Die gespeicherten Angaben waren ohne die gesperrten Daten, jedoch mit Sperrhinweis, an den Computerhändler weitergegeben worden, was dort zur Ablehnung des Rechnungskaufs führte. Die übermittelten Angaben waren von dem Händler offenbar als Negativinformation über den Betroffenen verstanden worden.

Gemäß § 35 Abs. 2 Nr. 4 BDSG haben Auskunfteien personenbezogene Daten zu löschen, wenn eine Prüfung am Ende des fünften Kalenderjahres nach der erstmaligen Speicherung der Daten ergibt, daß eine längerwährende Speicherung nicht erforderlich ist und Gründe, die zu einer Sperrung anstelle der Löschung hätten führen können, nicht ersichtlich sind. Diese sehr nachgiebige gesetzliche Regelung

auf den vorliegenden Fall angewendet, ergibt folgendes. Zunächst einmal nennt das Gesetz selbst eine Regelfrist von fünf Kalenderjahren. Nach Ablauf dieser gesetzlichen Frist sind in aller Regel zu einer Person gespeicherte Negativdaten zu löschen. Gründe für eine weitere Speicherung der Negativdaten des Petenten hat auch die Auskunftei nicht gesehen, denn sie hat schließlich die Daten gesperrt. Gesperrte Daten stehen für eine Auskunft an Dritte nicht mehr zur Verfügung. Eine Sperrung von Daten kann erfolgen, wenn besondere Gründe im Innenverhältnis zwischen Kunden und Auskunftei vorliegen, wie z. B. bei einem anhängigen oder zur erwartenden Rechtsstreit oder bei einer Beweisnot des Kunden oder der Auskunftei. In jedem Falle müssen aber besondere Gründe vorliegen, die eine Aufrechterhaltung der Speicherung der gesperrten Daten erforderlich machen. Solche Gründe konnten von der Auskunftei nicht genannt werden. Im vorliegenden Fall hätten die gesperrten Daten, die nunmehr die gesetzliche Löschfrist um rund 10 Jahre überlebt hatten, längst gelöscht werden müssen. Dann hätte der Auskunftei der Fehler gar nicht unterlaufen können, auch das Vorliegen des Merkmals "Sperrvermerk" mit zu beauskunften. Im übrigen gehe ich davon aus, daß generell wegen seiner negativen Folgen auch der Sachverhalt, das ein Sperrvermerk vorliegt, nicht an Dritte mitgeteilt werden darf, denn Sinn und Zweck der Sperrung ist, daß die Daten nur noch für den Zweck zur Verfügung stehen sollen, die Grund dafür sind, daß die Daten nicht gelöscht, sondern gesperrt werden. Dies ergibt sich aus Sinn und Zweck der Sperrungsregelungen in den Datenschutzgesetzen im allgemeinen. Würde ein Sperrvermerk mit beauskunftet, würde die Intention des Gesetzgebers geradezu kontakariert. Ob im geschilderten Fall auch gegen die gemäß § 33 Abs. 1 BDSG vorgesehene Benachrichtigungspflicht verstoßen worden ist, ließ sich nicht mehr feststellen.

Die Obersten Datenschutzaufsichtsbehörden haben sich im "Düsseldorfer Kreis" unter folgenden Aspekten mit der Datenverarbeitung der Auskunfteien befasst.

Die **Creditreform Experian GmbH** ist ein bundesweit tätiges Gemeinschaftsunternehmen des Verbandes der Vereine Creditreform e. V. und der Experian Deutschland GmbH mit Sitz in Neuss, das sich als Ziel gesetzt hat, als Konsumenten-Auskunftei alle national verfügbaren Daten über das Zahlungsverhalten von Konsumenten in den Kreditprüfungsprozess ihrer Kunden einzubringen. Zu den Kunden der Creditreform Experian GmbH zählen Unternehmen aus den Bereichen Banken, Finanzdienstleister, Telekommunikationsdienstleister sowie Versand- und Einzelhandel, denen die von ihnen angeforderten Daten auch online zur Verfügung gestellt werden. In das Informationssystem der Auskunftei fließen neben allgemein zugänglichen Informationen auch Daten und Mitteilungen der beiden beteiligten Auskunfteien, der Kunden sowie spezifischer Register wie z. B. das Schuldnerverzeichnis ein.

Auf rechtliche Bedenken bei den Obersten Aufsichtsbehörden für den Datenschutz waren nach der Gründung der Creditreform Experian GmbH im Jahre 1998 insbesondere die Art und der Umfang der Daten, die in das Informationssystem der Auskunftei einfließen bzw. dort verarbeitet werden, gestoßen. Das Unternehmen beabsichtigte zunächst, neben Informationen zu Einkommen, Krediten, Zahl der Familienangehörigen , Daten über das Wohnumfeld und den Haustyp (gute und schlechte Adressen im Hinblick auf ein kreditorisches Risiko) auch Daten über Arbeitsverhältnisse und Arbeitgeber zu speichern und weiterzugeben. Zu den Krediten sollten u. a. die Finanzierungsgründe Möbel, Kleidung, Hochzeit oder auch Gesundheit angegeben werden. Vorgesehen war auch,

Angaben über die Zahlungsweise, z.B. bar oder mit Kreditkarte, in das Informationssystem aufzunehmen.

Besonders heftig kritisierten die Obersten Aufsichtsbehörden die vorgesehene Einwilligungserklärung für die Übermittlung der Daten an die Auskunftei. Die Übermittlung allgemeiner Vertrags- und Positivdaten eines Betroffenen ist nur auf der Grundlage einer Einwilligungserklärung, die den Anforderungen des § 2 Abs. 4 BDSG entsprechen muss, zulässig. Die zunächst von dem Unternehmen vorgeschlagene Übernahme des Wortlautes der Schufa-Klausel kam den datenschutzrechtlichen Vorstellungen allerdings nicht entgegen, da die beabsichtigte Datenverarbeitung sich hinsichtlich Umfang und angeschlossenem Teilnehmerkreis wesentlich von dem Schufa-Verfahren unterscheidet. Die Kritikpunkte sind auch heute noch nicht abschließend ausgeräumt.

Beim **Scoring-Verfahren der Schufa** werden mittels mathematisch-statistischer Verfahren aus dem Schufa-Datenbestand insgesamt und unter Beücksichtigung der individuellen Daten sog. Score-Werte ermittelt, die den einzelnen Betroffenen dann zur Beurteilung ihrer Kreditwürdigkeit zugeordnet und an die Kreditgeber übermittelt werden. Kritisiert worden war von den Obersten Datenschutzaufsichtsbehörden u.a. die mangelnde Transparenz des Berechnungsverfahrens sowie der dem Betroffenen zunächst nicht zugestandene Auskunftsanspruch.

Die Schufa hat sich zwischenzeitlich bereit erklärt, bei der beabsichtigten Neufassung der Schufa-Klausel einen Hinweis auf das Scoring-Verfahren aufzunehmen und ein Merkblatt mit Erläuterungen zu dem Score-Verfahren zu erstellen. Das Merkblatt soll in Verantwortung der Kreditwirtschaft erstellt und den Bankkunden auf Wunsch ausgehändigt werden. Der Auskunftsanspruch des Betroffenen soll auch den (zum Zeitpunkt der Auskunftserteilung errechneten) Score-Wert umfassen. Über den Auskunftsanspruch gegenüber den Anschlusskunden der Schufa könne zudem der zum Zeitpunkt der Kreditanfrage errechnete Score-Wert erfragt werden.

Die privatärztlichen Verrechnungsstellen sowie Ärzte und Zahnärzte haben Interesse bekundet, die **Bonität** der von ihnen zu behandelnden **Patienten** durch entsprechende Anfragen bei einem Kreditschutzunternehmen oder einer Auskunftei überprüfen zu können. Der Wunsch wird damit begründet, daß bei umfangreichen ärztlichen und zahnärztlichen Behandlungen - z.B. unter Beteiligung von Zahntechnikern - finanzielle Vorleistungen erforderlich werden können, die mit einem erheblichen Risiko - mangelnde Zahlungsfähigkeit des Patienten - verbunden sind. Das Risiko kann sowohl bei privatärztliche Verrechnungsstellen, an die eine ärztliche Honorarforderung zum Einzug abgetreten wurde, als auch bei Ärzten, die mit ihren Patienten selbst abrechnen, entstehen.

Datenschutzrechtliche Bedenken ergeben sich insbesondere daraus, daß der anfragende Arzt den Betroffenen gegenüber dem Kreditschutzunternehmen oder der Auskunftei eindeutig identifizieren muss, bevor er die gewünschte Auskunft erhalten kann. Durch die Übermittlung der zur Identifikation benötigten Angaben wird zugleich offenbart, daß sich der Betroffene in ärztlicher Behandlung befindet. Es werden somit besonders schutzwürdige Daten weitergegeben, die nach § 203 Strafgesetzbuch der ärztlichen Schweigepflicht unterliegen.

Nach herrschender Rechtsprechung wird bereits durch die Mitteilung, daß sich eine bestimmte Person in ärztlicher Behandlung befindet, die Schweigepflicht durchbrochen. Die Übermittlung von Patientendaten ist ohne Wissen und Einwilligung des Betroffenen unzulässig. Die ärztliche Schweigepflicht darf nur durchbrochen werden, wenn der Patient vorher über die beabsichtigte Weitergabe seiner Daten informiert worden ist und er in sie ausdrücklich schriftlich eingewilligt hat. Ich vertrete deshalb die Auffassung, daß für die Fälle, in denen die ärztliche Honorarforderung an eine privatärztliche Verrechnungsstelle abgetreten wurde, die Erklärung, mit der der Patient in die Übermittlung seiner Daten an die Verrechnungsstelle einwilligt, dahingehend ergänzt werden muss, daß die Verrechnungsstelle zu dem Betroffenen Auskünfte bei einer Kreditschutzorganisation oder einer Auskunftei einholen darf. Rechnet der Arzt mit dem Patienten selbst ab, so könnte die auch in diesem Fall erforderliche schriftliche Einwilligung in Verbindung mit einem Kostenvoranschlag für die Behandlung eingeholt werden. Die mögliche Lösung des Problems soll unter den Mitgliedern des Düsseldorfer Kreises schriftlich abgestimmt werden.

16.8. Versicherungswirtschaft

16.8.1. Versicherungen im Internet

Zusammen mit anderen Datenschutzaufsichtsbehörden habe ich mich im Berichtsjahr erneut um eine datenschutzgerechte Realisierung der Präsentation und Abwicklung von Geschäften der Versicherungswirtschaft im Internet engagiert. Dabei wurde deutlich, daß auf Seiten der Versicherungswirtschaft noch Erläuterungsbedarf zu den Anforderungen und der Umsetzung der Datenschutzvorschriften des Teledienstedatenschutzgesetzes und des Mediendienstestaatsvertrages, insbesondere für Kundeninformationen, Verschlüsselung und Anbieterkennzeichnung bestehen. Es ist beabsichtigt, diese Fragen noch im Jahre 2000 voranzubringen.

16.8.2. Datenerhebung in Antragsformularen der Versicherungswirtschaft

Ein weiterer Punkt, der erst am Ende des Berichtsjahres aufgetaucht ist und in den kommenden Jahren noch weiterer Beobachtung bedarf, betrifft die Datenerhebung in Antragsformularen der Versicherungswirtschaft. Im konkreten Fall bin ich aufgrund einer Anfrage darauf aufmerksam gemacht worden, daß in einem Antragsformular zum Abschluß einer Kfz-Versicherung unter "Fragen zur Familie" auch Geburtstag, -monat und –jahr des jüngsten Kindes abgefragt wird, wie auch die Frage gestellt wird, ob Haus- und Wohnungseigentum vorhanden ist. Da diese beiden Fragen nicht ursächlich im Zusammenhang mit dem Führen eines Kraftfahrzeuges stehen, habe ich mich an das betreffende Versicherungsunternehmen gewandt und um Auskunft gebeten, ob die Fragen in irgendeinem Zusammenhang Relevanz bei der vertraglichen Ausgestaltung entfalten. In dem Antragsformular heißt es konkret "Ich oder mein Ehe- bzw. in häuslicher Gemeinschaft lebender Lebenspartner bin/ist Eigentümer eines selbst bewohnten Ein- oder Zweifamilienhauses für das eine Wohngebäudeversicherung bei a) Versicherungsunternehmen des Kfz-Versicherers, b) einer anderen Gesellschaft besteht. (Bitte Nachweis beifügen)." Die gleiche Frage bezieht sich auf eine selbst bewohnte Eigentumswohnung. Auch hier wird ein Nachweis erbeten.

Das Versicherungsunternehmen hat daraufhin mir gegenüber erklärt, daß bei Haus- und Wohnungseigentum ein Preisnachlaß in der Kfz-Versicherung nur gewährt wird, wenn diese beim gleichen Versicherungsunternehmen versichert sind.

Aus meiner Sicht sollte die Frage sich präzise nur auf diese Konstellation beziehen und nicht alle Haus- und Wohnungseigentümer verpflichtet werden, durch Beifügung einer entsprechenden Versicherungsbescheinigung dem Versicherungsunternehmen nicht benötigte Informationen mitzuliefern. Zur Frage nach dem Geburtsdatum des jüngsten Kindes wurde von dem Versicherungsunternehmen geantwortet, man habe herausgefunden, daß Kraftfahrzeughalter mit Kindern vorsichtiger fahren würden. Auch hier erscheint mir ausreichend, wenn man lediglich das Geburtsjahr des Kindes abfragen würde, nicht hingegen auch noch Tag und Monat.

Im konkreten Fall habe ich daher die zuständige Datenschutzaufsichtsbehörde informiert und sie gebeten, den aufgeworfenen Datenschutzfragen nachzugehen.

Insgesamt liegt auf der Hand, daß die abgefragten Daten selbstverständlich auch zu anderen Zwecken als zum Abschluß eines Kfz-Versicherungsvertrages genutzt werden können. Da zu befürchten ist, daß nicht nur in der Kfz-Versicherung über einen Vertrag weitere Informationen über den Kunden abgefragt werden, die nicht für den einzelnen Vertrag relevant sind, habe ich beschlossen, auf diesen Bereich in Zukunft ein besonderes Augenmerk zu richten.

16.9. Bundesweite Themen der Obersten Aufsichtsbehörden für den Datenschutz

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

Wichtige Themenfelder im Berichtsjahr waren u. a. die Novellierung des BDSG (nicht-öffentlicher Teil), die Umsetzung der EG-Datenschutzrichtlinie in den Ländern, die elektronische Häuser- und Gebäudekarte „City Server“, Research-Systeme der Banken zur Bekämpfung der Geldwäsche, Geldkarte/Elektronische Geldbörse, Mustervereinbarung des Bankenfachverbandes zum gebietsübergreifenden Datenschutz, ärztliche Schweigepflicht, Bonitätsanfragen vor ärztlicher/zahnärztlicher Behandlung, Datenverarbeitung durch Privatärztliche Verrechnungsstellen, Schweigepflicht der Mitarbeiter von privatärztlichen Verrechnungsstellen, Verwendung von Rezeptdaten durch Apotheken-Rechenzentren, Auskunftei Creditreform Experian GmbH, Scoringverfahren einzelner Auskunfteien, Erstellung von Nutzerprofilen mittels Cookies im Internet.

Der Düsseldorfer-Kreis und seine Arbeitsgruppen fassen keine förmlichen Beschlüsse, die dann für die Datenschutzaufsichtsbehörden bindend wären. Die hier erfolgende Meinungsbildung prägt allerdings die Meinung der Datenschutzaufsichtsbehörden wesentlich mit. Leider ist die Abstimmung

in diesen Gremien gelegenlich relativ schwerfällig, dies liegt oft an der mangelnden Informations- und Kooperationsbereitschaft der Gesprächspartner, d.h. der jeweiligen Branchenverbände.

16.10. Wo bleibt die BDSG-Novelle?

Wie war die Ausgangslage am Anfang des Berichtsjahres? Nun, im 0ktober 1995 war die EG-Datenschutzrichtlinie verabschiedet worden. Danach standen den EG-Mitgliedsstaaten und damit auch Deutschland drei Jahre für die Umsetzung der Richtlinie in nationales Recht zur Verfügung. Wie es damals schien, ein ausreichend langer Zeitraum, wurde doch damals schon sehr intensiv die europäische Diskussion von Regierung und einer Ländervertretung begleitet. Dann gab es erste Entwürfe zur Änderung des Bundesdatenschutzgesetzes. Gleichwohl erreichte keiner der verschiedenen Referentenentwürfe Kabinettsreife. Schließlich, so verlautete aus dem Innenministerium, blockierte der anstehende Wahlkampf die Ministerialbürokratie wie die Politik. Die neue Regierungskoalition vereinbarte dann im Oktober 1998, die notwendigen Anpassungen des nationalen Rechts an die EG-Richtlinie kurzfristig umzusetzen. So die Ausgangslage.

Doch die neue Bundesregierung wollte auch neuen Ansprüchen genügen und nicht nur das von der Richtlinie unbedingt Geforderte umsetzen, Sie sah sich plötzlich einer Vielzahl weiterer Wünsche ausgesetzt. Andererseits drängte die Zeit und man konnte ohne eine ordentliche Vorbereitung nicht weitere gravierende Änderungen und neue Komplexe im BDSG unterbringen. So entschied man sich zu einer Vorgehensweise in zwei Stufen. In der ersten Stufe sollen alle unumgänglichen gesetzgeberischen Anpassungen an die Richtlinie erfolgen und darüber hinaus einige auch von der Konferenz der Datenschutzbeauftragten geforderte Modernisierungsregelungen eingearbeitet werden. Hierzu zählen z.B. Regelungen zu Chipkarten, die Verpflichtung zur Datenvermeidung und zur Datensparsamkeit, die Verpflichtung zu einer frühzeitigen Anonnymi- oder Pseudonymisierung sowie die Einführung eines Datenschutzaudits.

Dies zusammen ergibt nach Aussage des Bundesbeauftragten für den Datenschutz eine Summe von weit über 60 Änderungen gegenüber dem ursprünglichen Entwurf der alten Bundesregierung aus 1997. Daß hier ein erneuter, nicht zu unterschätzender Abstimmungsbedarf entstanden ist, liegt auf der Hand. Zuletzt am 28. Januar diesen Jahres hat es in diesem Zusammenhang ein Gespräch zwischen den zuständigen Ländervertretern und dem federführenden Bundesministeriums des Innern gegeben. Gleichwohl, festzuhalten bleibt, daß zum Zeitpunkt des Redaktionsschlusses zu diesem Bericht noch kein Regierungsentwurf vorliegt. Die Zeit drängt, denn die Europäische Kommission hat nach Überschreiten der Übergangsfrist der Bundesregierung bereits zweimal schriftlich dies in Erinnerung gerufen und sie wird nicht zögern, mit der Einleitung eines Vertragsverletzungsverfahrens zu beginnen, in dessen Verlauf die Festsetzung eines Zwangsgeldes droht. Es ist daher wünschenswert, daß die Vorarbeiten an dem Gesetzentwurf nun bald beendet werden können, denn die parlamentarische Behandlung nimmt schließlich auch noch Zeit in Anspruch. Vor allem aber ist wünschenswert, daß endlich die Kapazitäten auch genutzt werden können, um auf dem dann in Kraft befindlichen neuen BDSG fußend, damit anzufangen die jetzt in die zweite Stufe verschobenen nicht minder drängenden Datenschutzprojekte in Angriff nehmen zu können.

Die Regelungen in einem neuen BDSG hätten auch **Auswirkungen auf die Datenschutzaufsicht.** Um gewappnet zu sein, habe ich mich natürlich schon im Berichtsjahr darum gekümmert, welche neuen Aufgaben durch das neue BDSG, wenn es so, wie im Referentenentwurf bisher vorgesehen, in Kraft treten würde, auf die Aufsichtsbehörde zukommen würden. Meine Übelegungen habe ich in einem Papier zusammengestellt und in einem Workshop der Datenschutzaufsichtsbehörden zur Diskussion gestellt. Die Ergebnisse habe ich in das Papier eingearbeitet und allen Interessierten zur Verfügung gestellt. Im Ergebnis komme ich zu der Einschätzung, daß eine ganze Reihe neuer Beratungspflichten und Prüfaufgaben auf die Datenschutzaufsichtsbehörden zukommen, z. B. bei Fragen zum Datentransfer in Drittstaaten außerhalb der EU, bei der Vorabkontrolle besonders riskanter automatisierter Datenverarbeitung wie mobile Speicher- und Verarbeitungsmedien, und nicht zuletzt die Änderungen im Meldeverfahren haben Auswirkungen auf Inhalt und Umfang des von mir zu führenden Registers. Bei all diesen Punkten habe ich allerdings den Eindruck, daß Bremen im Vergleich zu den Aufsichtsbehörden der anderen Länder gut im Rennen liegt und schon jetzt Anstrengungen unternimmt, sich auf die kommenden Aufgaben vorzubereiten.

16.11. Datenexport in Drittstaaten - Probleme mit dem "Safe Harbor"-Konzept der USA

Schwerpunkt der Tätigkeit der Gruppe nach Art. 29 der Datenschutzrichtlinie 95/46/EG, an der auch der ausgeschiedene Landesbeauftragte für den Datenschutz Bremen regelmäßig teilgenommen hat, war auch im Jahr 1999 die Begleitung der Gespräche der EG-Kommission mit der amerikanischen Regierung über die Zulässigkeit von Datenexporten aus EU-Mitgliedstaaten in die USA (vgl. zuletzt 21. JB, Ziff. 5.4.). Das Ziel, diese Gespräche auf den EU-US-Gipfeln abzuschließen, konnte in 1999 nicht erreicht werden.

Noch nicht endgültig geklärt ist nach wie vor die zentrale Frage, wie überprüft werden kann, daß amerikanische Unternehmen, die Daten aus der EU importieren und sich durch eine Erklärung gegenüber dem amerikanischen Handelsministerium den Datenschutzprinzipien des sog. „Safe Harbor“-Konzepts unterworfen haben, diese Grundsätze auch tatsächlich einhalten. Erst sehr spät, d.h. im November, hat die US-Seite den lange angeforderten Bericht darüber geliefert, welche Rolle die verschiedenen US-Behörden, wie etwa die Federal Trade Commission, bei der Kontrolle der Einhaltung der Prinzipien spielen.

Die Kommission kann die Adäquanz des Datenschutzniveaus in den USA nach Art. 25 Abs. 6 der Richtlinie nur feststellen, wenn die US-Seite in der Lage ist, zu zeigen, daß ihr Konzept der Selbstregulierung der Wirtschaft im Bereich des Datenschutzes effektiv durchgesetzt wird. In diesem Zusammenhang bleibt auch zu klären, welche Befugnisse den europäischen Datenschutzbehörden, etwa gegenüber dem datenexportierenden Unternehmen, verbleiben. Aber auch der Inhalt der „Safe Harbor-Principles“ selbst und der sie interpretierenden Texte (Frequently Asked Questions) war Ende 1999 noch teilweise in der Diskussion. Schwer tut sich die europäische Seite auch mit dem Wunsch der US-Regierung, den amerikanischen Firmen eine Übergangsfrist („grace period“) einzuräumen.

Diese äußerst schwierigen Verhandlungen werden sowohl von den Datenschutzinstanzen der Mitgliedstaaten in der Art. 29-Gruppe als auch von den nationalen Regierungsvertretern in der Art. 31 Gruppe intensiv begleitet. Beide Gesprächspartner, EG-Kommission und US-Regierung, sind dringend

an einer schnellen Lösung interessiert, um Probleme im transatlantischen Datenverkehr zu verhindern, die insbesondere in den Bereichen Kreditkarten, Flugreservierung, Kreditinformationen und Direktmarketing auftauchen könnten. Dabei hat die EG-Seite allerdings insofern eine besondere Datenschutzverantwortung, als der mit den USA vereinbarte Rechtsrahmen auch anderen Drittstaaten angeboten werden muß. Er kann damit zu einer Art „Weltstandard“ für den Umgang mit ins Ausland übermittelten Daten europäischer Bürgerinnen und Bürger werden.

17. Meldepflichtige Stellen: Statistische Übersicht, Prüfergebnisse, Bußgeldverfahren

17.1. Umstellung des Registers nach BDSG-Novellierung

Durch die zu erwartende Novellierung des BDSG wird sich die Meldepflicht der nicht-öffentlichen Stellen gegenüber den Datenschutzaufsichtsbehörden, sowohl was den Kreis der verpflichteten Stellen als auch was den Inhalt der Meldung anbetrifft, erheblich verändern. Das bedeutet, daß sich auch die Registerführung der Datenschutzaufsichtsbehörden wesentlich verändern wird. Die bisherigen Registerverfahren, inzwischen weitgehend dv-gestützt, müssen umgestellt und die Datenbestände in bereinigter Form übergeleitet werden. Auch die Verfahrensweisen zur Führung des Registers und zur Einsichtnahme in das Register müssen neu gestaltet werden. Das gilt auch für mein Registerverfahren.

Ich strebe an, daß bundeseinheitliche Vorgaben für ein neues Registerverfahren erarbeitet werden. Dieses könnte dann auf der Basis der einheitlichen Vorgaben und eines Standard-Datenbank-Systems programmiert und lauffähig realisiert werden. Ein solches neues DV-Verfahren könnte nach Fertigstellung dann von allen Aufsichtsbehörden übernommen und eingesetzt werden. Dies wäre auch für die meldepflichtigen Stellen sicher sehr hilfreich.

17.2. Statistische Übersicht - Entwicklungen

Die Zahl der Stellen, die mir zum Register nach § 32 BDSG gemeldet sind, hat sich im Berichtszeitraum wiederum leicht erhöht. Insgesamt weist das Register Anfang Januar 2000 die Zahl von 140 Stellen gegenüber 130 Stellen im Vorjahr aus. Davon befinden sich 119 Stellen in Bremen und 21 in Bremerhaven. Die Mehrzahl der angemeldeten Stellen ist dem Bereich der Auftragsdatenverarbeiter, insbesondere den DV- und TK-Dienstleistungsanbietern zuzuordnen.

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

Die Entwicklung im Bereich der Informations- und Kommunikationstechnik, die Dezentralisierung der Datenverarbeitung, die Auslagerung betrieblicher Funktionen, insbesondere auch der DV-Aktivitäten sowie neuartige DV-, Tele- und TK-Dienstleistungen führen zu häufigen Änderungen im Register.

Aktuellstes Beispiel ist hier die Call-Center-Branche mit ihren z. T. neuartigen Dienstleitungen. Soweit diese Betriebe bzw. Unternehmen geschäftsmäßig personenbezogene Daten dateibezogen verarbeiten – was in allen mir bekannten Fällen wegen der Tätigkeit und der eingesetzten Technik gegeben ist – gelten für sie insbesondere die datenschutzrechtlichen Bestimmungen des BDSG. Ich habe inzwischen mehrere Call-Center als DV-Dienstleister in meinem Register nach § 32 BDSG. Ihre

Zahl dürfte sich im Hinblick auf die stürmische Entwicklung dieses Bereichs in den nächsten Jahren deutlich erhöhen.

Registeränderungen ergeben sich auch dadurch, daß ich Betriebe, bei denen ich aufgrund von Handelsregistereintragungen oder von Branchenzuordnungen eine datenschutzrechtliche Meldepflicht vermute, anschreibe und um Prüfung ihrer Meldepflicht (deren Nichtbefolgung ja bußgeldbewehrt ist) bitte. Bei einigen angeschriebenen Betrieben ergibt sich, z. T. auch aufgrund tatsächlicher Feststellungen, daß meldepflichtige Tätigkeiten ausgeübt werden, die dann zu einer Registereintragung führen.

Einzelheiten zum Stand des Registers zeigt die nachfolgende Übersicht:

Art der Tätigkeit	**insgesamt**	**Bremen**	**Bremerhaven**
Speicherung personenbezogener Daten zum Zwecke der Übermittlung (insgesamt)	**6**	**4**	**2**
Auskunfteien	4	3	1
Adreßverlage/Adreßhändler	2	1	1
Speicherung personenbezogener Daten zum Zwecke der anonymisierten Übermittlung (insgesamt)	**4**	**4**	**-**
Markt- u. Meinungsforschung	4	4	-
Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (insgesamt)	**130**	**111**	**19**
Datenerfassung	5	5	-
Dienstleistung/Rechenzentren	93	79	14
Mikroverfilmer	14	10	4
Mailboxdienste/Provider	8	8	-
Datenlöschung/Datenträgervernichtung	8	8	-
Call-Center	6	5	1
Gesamt	**140**	**119**	**21**

Stand: 01.01.2000

17.3. Ergebnisse der Registerprüfungen

Ich habe im Berichtsjahr vor Ort bei insgesamt 8 nach § 32 BDSG meldepflichtigen Stellen einfache Registerprüfungen aufgrund des § 38 Abs. 2 BDSG durchgeführt. Darüber hinaus habe ich aufgrund von Beschwerden oder wegen Presseberichten eine eingeschränkte Datenschutzprüfung bei einem bremischen Internet-Provider sowie Prüfungen bei einem Kreditinstitut und bei Versicherungsmakler- und Anlageberatungsbüros durchgeführt.

Bei den einfachen Registerprüfungen nach § 38 Abs. 2 BDSG überprüfe ich lediglich das Bestehen der Meldepflicht nach § 32 BDSG sowie die Richtigkeit der Meldung, die Bestellung und Tätigkeit des betrieblichen Datenschutzbeauftragten nach den §§ 36, 37 BDSG, die Verpflichtung der Mitarbeiter auf das Datengeheimnis gemäß § 5 BDSG und ggf. die Beachtung der für die DV- Servicebetriebe geltenden Regelungen zur Auftragsdatenverarbeitung nach § 11 BDSG. Technisch-organisatorische Sicherungsmaßnahmen, die Umsetzung der datenschutzrechtlichen Betroffenenrechte sowie die Zulässigkeit der personenbezogenen Datenverarbeitung werden hierbei nicht geprüft, dies bleibt gesonderten Prüfungen vorbehalten. Dabei ist darauf hinzuweisen, daß die Zulässigkeit der personenbezogenen Datenverarbeitung, die bei den mir gemeldeten Auftragsdatenverarbeitern stattfindet, von den jeweiligen Auftraggebern datenschutzrechtlich zu verantworten ist. Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Bei der eingeschränkten Datenschutzprüfung bei dem bremischen Internet-Provider nach § 38 BDSG habe ich auch die Umsetzung der Regelungen des Teledienstedatenschutzgesetzes (TDDSG) überprüft.

Bei meinen Prüfungen habe ich auch dieses Jahr wieder Mängel feststellen müssen. Die wesentlichen Mängel lagen im Bereich der Registermeldungen (z. B. fehlende Meldung, Aktualität der Meldung), beim betrieblichen Datenschutzbeauftragten (z. B. fehlende bzw. nicht-formgerechte Bestellung, Bündelung mehrerer Funktionen), bei den Verpflichtungen der Mitarbeiter auf das Datengeheimnis und bei der Gestaltung des Vertragsverhältnisses zur Auftragsdatenverarbeitung. Bei dem geprüften Internet-Provider habe ich in allen Prüfpunkten Mängel feststellen müssen.

17.4. Bußgeldverfahren

Gegen eine private Abrechnungsgesellschaft hatte ich in 1998 ein Bußgeldverfahren wegen Verstoßes gegen die Meldepflicht nach § 32 BDSG eingeleitet; dieses Verfahren habe ich eingestellt. Das im Vorjahr gegen eine bei mir gemeldete Wirtschafts- und Handelsauskunftei eingeleitete Bußgeldverfahren wegen unzureichender Benachrichtigung von Betroffenen nach § 33 Abs. 1 BDSG wurde im Berichtsjahr vom Amtsgericht Bremerhaven gemäß § 47 Abs. 2 OwiG eingestellt. Ein Versicherungsunternehmen, daß mir auf einen von einem Ehepaar behaupteten Datenschutzverstoß zunächst keine Antwort gab, reagierte sofort, nachdem ich mit einer Anhörung die Verhängung eines Bußgeldes angedroht hatte.

18. Die Entschließungen der Datenschutzkonferenzen im Jahr 1999

18.1. Modernisierung des Datenschutzes - umfassende Novellierung des BDSG nicht aufschieben

(Entschließung der 57.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999)

Die deutschen Datenschutzbeauftragten haben bereits früh gefordert, die Novellierung des BDSG zur Umsetzung der EG-Datenschutzrichtlinie zu einer gründlichen Modernisierung des veralteten deutschen Datenschutzrechts zu nutzen. Da die dreijährige Anpassungsfrist im Oktober 1998 verstrichen ist, besteht jetzt ein erheblicher Zeitdruck. Für die Neuregelung, die derzeit in der Bundesregierung und in Koalitionsgremien vorbereitet wird, ist daher ein "Zwei-Stufen-Konzept" vorgesehen. Einem ersten, in Kürze vorzulegenden Novellierungsgesetz soll zu einem späteren

Zeitpunkt eine zweite Änderung folgen, die weitere Verbesserungen enthalten soll. Die Konferenz geht davon aus, daß das Zweistufenkonzept von dem festen politischen Willen getragen wird, die zweite Stufe nach Einbindung des ersten Gesetzentwurfes zügig in Angriff zu nehmen und noch in dieser Legislaturperiode abzuschließen. Auch der in dieser Stufe bestehende Handlungsbedarf duldet keinen Aufschub.

Die Konferenz begrüßt, daß jetzt mit Hochdruck an der BDSG-Novellierung gearbeitet wird und Verantwortliche in Regierung und Fraktionen zugesagt haben, die erste Stufe der Neuregelung werde sich nicht auf das von der Richtlinie geforderte Minimum beschränken. Sie unterstützt die Vorschläge, Regelungen zur Videoüberwachung, zu Chipkarten und zum Datenschutzaudit aufzunehmen. Gleiches gilt für die Übernahme der zukunftsweisenden Bestimmungen zur Datenvermeidung sowie zur anonymen bzw. pseudonymen Nutzung von Telediensten aus dem Multimediarecht. Diese sind wichtige und dringend notwendige Regelungen zur Modernisierung des Datenschutzrechts. Die Konferenz drückt daher ihre Erwartung darüber aus, daß diese Vorschriften in der ersten Stufe des Gesetzge-bungsverfahrens zügig verabschiedet werden.

Zu den Punkten, die keinen Aufschub dulden, gehört auch die Verbesserung der Voraussetzungen für eine effektive Datenschutzkontrolle. Die völlig unabhängige Gestaltung der Kontrolle im nichtöffentlichen Bereich muß institutionell sichergestellt und durch eine sachgerechte finanzielle und personelle Ausstattung unterstützt werden. Gegenwärtig noch bestehende Einschränkungen der Kontrollkompetenzen im öffentlichen Bereich müssen abgebaut, den Aufsichtsbehörden müssen wirksamere Befugnisse an die Hand gegeben werden.

Zum Schutz der Bürgerinnen und Bürger sind bei massenhaften Datenerhebungen mit unkalkulierbaren Datenverarbeitungsrisiken oder ungeklärter Zweckbestimmung klare materielle Grenzen durch den Gesetzgeber zu ziehen.

Die bereichsspezifischen Gesetze, z. B. die Sicherheitsgesetze, dürfen nicht vom Bundesdatenschutzgesetz mit den dort zu erwartenden substantiellen Fortschritten für die Bürgerinnen und Bürger, wie beispielsweise einem verbesserten Auskunftsrecht, abgekoppelt werden.

Notwendig ist nach Auffassung der Konferenz, daß das Datenschutzrecht auch in Zukunft bürgerfreundlich und gut lesbar formuliert ist. Dies ist eine unverzichtbare Akzeptanzvoraussetzung für den Datenschutz bei Bürgern, Wirtschaft und Verwaltung.

18.2. Entschließung zur geplanten erweiterten Speicherung von Verbindungsdaten in der Telekommunikation

(Entschließung der 57.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999)

Die Bundesregierung und der Bundesrat werden demnächst über den Erlaß der seit längerem überfälligen Rechtsverordnung zum Datenschutz in der Telekommunikation auf Grund des Telekommunika-tionsgesetzes zu entscheiden haben.

Im Gegensatz zur früheren analogen Vermittlungstechnik erzeugt und verarbeitet das digitalisierte Telekommunikationsnetz (ISDN-Netz) in großem Umfang personenbezogene Verbindungsdaten. Dies

zwingt zu begrenzenden, am Grundsatz der Datensparsamkeit orientierten Regelungen, um das Fernmeldegeheimnis und das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation zu garantieren.

Die bisher geltende Telekommunikationsdienstunternehmen-Datenschutzverordnung von 1996 sieht vor, daß die Verbindungsdaten unter Kürzung der Zielrufnummer regelmäßig bis zu 80 Tagen nach Versendung der Rechnung gespeichert werden dürfen. Über diese Frist hinaus dürfen Verbindungsdaten nur gespeichert bleiben, wenn Streit zwischen dem Telekommunikationsunternehmen und den Kunden über die Richtigkeit der Abrechnung entsteht.

Demgegenüber gibt es Überlegungen für eine neue Telekommunikations-Datenschutzverordnung, daß alle Verbindungsdaten in der Regel selbst bei unbestrittenen oder bezahlten Rechnungen zwei Jahre lang nach Ende der Verbindung gespeichert bleiben können. Da die Speicherungsfrist erst am Ende des Jahres beginnen soll, in dem die Verbindung stattfand, kann dies in Einzelfällen dazu führen, daß die Daten bis zu drei Jahre lang vorgehalten werden.

Hiergegen wenden sich die Datenschutzbeauftragten des Bundes und der Länder mit Entschiedenheit. Sie sehen darin einen unverhältnismäßigen Eingriff in das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation. Auch das Telekommunikationsgesetz hebt die Grundsätze der Verhältnismäßigkeit und der Zweckbindung ausdrücklich hervor. Personenbezogene Daten, die für Zwecke der Telekommunikation erhoben und verarbeitet werden, dürfen nur solange gespeichert bleiben, wie es zu diesen Zwecken erforderlich ist. Auch die vom Gesetz geforderte Höchstfrist für die Speicherung von Verbindungsdaten muß sich am Grundsatz der Datensparsamkeit orientieren, solange sich die Kundin und der Kunde nicht ausdrücklich für eine längere Speicherung entscheiden.

Die Dauer einer zivilrechtlichen Verjährungsfrist kann ebenfalls kein rechtfertigender Anlaß für eine solche Datenspeicherung sein. Jedenfalls müssen die Daten unverzüglich gelöscht werden, wenn die Rechnung beglichen und unbestritten ist und damit der vertragliche Speicherzweck erledigt ist.

Da eine telekommunikations- oder zivilrechtlich bedingte Notwendigkeit für eine derart lange Speicherfrist der Verbindungsdaten somit nicht ersichtlich ist, würde sie eine unzulässige Datenspeicherung auf Vorrat zu unbestimmten Zwecken darstellen.

Diese Speicherung von Kommunikationsdaten wäre auch nicht mit der Überlegung zu rechtfertigen, daß diese Daten zum Zwecke eventueller künftiger Strafverfolgung benötigt werden könnten. Die mit einer solchen Speicherung verbundene vorsorgliche Überwachung unverdächtiger Bürgerinnen und Bürger wäre unzulässig.

18.3. Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL '98)

(Entschließung der 57.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999)

Die Konferenz der Datenschutzbeauftragten hält es für inakzeptabel, daß der entsprechende Entwurf bisher geheimgehalten und ohne Einbeziehung der Datenschutzbeauftragten beraten wird.

Sie fordert die Bundesregierung auf, der Schaffung gemeinsamer Standards zur grenzüberschreitenden Überwachung der Telekommunikation nur insoweit zuzustimmen, als damit nicht zusätzliche Eingriffe in das Grundrecht auf unbeobachtete Kommunikation und das Fernmeldegeheimnis verbunden sind und die Nutzung datenschutzfreundlicher Technologien (z. B. prepaid cards) nicht konterkariert wird.

18.4. Transparente Hard- und Software

(Entschließung der 57.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999)

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt für die Nutzung datenschutzfreundlicher Technologien eingesetzt. Sie sehen jedoch mit Sorge die Entwicklung im Bereich der Informationstechnik, die zu neuen Industriestandards und Produkten führt, die für die Benutzerinnen und Benutzer kaum durchschaubar und selbst für Fachleute nur noch eingeschränkt revisionsfähig sind.

Beispielsweise sind seit kurzem mit dem Intel Pentium III-Prozessor bestückte PCs auf dem Markt, deren Prozessor bei der Herstellung mit einer eindeutigen Nummer (Processor Serial Number - PSN) versehen wurde. Intel sieht vor, das Auslesen der PSN durch die Nutzerinnen und Nutzer kontrollieren zu lassen. Die mittlerweile bekannt gewordenen Manipulationsmöglichkeiten der dafür erforderlichen Software machen deutlich, daß die Existenz einer solchen eindeutigen Kennung kaum kontrollierbare Nutzungsmöglichkeiten eröffnet, die dem Datenschutz diametral zuwider laufen.

Die durch den Intel Pentium III initiierte Debatte um eindeutige Kennungen brachte ans Tageslicht, daß Softwarehersteller Nutzern neuerer Office-Produkte ohne deren Wissen eindeutige Kennungen zuordnen. Diese Kennungen können in Dokumenten versteckt sein und bei der Nutzung des Internets von Softwareherstellern verdeckt abgefragt werden.

Werden Daten der Nutzerinnen und Nutzer übermittelt, ohne daß sie dies bemerken, kann deren mißbräuchliche Verwendung die Anonymität der Anwender von Informationstechnik weiter aushöhlen. Den Erfordernissen des Datenschutzes wird aber nur dann ausreichend Rechnung getragen, wenn zum Schutz der Privatheit transparente und von den Nutzerinnen und Nutzern in eigener Verantwortung bedienbare Sicherheitsfunktionen zur Verfügung stehen.

Deshalb erwarten die Datenschutzbeauftragten des Bundes und der Länder von Herstellern von Informations- und Kommunikationstechnik, Hard- und Software so zu entwickeln und herzustellen, daß Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können.

Den Anwendern moderner Technik empfehlen die Datenschutzbeauftragten, nur solche Produkte einzusetzen, welche auch eine Transparenz der Verfahrensabläufe gewährleisten.

18.5. Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern

(Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17. Juni 1999)

Bei der Einführung der Befugnis zum „Großen Lauschangriff„ hat der Gesetzgeber im Grundgesetz ein Verfahren zur parlamentarischen Kontrolle weitreichender Eingriffe in das Grundrecht auf Unverletzlichkeit der Wohnung verankert (Artikel 13 Abs. 6 GG). Dieses Verfahren dient nach dem Willen des Gesetzgebers der parlamentarischen Kontrolle der Normeffizienz hervor. Auch wenn es die Überprüfung von Lauschangriffen durch die Gerichte und Datenschutzbeauftragten nicht ersetzt, hat es gleichwohl eine grundrechtssichernde Bedeutung. Jetzt ist jedoch bekannt geworden, daß einige Landesjustizverwaltungen der Ansicht sind, Art. 13 Abs. 6 GG sehe eine Berichtspflicht über Lauschangriffe zu Strafverfolgungszwecken gegenüber den Landesparlamenten nicht vor.

Im Gegensatz dazu vertritt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Auffassung, daß die Verfassung eine effektive parlamentarische Kontrolle von Lauschangriffen auf Landesebene vorschreibt, die der Kontrolle auf Bundesebene gleichwertig sein muß. Bei Maßnahmen zur Strafverfolgung durch Landesbehörden besteht die parlamentarische Verantwortlichkeit gegenüber den Landesparlamenten. Die Landtage müssen die Möglichkeit haben, die ihnen in anonymisierter Form übermittelten Berichte der Landesregierungen öffentlich zu erörtern. Die Landesparlamente sollten deshalb durch Gesetz eine regelmäßige Berichtspflicht der Landesregierung für präventiv-polizeiliche und repressive Lauschangriffe vorsehen. Nur auf diese Weise ist eine wirksame parlamentarische Kontrolle der Ausübung dieser einschneidenden Überwachungsbefugnisse gewährleistet.

Wird durch eine solche Kontrolle deutlich, daß die akustische Wohnraumüberwachung für Zwecke der Strafverfolgung in der Praxis nicht die vom Gesetzgeber angestrebte Effizienz im Verhältnis zur Häufigkeit und Intensität der Grundrechtseingriffe zeigt, können Landesregierungen, die das Bundesrecht in eigener Verantwortung auszuführen haben, über den Bundesrat darauf hinwirken, die Befugnis für eine derartige Überwachung wieder aufzuheben oder zumindest zu modifizieren.

18.6. "Angemessener Datenschutz auch für Untersuchungsgefangene"

(Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16. August 1999)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, daß die Bundesregierung den Entwurf eines Gesetzes zur Regelung des Vollzuges der Untersuchungshaft vorgelegt hat. Damit wird die seit Jahren erhobene Forderung der Datenschutzbeauftragten nach einer bereichsspezifischen gesetzlichen Regelung aufgegriffen.

Diese Regelung muß das Strafverfolgungs- und Sicherheitsinteresse des Staates im Rahmen des gesetzlichen Zwecks der Untersuchungshaft berücksichtigen. Gleichzeitig sind jedoch das Persönlichkeitsrecht der Gefangenen sowie die Unschuldsvermutung und der Anspruch auf wirksame Verteidigung im Strafverfahren angemessen zur Geltung zu bringen.

Der Gesetzentwurf der Bundesregierung trägt diesem Anliegen durch differenzierende Vorschriften teilweise Rechnung, läßt allerdings noch Raum für datenschutzrechtliche Verbesserungen. Die Stellungnahme des Bundesrates betont demgegenüber einseitig das staatliche Vollzugsinteresse und entfernt sich damit deutlich vom Ziel einer sorgfältigen Güterabwägung.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder muß die gesetzliche Regelung insbesondere folgenden Anforderungen genügen:

- Entgegen dem Vorschlag des Bundesrates, von einer inhaltlichen Überwachung nur ausnahmsweise nach dem Ermessen des Gerichts abzusehen, sollte im weiteren Gesetzgebungsverfahren an der Konzeption der Bundesregierung festgehalten werden. Der Gesetzentwurf der Bundesregierung differenziert bei der Überwachung der Unterhaltung mit Besucherinnen und Besuchern sowie bei der Kontrolle des Textes von Schriftstücken sachgerecht nach Haftgründen. Nur im Falle der Untersuchungshaft wegen Verdunkelungsgefahr sollten diese Maßnahmen unmittelbar und generell durch Gesetz vorgeschrieben werden, während sie bei Vorliegen anderer Haftgründe (z.B. Fluchtgefahr) nur im Einzelfall aufgrund richterlicher Anordnung erfolgen dürfen.

  Darüber hinaus sollte im weiteren Gesetzgebungsverfahren die Möglichkeit unüberwachter Kontakte der Gefangenen zu nahen Angehörigen mit Zustimmung der Staatsanwaltschaft auch in Fällen der Untersuchungshaft wegen Verdunkelungsgefahr erwogen werden. Stichprobenartige Überprüfungen von Schriftstücken durch die Vollzugsanstalt anstelle einer Textkontrolle sollten nicht den gesamten Schriftverkehr einzelner Gefangener umfassen. Dies könnte sich im Ergebnis als verdachtsunabhängige Totalkontrolle ohne richterliche Entscheidung auswirken.

- Das Recht auf ungehinderten und unüberwachten telefonischen Kontakt zwischen Verteidigung und Beschuldigten muß auch in der Untersuchungshaft gewährleistet sein. Mit dem rechtsstaatlichen Gebot wirksamer Strafverteidigung wäre es nicht vereinbar, diesen Kontakt von einer besonderen Erlaubnis des Gerichts abhängig zu machen, wie vom Bundesrat befürwortet.

- Bei Datenübermittlungen an öffentliche Stellen außerhalb der Vollzugsanstalt (z.B. Sozialleistungsträger, Ausländerbehörden) und an Forschungseinrichtungen müssen die schutzwürdigen Interessen der Betroffenen im Rahmen einer Abwägung berücksichtigt werden. Auch die Erteilung von Auskünften an die Verletzten der Straftat sollte der Gesetzgeber unter Beachtung der Unschuldsvermutung regeln.

- Die vom Bundesrat vorgeschlagene erhebliche Einschränkung des Auskunfts- und Akteneinsichtsrechts von Gefangenen im Hinblick auf den Zweck der Untersuchungshaft würde wesentliche Datenschutzrechte in einem besonders sensiblen Bereich weitgehend entwerten und ist daher abzulehnen.

18.7. "Gesundheitsreform 2000"

(Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25.08.1999)

Die Datenschutzbeauftragten von Bund und Ländern erklären zu dem Entwurf eines Gesetzes "Gesundheitsreform 2000":

Die Datenschutzbeauftragten haben großes Verständnis für die Bemühungen, die Kosten im Gesundheitswesen zu begrenzen und eine gute Versorgung der Patientinnen und Patienten sicherzustellen. Bei der Wahl der Mittel ist es aber Aufgabe des Gesetzgebers, beim Eingriff in das Recht auf informationelle Selbstbestimmung das Prinzip der Erforderlichkeit und der Verhältnismäßigkeit zu wahren.

Der Entwurf läßt jede Begründung vermissen, warum die bisherigen Kontrollmechanismen, die das Entstehen umfangreicher medizinischer Patientendatenbestände bei den Krankenkassen vermeiden, ungeeignet sein sollen, die Wirtschaftlichkeit und Qualität ärztlicher Leistungserbringung sicherzustellen.

Der Entwurf gibt das bisherige Konzept der Datenverarbeitung in der gesetzlichen Krankenversicherung auf. Insbesondere standen bisher aus dem ambulanten Bereich personenbezogene Abrechnungsdaten mit medizinischen Inhalten und Diagnosedaten den Krankenkassen nur ausnahmsweise zu Prüfzwecken zur Verfügung, künftig sollen diese Informationen den Krankenkassen dagegen generell versichertenbezogen übermittelt werden. Damit entstehen bei den gesetzlichen Krankenkassen vollständige personenbezogene medizinische Datenbestände der gesetzlich Versicherten mit der Möglichkeit, für jede einzelne Person umfassende Darstellungen ihres Gesundheitszustandes zu bilden. Bei den Kassen entstehen gläserne Patientinnen und Patienten. Das Patientengeheimnis wird ausgehöhlt.

Die Datenschutzbeauftragten richten an den Gesetzgeber die dringende Bitte, die bisher versäumte eingehende Prüfung von Erforderlichkeit und Verhältnismäßigkeit der weiterreichenden Datenverarbeitungsbestimmungen nachzuholen. Der Bundesbeauftragte für den Datenschutz, mit dem der Entwurf entgegen anders lautenden Äußerungen von Regierungsvertretern in der Sache bisher in keiner Weise abgestimmt wurde, sowie die Datenschutzbeauftragten der Länder stehen hierfür zur Diskussion zur Verfügung.

Insbesondere klärungsbedürftig sind folgende Punkte:

- Der Entwurf erweitert die Aufgaben der Krankenkassen auch auf eine steuernde und durch die Patientinnen und Patienten nicht geforderte Beratung über Gesundheitserhaltungsmaßnahmen und auf eine Prüfung der u. a. durch die Ärztinnen und Ärzte erbrachten Leistungen. Er sieht dafür umfangreiche Datenerhebungs- und -verarbeitungsbefugnisse vor.
- Der Wortlaut des Entwurfes beschreibt diese Aufgabe allerdings nur vage. Er läßt nicht erkennen, was auf die Patientinnen und Patienten zukommt. Weder ist klar geregelt, wie weit die Beratung reichen darf, noch mit welchen Rechtsfolgen die oder der Einzelne rechnen muss. Es ist zu befürchten, daß diese Beratung dazu dienen wird, die Patientinnen und Patienten, Ärztinnen und

Ärzte und die sonstigen Leistungserbringer zu kontrollieren und zu beeinflussen und daß hierdurch das Arzt-Patienten-Vertrauensverhältnis belastet wird.

- Wegen der vagen Aufgabenbeschreibung sind auch die damit verbundenen Datenverarbeitungs- und -zusammenführungsbefugnisse in gleicher Weise unklar und verschwommen. Eine Präzisierung und Eingrenzung ist dringend erforderlich.

- Der Entwurf sieht im Gegensatz zum bisherigen System vor, daß Abrechnungsdaten und Diagnosen aus der ambulanten ärztlichen Behandlung generell patientenbezogen an die Krankenkassen übermittelt werden. Dadurch entstehen bei den Kassen umfangreiche sensible Datenbestände, aus denen sich für jede einzelne Patientin und jeden einzelnen Patienten ein vollständiges Gesundheitsprofil erstellen lässt. Wegen der Verpflichtung, die Diagnosen nach dem international gültigen ICD-10-Schlüssel zu codieren, sind diese medizinischen Informationen z. B. im Bereich der Psychotherapie auch hochdifferenziert.

- Die zur Begründung besonders angeführten Punkte "Unterrichtung der Versicherten über die in Anspruch genommenen Leistungen, Kontrolle der Einhaltung der zweijährigen Gewährleistungspflicht bei den Zahnärzten, Unterstützung der Versicherten bei Behandlungsfehlern" vermögen insoweit nicht zu überzeugen. Bereits jetzt können die Versicherten über die beanspruchten Leistungen und deren Kosten informiert werden und von ihrer Krankenkasse auch im Übrigen Unterstützung erbitten, so daß keine Notwendigkeit für die Anlegung derart sensibler, umfangreicher und zentraler Datenbestände ersichtlich ist.

- Der Eingriff in die Rechte der Patientinnen und Patienten steht damit in keinem Verhältnis zu den angegebenen Zwecken.

- Die beabsichtigte Einführung von zentralen Datenannahme- und -verteilstellen, bei denen nicht einmal klar ist, in welcher Rechtsform (öffentlich oder privat) sie betrieben werden sollen, hat eine weitere, diesmal Krankenkassen übergreifende zentrale Sammlung medizinischer personenbezogener Patientendaten zur Folge. Wegen des hohen weiteren Gefährdungspotentials von derart umfassenden Datenbeständen müsste der Entwurf im Einzelnen begründen, warum eine konsequente Umsetzung der schon bisher möglichen Kontrollmechanismen nicht ausreicht.

Die angesprochenen Punkte stellen besonders gewichtige, aber keineswegs die einzigen Probleme dar. Zu nennen sind hier nur beispielsweise die Verlängerung der Speicherdauer von Patientendaten beim Medizinischen Dienst der Krankenversicherung (MDK) von 5 auf 10 Jahre, unzureichende Regelungen bei den Speicherfristen, bei Umfang, Zweckbindung und Freiwilligkeit der Datenerhebung beim Hausarztmodell, der integrierten Versorgung und den Bonus-Modellen sowie unzureichende Pseudonymisierung bei den Arbeitsgemeinschaften. Abzulehnen ist auch die völlig mangelhafte Zweckbindung der Daten bei den Krankenkassen.

18.8. Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

(Entschließung der 58.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich am 09./10.03.1995 gefordert, daß insbesondere die Dauer der Aufbewahrung von Strafakten nach rechtskräftigem Abschluß eines Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch formelles, den Grundsätzen des Volkszählungsurteils entsprechendes Gesetz bedarf.

Mit Beschluß vom 16.08.1998 hat das Oberlandesgericht Frankfurt am Main festgestellt, daß der derzeitige Zustand zwar für eine Übergangsfrist noch hinzunehmen sei, daß die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten jedoch nicht als nur mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei. In gleicher Weise hat auch das OLG Hamm mit Beschluß von 17.09.1998 darauf hingewiesen, daß die Aufbewahrung von Strafakten einer gesetzlichen Grundlage bedarf. Auch der Entwurf des Strafverfahrensänderungsgesetzes 1999 enthält insoweit keine Regelung.

Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für dringend geboten, daß unverzüglich mit der Umsetzung dieser Aufgabe begonnen wird. Sie weisen ferner darauf hin, daß auch für die Aufbewahrung von Zivilakten und Akten im Bereich der freiwilligen Gerichtsbarkeit umgehend gesetzliche Regelungen zu schaffen sind, die die Dauer der Aufbewahrung auf das erforderliche Maß festlegen.

18.9. Entschließung zu "Täter-Opfer-Ausgleich und Datenschutz"

(Entschließung der 58.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Kernstück datenschutzrechtlicher Überlegungen zum Täter-Opfer-Ausgleich ist die Frage, ob Institutionen zur Durchführung des Ausgleichsverfahrens umfassende Informationen insbesondere über Opfer von Straftaten erhalten dürfen, ohne daß diese davon Kenntnis erlangt und eingewilligt haben.

Darin wäre ein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen zu sehen. Dies ist nach geltendem Recht unzulässig.

Der nunmehr vorliegende Gesetzentwurf der Bundesregierung (BR-Drs. 325/99 vom 28.05.1999) sieht in § 155 a Satz 3 StPO-Entwurf vor, daß nur der ausdrücklich geäußerte entgegenstehende Wille der oder des Verletzten dazu führt, daß keine Datenübermittlungen an Schlichtungsstellen erfolgen sollen. Das bedeutet, daß solche im Einzelfall gleichwohl möglich sind. Dies halten die Datenschutzbeauftragten nicht für ausreichend.

Der Bundesrat ist sogar dem Gesetzentwurf der Bundesregierung nicht gefolgt; er hat vielmehr angeregt, im Gesetz klarzustellen, daß es für solche Datenübermittlungen auf den Willen der Opfer nicht ankommen soll. Folgende Argumente werden dafür genannt: Eine vor der Einschaltung von

Schlichtungsstellen durch die Justiz einzuholende Einwilligung führe dazu, daß das kriminalpolitisch wichtige Institut des "Täter-Opfer-Ausgleichs" nicht ausreichend genutzt werde. Erst die professionelle Tätigkeit der Schlichtungsstellen mit ihrem Selbstverständnis als "objektive Dritte mit dem Gebot der Unterstützung jeder Partei" könnte wirksame Überzeugungsarbeit leisten; nur dann könne der Rechtsfriede dauerhafter als bei herkömmlichen Verfahren sichergestellt werden, wenn durch die "fachlich geleitete Auseinandersetzung" der "am strafrechtlich relevanten Konflikt beteiligten Parteien im Idealfall Verständnis und wechselseitige Toleranz geweckt werden".

Dieser Argumentation widersprechen die Datenschutzbeauftragten entschieden: Die Achtung und wirksame Unterstützung der Opfer ist ein wesentliches Anliegen des Strafverfahrens. Rechtsfriede und Toleranz können nur verwirklicht werden, wenn die Strafverfolgungsbehörden bei Datenübermittlungen an Schlichtungsstellen (z. B. in der Rechtsform von Vereinen) den Willen und die Eigenverantwortung der Opfer uneingeschränkt respektieren. Auch die Sicht der Beschuldigten, ohne deren Mitwirkung der Täter-Opfer-Ausgleich nicht durchgeführt werden kann, sollte von den Strafverfolgungsbehörden dabei berücksichtigt werden. Die Konferenz der Datenschutzbeauftragten fordert deshalb, daß an der Voraussetzung der unzweifelhaften Einwilligung vor solchen Datenübermittlungen festgehalten wird.

Ferner sollte der Gesetzgeber festlegen, daß die Berichte der Schlichtungsstellen an Staatsanwaltschaft und Gericht nur für Zwecke der Rechtspflege verwendet werden dürfen. Das besondere Vertrauensverhältnis zwischen den Schlichtungsstellen und den am "Täter-Opfer-Ausgleich" Beteiligten muss gesetzlich geschützt werden.

18.10. Entschließung zum Beschluß des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union

(Entschließung der 58.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Der Europäische Rat hat anläßlich seiner Zusammenkunft am 4. Juni 1999 in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen. In dem Ratsbeschluß heißt es: "Im gegenwärtigen Entwicklungszustand der Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern".

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen nachhaltig die Initiative des Europäischen Rates zur Ausarbeitung einer europäischen Grundrechtscharta. Sie fordern Bundesregierung, Bundestag und Bundesrat auf, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union einzusetzen. Damit würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung getragen.

Die europäische Datenschutzrichtlinie verpflichtet die Mitgliedstaaten zur Gewährleistung des Schutzes der Grundrechte und Grundfreiheiten und insbesondere des Schutzes der Privatsphäre (Art. 1 Abs.1). Die Datenschutzbeauftragten weisen darauf hin, daß einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben; in einigen anderen Ländern wurde

ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt. In Deutschland wird das vom Bundesverfassungsgericht aus dem Persönlichkeitsrecht (Art. 2 Abs. 1 i.V. m. Art. 1 Abs.1 GG) abgeleitete Grundrecht auf Datenschutz als solches von zahlreichen Landesverfassungen ausdrücklich erwähnt.

18.11. Patientenschutz durch Pseudonymisierung

(Entschließung der 58.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Im Gesundheitsausschuß des Deutschen Bundestages wird derzeit der vom Bundesministerium für Gesundheit vorgelegte Gesetzesentwurf zur Gesundheitsreform 2000 dahingehend geändert, daß die Krankenkassen künftig von den Leistungserbringern (z. B. Ärztinnen und Ärzte, Krankenhäuser, Apotheken) die Patientendaten nicht in personenbezogener, sondern in pseudonymisierter Form erhalten. Dieses neue Modell nimmt eine zentrale Forderung der Datenschutzbeauftragten auf, für die Verarbeitung von Patientendaten solche technischen Verfahren zu nutzen, die die Persönlichkeitsrechte der Betroffenen wahren und so die Entstehung des "gläsernen Patienten" verhindern.

Auch anhand von pseudonymisierten Daten können die Krankenkassen ihre Aufgaben der Prüfung der Richtigkeit der Abrechnungen sowie der Wirtschaftlichkeit und der Qualität der Leistungen erfüllen.

Die Konferenz unterstützt den Bundesbeauftragten für den Datenschutz dabei, daß in den Ausschußberatungen die Wirksamkeit der Pseudonymisierung, die gesetzliche Festlegung von Voraussetzungen für die Identifizierung der Versicherten zu bestimmten Zwecken und die Definition strikter Zweckbindung dieser Daten durchgesetzt werden.

18.12. DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen

(Entschließung der 58.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

In der Strafprozessordnung ist der Einsatz der DNA-Analyse zur vorbeugenden Verbrechensbekämpfung nur mit richterlicher Anordnung vorgesehen.

In einigen deutschen Ländern werden DNA-Analysen ohne richterliche Anordnung gestützt allein auf die Einwilligung der Betroffenen durchgeführt. Soweit die dabei erhobenen Daten zum Zweck der Identitätsfeststellung in künftigen Strafverfahren genutzt werden sollen, bedürfen DNA-Analysen nach der klaren gesetzlichen Regelung des DNA-Identitätsfeststellungsgesetzes jedoch einer richterlichen Anordnung. Der Richter oder die Richterin hat u. a. die Prognose zu treffen, ob Grund zur Annahme besteht, daß gegen Betroffene künftig erneut Strafverfahren wegen des Verdachts erheblicher Straftaten zu führen sind. Wenn nunmehr auch DNA-Analysen gespeichert und zum Zweck der zukünftigen Strafverfolgung genutzt werden dürfen, die auf freiwilliger Basis – also ohne richterliche Anordnung – erstellt worden sind, und dies sogar durch die Errichtungsanordnung für die DNA-Analyse-Datei beim BKA festgeschrieben werden soll, werden damit die eindeutigen gesetzlichen Vorgaben des DNA-Identi- tätsfeststellungsgesetzes unterlaufen.

Die von Strafgefangenen erteilte Einwilligung zur Entnahme, Analyse und Speicherung kann keine Grundlage für einen derartigen Eingriff sein. Eine wirksame Einwilligung setzt voraus, daß sie frei von psychischem Zwang freiwillig erfolgt. Da Strafgefangene annehmen können, daß die Verweigerung der Einwilligung Auswirkungen z. B. auf die Gewährung von Vollzugslockerungen hat, kann hier von Freiwilligkeit keine Rede sein. Ausschlaggebend für die Beurteilung der Freiwilligkeit einer Einwilligung ist die subjektive Einschätzung des Betroffenen. Auch wenn im Einzelfall die Weigerung von Strafgefangenen, sich einer DNA-Analyse zu unterziehen, die Entscheidung über Vollzugslockerungen nicht beeinflusst, ist dennoch davon auszugehen, daß die Befürchtung, die Verweigerung habe negative Folgen, die freie Willensentscheidung beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder halten deshalb die Praxis einiger Länder, DNA-Analysen – abweichend von den gesetzlich vorgesehenen Verfahren – systematisch auf der Grundlage von Einwilligungen durchzuführen, für eine Umgehung der gesetzlichen Reglung und damit für unzulässig. Die möglicherweise mit der Beantragung richterlicher Anordnungen verbundene Mehrarbeit ist im Interesse der Rechtmäßigkeit der Eingriffsmaßnahmen hinzunehmen. Die Datenschutzbeauftragten fordern daher, DNA-Analysen zum Zweck der Identitätsfeststellung für künftige Strafverfahren nur noch auf der Grundlage richterlicher Anordnungen durchzuführen.

18.13. Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation

(Entschließung der 58.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Die Ausbreitung moderner Telekommunikationsnetze und die Fortentwicklung der Informationstechnologie erfolgen in großen Schritten. Dieser technische Fortschritt hat einerseits zu einer massenhaften Nutzung der neuen Möglichkeiten der Telekommunikation und damit zu einer grundlegenden Veränderung des Kommunikationsverhaltens der Bevölkerung geführt. Andererseits erhalten dadurch die herkömmlichen Befugnisse der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs eine neue Dimension, weil aufgrund der weitreichenden Digitalisierung immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden.

Die bei der Telekommunikation anfallenden Daten können mit geringem Aufwand in großem Umfang kontrolliert und ausgewertet werden. Anhand von Verbindungsdaten läßt sich nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Bereits auf der Ebene der bloßen Verbindungsdaten können so Verhaltensprofile erstellt werden, die die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen. Eine staatliche Überwachung dieser Vorgänge greift daher tief in das Telekommunikationsgeheimnis der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse.

Die bisherige rechtliche Grundlage für den Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in § 12 des Fernmeldeanlagengesetzes (FAG) stammt noch aus einer Zeit, in der die analoge Vermittlungstechnik vorherrschte, nicht für jedes Gespräch personenbezogene

Verbindungsdaten erzeugt wurden und die Telekommunikationsdienste in wesentlich geringerem Maße als heute genutzt wurden. Die Vorschrift erlaubt auch Zugriffe auf Verbindungsdaten wegen unbedeutenden Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation unzulässig wäre. Unter Berücksichtigung der Digitaltechnik, der vollständigen Datenerfassung und der Möglichkeit zur Bildung von Verhaltensprofilen verstößt § 12 FAG daher gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen.

In einem früheren Gesetzesentwurf war vorgesehen, den Zugriff auf Verbindungsdaten grundsätzlich auf nicht unerhebliche Straftaten zu beschränken. Beschlossen wurde aber lediglich die unveränderte Fortgeltung des § 12 FAG, zuletzt befristet bis zum 31.12.1999. Nunmehr wollen der Bundesrat und die Justizministerkonferenz die Befristung für die Weitergeltung dieser Vorschrift aufheben und es damit beim bisherigen, verfassungsrechtlich bedenklichen Rechtszustand belassen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG und fordern statt dessen eine Neufassung der Eingriffsbefugnis unter Beachtung der grundrechtlichen Bindungen und Anforderungen, die sich aus dem von Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis ergeben.

Die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten gehört sachlich in die Strafprozessordnung. Die gesetzlichen Zugriffsvoraussetzungen sollten in Abstimmung mit § 100 a StPO neu geregelt werden.

18.14. Eckpunkte der deutschen Kryptopolitik - ein Schritt in die richtige Richtung

(Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08.10.1999)

Das Brief-, Post- und Fernmeldegeheimnis zählt zu den traditionellen und wichtigsten Garantien einer freiheitlichen Verfassung. Artikel 10 Grundgesetz gewährleistet deshalb die freie Entfaltung der Persönlichkeit durch einen privaten, vor Dritten verborgenen Austausch von Nachrichten, Gedanken und Informationen. Deshalb darf nur in Ausnahmefällen im überwiegenden Allgemeininteresse auf gesetzlicher Grundlage in dieses Grundrecht eingegriffen werden.

Im Zuge der Privatisierung der Telekom hat der Staat sein Post- und Fernmeldemonopol verloren, so daß zum Grundrechtsschutz die bloße Abwehr unrechtmäßiger staatlicher Eingriffe nicht mehr genügt. Darüber hinaus bestehen die Möglichkeiten der staatlichen Datenschutzkontrolle in offenen Netzen nur in eingeschränktem Maße. Der Schutz personenbezogener Daten während der Verarbeitung und Übertragung ist häufig nicht ausreichend gewährleistet. Deshalb sind ergänzende staatliche Maßnahmen zum Schutz Aller gegen neugierige Dritte (z. B. Systembetreiber, Unternehmen mit wirtschaftlichen Interessen, Hacker und Hackerinnen, ausländische Geheimdienste) erforderlich.

Die Privatsphäre läßt sich jedoch nur mit Rechtsvorschriften nicht ausreichend schützen. Neben bestehenden Ge- und Verboten sind wirksame technische Vorkehrungen nötig. Systemdatenschutz und datenschutzfreundliche Technologien sind unverzichtbar. Den Bürgerinnen und Bürgern müssen

effektive Instrumente zum Selbstschutz an die Hand gegeben werden. Der Datenverschlüsselung kommt deshalb in einem modernen Datenschutzkonzept eine herausragende Bedeutung zu.

Bislang mußte befürchtet werden, daß auf Betreiben der staatlichen Sicherheitsbehörden in Deutschland das Recht auf Verschlüsselung eingeschränkt würde. Jetzt jedoch hat die Bundesregierung mit dem Eckpunktepapier vom 2. Juni 1999 die Diskussion auf eine völlig neue Basis gestellt. Richtigerweise wird darin die Kryptographie als "eine entscheidende Voraussetzung für den Datenschutz der Bürger" besonders hervorgehoben.

Die Position der Bundesregierung, die freie Verfügbarkeit von Verschlüsselungsprodukten nicht einschränken zu wollen, wird von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt. Damit wurde ein erster wichtiger Schritt in die richtige Richtung getan, dem jedoch weitere folgen müssen. Der im Sinne des Artikels 10 des Grundgesetzes legitime und grundrechtlich geschützte Anspruch Aller auf unbeobachtete Telekommunikation und auf den Schutz ihrer personenbezogenen Daten sollte von der Bundesregierung noch stärker unterstützt werden. Um der Bedeutung geschützter Telekommunikation unter den Bedingungen der Informationsgesellschaft gerecht zu werden, sind konkrete Maßnahmen notwendig. Vorrangig sind zu nennen:

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken in der öffentlichen Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen,
- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern,
- Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte und Ärztinnen, Anwälte und Anwältinnen, Psychologen und Psychologinnen),
- Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation,
- Förderung einer neutralen Bewertung von Verschlüsselungsprodukten mit dem Ziel, den Verbrauchern Empfehlungen für ihren Gebrauch zu geben,

Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offengelegten Algorithmen.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen. Sie sollten vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptographischer Verfahren zum Schutz personenbezogener Daten prüfen und derartige Lösungen häufiger als bisher einsetzen. Künftig muß Kryptographie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.

Hersteller von Produkten der Informations- und Telekommunikationstechnik werden aufgefordert, die guten Voraussetzungen zur Entwicklung von Verschlüsselungsprodukten in Deutschland zu nutzen, um sichere, leicht bedienbare und interoperable Produkte zu entwickeln und den Anwendern kostengünstig anzubieten. Die Datenschutzbeauftragten des Bundes und der Länder bieten hierfür ihre Kooperation an.

19. Liste des verfügbaren Informationsmaterials

Folgende Informationsmaterialien können beim

Landesbeauftragten für den Datenschutz der Freien Hansestadt Bremen
Postfach 10 03 80, 27503 Bremerhaven
Telefon: 0471/9 24 61-0
Telefax: 0471/9 24 61-31
e-mail: office@datenschutz.bremen.de

angefordert werden:

10. Jahresbericht 1987, Bürgerschafts-Drs. 12/163	(vergriffen)
11. Jahresbericht 1987, Bürgerschafts-Drs. 12/499	(vergriffen)
12. Jahresbericht 1989, Bürgerschafts-Drs. 12/815	(vergriffen)
13. Jahresbericht 1987, Bürgerschafts-Drs. 12/1187	(vergriffen)
14. Jahresbericht 1991, Bürgerschafts-Drs. 13/97	(vergriffen)
15. Jahresbericht 1992, Bürgerschafts-Drs. 13/520	(vergriffen)
16. Jahresbericht 1987, Bürgerschafts-Drs. 13/859	(vergriffen)
17. Jahresbericht 1994, Bürgerschafts-Drs. 13/1181	(vergriffen)
18. Jahresbericht 1995, Bürgerschafts-Drs. 14/272	(Restexemplare)
19. Jahresbericht 1996, Bürgerschafts-Drs. 14/627	(Restexemplare)
20. Jahresbericht 1997, Bürgerschafts-Drs. 14/1005	(vergriffen)
21. Jahresbericht 1998, Bürgerschafts-Drs. 14/1399	(vergriffen)

Broschüre "Tips zum Adressenhandel und gegen die Werbepapierflut im Briefkasten"

Broschüre "Mobilfunk und Datenschutz"

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

Faltblatt "Der betriebliche Datenschutzbeauftragte"

Faltblatt "Handels- und Wirtschaftsauskunfteien"

Broschüre "Datenschutz in der Freien Hansestadt Bremen"

Broschüre "Datenschutz bei WindowsNT"

BfD – Info 1 – Bundesdatenschutzgesetz – Text und Erläuterungen

BfD – Info 2 – Der Bürger und seine Daten

20. Index