17. Tätigkeitsbericht
des
Hamburgischen Datenschutzbeauftragten
zugleich
Tätigkeitsbericht der Aufsichtsbehörde
für den nicht öffentlichen Bereich
1998/1999

vorgelegt im Februar 2000

(Redaktionsschluß: 1. Dezember 1999)

Dr. Hans-Hermann Schrader

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Baumwall 7 · 20459 Hamburg · Tel.: 428412047
Auflage: 2.500 Exemplare
Druck:Lütcke & Wulff, 20097 Hamburg

INHALTSVERZEICHNIS

Vorbemerkung

Nach dem 16. Tätigkeitsbericht (TB) zum Berichtsjahr 1997 wird nun erstmals ein Zweijahresbericht – über die Berichtsjahre 1998 und 1999 – vorgelegt. Gemäß dem Hamburgischen Datenschutzgesetz mit den Änderungen vom März 1997 erstattet der Hamburgische Datenschutzbeauftragte „mindestens alle zwei Jahre“ Senat und Bürgerschaft einen Tätigkeitsbericht. Im Februar 1999 habe ich einen Zwischenbericht über wichtige Themen aus dem Jahr 1998 veröffentlicht.

Für diesen Tätigkeitsbericht haben wir das Schwerpunktthema „Mehr Service – weniger Datenschutz?“ gewählt. In der Einleitung zum 16. TB wurde bereits dargestellt, daß es zur Kundenorientierung nicht nur in der Wirtschaft, sondern ebenso in der Verwaltung gehört, den vielfach unterschiedlichen Datenschutzbelangen der Bürgerinnen und Bürger Rechnung zu tragen. Dem würde es entsprechen, nicht nur jeweils eine Einheitsregelung für alle zu treffen, sondern die von uns im 16. TB beschriebenen Wahlmöglichkeiten offenzuhalten.

Inzwischen führt die Kundenorientierung in Wirtschaft und Verwaltung jedoch zunehmend dazu, neue Formen der Verarbeitung personenbezogener Daten als bessere Serviceleistung anzupreisen, ohne dabei von vornherein den Datenschutz zu berücksichtigen oder sogar Wahlmöglichkeiten vorzusehen. Statt dessen gibt es immer wieder Fälle, in denen der bisher erreichte Datenschutz verringert wird oder ganz abhanden kommt.

Diese Entwicklung wird im 1. Abschnitt dieses Tätigkeitsberichts verdeutlicht; dabei wird auch dargestellt, daß bei mehr Service durchaus ein wirksamer Datenschutz möglich ist. Zusätzlich zu den nachstehend genannten wichtigen Beispielen werden in den einzelnen Abschnitten des Tätigkeitsberichts die dort jeweils einschlägigen Fälle behandelt (siehe außerdem im Stichwortverzeichnis bei „Service“).

Unser eigener Service für die Bürgerinnen und Bürger – mit unserer allgemeinen Beratung, der Betreuung der zahlreichen Eingaben und unserer Öffentlichkeitsarbeit – sowie die Entwicklung der Dienststelle werden am Ende dieses Tätigkeitsberichts wiedergegeben.

Schwerpunktthema

1. Mehr Service – weniger Datenschutz?

Wirtschaft und Verwaltung bieten den Kunden mit Hilfe neuer Informationstechniken häufig zusätzlichen Service an, ohne damit verbundene Datenschutzrisiken deutlich zu machen oder auszuschließen oder dem Kunden die Wahl zwischen dem Servicegewinn und besserem Datenschutz zu überlassen.

In allen Bereichen der Gesellschaft – in der öffentlichen Verwaltung, der Wirtschaft, aber auch auf den Gebieten von Freizeit und Kultur – wird der „Kunde“ mit immer mehr Service umworben. Hintergrund ist zum einen der schärfer werdende Wettbewerb, zum anderen aber auch die Notwendigkeit, knapper werdende Ressourcen besser zu nutzen. Die Entwicklung der Technik ermöglicht es heute, dem Einzelnen Angebote zu machen, die vor kurzer Zeit noch nicht im Entferntesten realisierbar waren.

Diese neuen technischen Möglichkeiten treffen zusammen mit einer verstärkten Betonung des Servicegedankens sowohl bei öffentlichen Stellen als auch bei privaten Unternehmen. Die Anbieter der Dienstleistungen versuchen, tatsächlichen oder angenommenen Kundenbedürfnissen soweit wie möglich zu entsprechen. In diesem Sinne streben sie an, den Kunden möglichst schnell und bequem zu bedienen und zudem die Qualität der Dienstleistungen zu verbessern. Viele Kunden erwarten einen möglichst umfassenden und bequemen Service. Dabei sind jedoch die Ansprüche im Einzelfall sehr unterschiedlich. So nutzt bisher nur eine verhältnismäßig kleine – wenn auch zunehmende – Minderheit die Möglichkeit, Dienstleistungen elektronisch über das Internet abzuwickeln. Für andere steht die Frage im Vordergrund, daß sie Dienste ortsunabhängig, d.h. nicht nur bei einer „Filiale“ in Anspruch nehmen können.

So angenehm diese Erleichterungen des Alltags sein mögen – sie dürfen nicht darüber hinwegtäuschen, daß damit auch Nachteile verbunden sein können. Mancher Service setzt die Verfügbarkeit personenbezogener Daten voraus, bei anderen Angeboten entstehen elektronische Spuren, die differenzierte Rückschlüsse auf die Interessen und das Verhalten der Kunden zulassen. Diese Nachteile ergeben sich zum Teil daraus, daß bestimmte Serviceleistungen nicht nur denjenigen angeboten werden, die sich dafür interessieren, sondern (auch aus Kostengründen) generell für alle Kunden vorgehalten werden.

Wir haben uns im Berichtszeitraum insbesondere mit den datenschutzrechtlichen Konsequenzen der neuen technischen Möglichkeiten auseinandergesetzt. Dabei hat sich herausgestellt, daß der Servicegewinn sehr unterschiedlich ist und dementsprechend auch rechtlich differenziert betrachtet werden muß. Nur in den seltensten Fällen wird die Anwendung oder Ausweitung automatisierter Datenverarbeitung zur Verbesserung des Service unzulässig sein, viel häufiger läßt sich mit etwas Phantasie und Beteiligung der Betroffenen ein alle Seiten zufriedenstellendes Ergebnis erzielen. Die nachstehenden Beispiele zeigen deutlich, daß es kaum möglich ist, generelle Aussagen darüber zu treffen, mit welchen Schutzmaßnahmen dem jeweiligen Datenschutzrisiko begegnet werden kann. Bis auf die Ausnahme, daß ein Vorhaben – wie die Videoüberwachung von Kinderspielplätzen (siehe 1.2.1) – am Datenschutz scheitert, finden sich fast immer technische oder rechtliche Schutzmaßnahmen bis hin zur Einwilligung der Betroffenen. In der Regel gehen diesen Lösungen eingehende Verhandlungen der datenverarbeitenden Stelle mit uns voraus.

Die folgende Darstellung orientiert sich an der Art des Servicegewinns für den Kunden: Das Serviceangebot kann dem Kunden räumlich näher gebracht werden, es kann ein neues zusätzliches Angebot sein oder dem Kunden die Nutzung erleichtern und bequemer machen.

1.1 Servicegewinn: Der Kunde wird überall bedient

Die technische Entwicklung, insbesondere die zunehmende Vernetzung, macht es möglich, daß Bürger und Kunden nicht länger angewiesen sind auf „ihre“ örtlich zuständige Behörde oder Filiale / Geschäftsstelle. Auch Ämter oder Filialen an anderen Orten, z.B. am Arbeits-, Freizeit- oder Urlaubsort bieten den gewünschten Service – und zwar auch dann, wenn dies detaillierte Informationen über frühere Vorgänge voraussetzt.

1.1.1 Dezentralisierung der Ausländerbehörde

Seit November 1998 werden schrittweise Ausländerdienststellen in den Bezirken eingerichtet („Teil-Dezentralisierung der Ausländerbehörde“). Sie übernehmen die Sachbearbeitung für diejenigen Ausländer, die eine Aufenthaltsgenehmigung besitzen und im Bezirk wohnen (bisher wurden alle Ausländerangelegenheiten zentral in der Ausländerbehörde bearbeitet). Diese neue örtliche Zuständigkeit der einzelnen Bezirke wird jedoch modifiziert durch einen erweiterten Zugriff der Sachbearbeiter auf die gemeinsame automatisierte Ausländerdatei PAULA der Behörde für Inneres und der Bezirksämter:

Servicegewinn

Zur Übertragung von Aufenthaltsgenehmigungen in ein neues Paßdokument, zur Verlängerung eines Visums für Touristen und Geschäftsreisende sowie zur Verlängerung von Reiseausweisen für anerkannte Flüchtlinge sollen die ausländischen Staatsangehörigen nicht allein auf „ihre“ örtliche Dienststelle
angewiesen sein. Die Zuständigkeitsanordnung des Senats sieht insoweit vielmehr eine „partielle Allzuständigkeit“ vor, d.h. die genannten Dienstleistungen stehen jedem Ausländer in allen Bezirken zur Verfügung. Darüber hinaus
sollen die bezirklichen Dienststellen den Ausländern aber auch in anderen Angelegenheiten qualifiziert Auskunft geben können. Dazu wird den – eigentlich örtlich nicht zuständigen – Sachbearbeitern der lesende und schreibende Zugriff auf alle Daten der gemeinsamen Hamburger Ausländerdatei eröffnet. Der Zugriff soll z.B. zulässig sein, wenn ein „bezirksfremder“ Ausländer persönlich vorspricht oder die Sachbearbeitung Informationen über einen in einem anderen Bezirk wohnenden Ausländer – z.B. einen Familienangehörigen – erfordert.

Datenschutzrisiko

Durch die bezirksübergreifenden Lese- und Schreibrechte können rund 100 Sachbearbeiter, Sachgebietsleiter und Rechtsreferenten der Bezirke alle Informationen über alle Ausländer in Hamburg zur Kenntnis nehmen. Dies bezieht sich nicht nur auf die Ausländer mit einer Aufenthaltsgenehmigung, für die nun die Bezirksämter zuständig sind, sondern auch auf alle Asylbewerber, Bürgerkriegsflüchtlinge, Ausgewiesene, Abschiebehäftlinge usw., für die nach wie vor allein die Behörde für Inneres zuständig bleibt. Durch die Einräumung von Schreibrechten für bestimmte Zwecke können die bezirklichen Sachbearbeiter alle diese Daten faktisch auch verändern. Darin liegt eine nicht unerhebliche Mißbrauchsgefahr. Verschärfend kommt hinzu, daß die Dezentralisierung der Ausländer-Sachbearbeitung auf 10 bezirkliche Standorte auch das Risiko widerrechtlicher Zugriffe durch Dritte – seien es Bezirksamtsmitarbeiter, Wartungstechniker, Reinigungskräfte oder Einbrecher – wesentlich erhöht.

Dabei ist zu berücksichtigen, daß es sich bei ausländerrechtlichen Angelegenheiten für die Betroffenen nicht selten um existentielle Entscheidungen handelt. Die Vergangenheit hat gezeigt, daß dabei auch Bestechung und Bestechlichkeit nicht ausgeschlossen werden können. Schließlich muß auch das mögliche Interesse ausländischer Geheimdienste oder politischer Gegner gerade gegenüber Asylbewerbern und anerkannten politischen Flüchtlingen in die Risikoanalyse einbezogen werden.

Der Servicegewinn für den „bezirksfremden“ ausländischen Staatsangehörigen ist also unmittelbar verbunden mit einem erhöhten datenschutzrechtlichen Gefährdungspotential für alle ausländischen Staatsangehörigen in Hamburg.

Schutzmaßnahmen

Wir haben die (Teil-)Dezentralisierung ausländerbehördlicher Aufgaben intensiv begleitet und sowohl an der Zuständigkeitsanordnung als auch an der Rechtsverordnung nach §11 a HmbDSB zur gemeinsamen automatisierten Datei im Ausländer- und Asylwesen mitgewirkt. Die Behörde für Inneres lehnte es als zu teuer ab, die bestehende PAULA-Datei so umzustrukturieren, daß nur die für den jeweiligen Bearbeitungszweck erforderlichen Daten bereitgestellt werden. Im Entwurf der Rechtsverordnung nach §11a HmbDSG konnte aber festgelegt werden, daß alle Datenzugriffe durch Paßwort geschützt und protokolliert werden. Der über die Kurzauskunft (Eingangsmaske) hinausgehende lesende Zugriff ist technisch an die automatisch protokollierte Angabe des Verarbeitungszwecks (Schlüsselziffer) gebunden. Die Behörde für Inneres hat ein Konzept zur Auswertung der Protokolle zugesagt. Die notwendigen Stichprobenprüfungen müssen einen bestimmten Umfang haben, um wenigstens eine minimale Abschreckungswirkung gegen Mißbrauch zu entfalten.

Auch wenn einzuräumen ist, daß schon die bisherige zentrale Ausländerverwaltung jedem Sachbearbeiter einen umfassenden, allerdings unprotokollierten Datenzugriff auf alle PAULA-Daten ermöglichte, können die erreichten Datenschutzmaßnahmen insgesamt kaum befriedigen.

1.1.2 Überregionaler Datenzugriff der AOK-Geschäftsstellen

Das Problem des umfassenden Zugriffs aller Hamburger AOK-Geschäftsstellen auf alle Daten aller Versicherten der AOK Hamburg wurde mehrfach beschrieben (zuletzt 16.TB, 6.2.1). Im Berichtszeitraum hat es weitere Bemühungen um Datenschutzverbesserungen gegeben.

Servicegewinn

Jede versicherte Person kann im Bereich der AOK Hamburg in jeder Geschäftsstelle vorsprechen und seine Angelegenheiten bearbeitet bekommen. So kann der Versicherte, der in Bergedorf wohnt und in Altona arbeitet, in der Geschäftsstelle Ottensen die individuellen Voraussetzungen für eine Kostenerstattung seiner Kontaktlinsen klären, die Rechnung des Optikers einreichen und eine Abrechnungsanweisung durch die AOK-Sachbearbeiterin veranlassen. Dasselbe kann der Versicherte auch anläßlich eines Verwandtenbesuchs in Wandsbek bei der dortigen Geschäftsstelle erreichen.

Außerhalb Hamburgs wurden die Zuständigkeitsbereiche einer AOK durch Fusionen zu einer Landes-AOK erheblich erweitert; dadurch wurde auch die Geschäftsstellen-Auswahl für die Versicherten wesentlich vergrößert.

Datenschutzrisiko

Je größer der Zuständigkeitbereich einer Landes-AOK und die Zahl der von ihr unterhaltenen Geschäftsstellen, desto mehr AOK-Mitarbeiterinnen und Mitarbeiter haben Zugriff auf alle Leistungsdaten von Tausenden von Versicherten, mit denen sie in der Mehrzahl niemals etwas zu tun haben werden. Auch ist ein großer Teil der Bevölkerung bei der AOK versichert. Die AOK-Mitarbeiterin in einer Geschäftsstelle hat also durchaus die Chance, sensible Gesundheitsdaten von Freunden und Bekannten zu lesen, die in einem ganz anderen Stadtteil wohnen. Solche Zugriffe werden nicht protokolliert und sind technisch nicht beschränkt.

Schutzmaßnahmen

Die versicherte Person sollte selbst auswählen, welche Geschäftsstelle(n) Zugriff auf die Versichertendaten haben darf bzw. dürfen. Der Kunde sollte also zwischen Servicegewinn und Datenschutzrisiko nach seinen eigenen Interessen abwägen können. Die AOK müßte diese Entscheidung technisch in der Weise umsetzen, daß die nicht ausgewählten Geschäftsstellen keinen Zugang zu den Versichertendaten im Einzelnen bekommen. Denn ein Widerspruch des Versicherten gegen den Zugriff „nicht-zuständiger" Geschäftsstellen auf seine Daten ist letztlich nur dann wirksam, wenn die Zugriffsmöglichkeiten der nicht-zuständigen Geschäftsstelle technisch gesperrt bzw. wenn sie nur für die zuständige(n) Geschäftsstelle(n) freigeschaltet werden.

Zwischen der AOK Hamburg, der Behörde für Arbeit, Gesundheit und Soziales und uns wurde vereinbart, daß Alt-Versicherte dem Zugriff anderer Geschäftsstellen ausdrücklich widersprechen können und Neu-Versicherte von Anfang an die zuständige Geschäftsstelle frei wählen (vgl. 16. TB, 6.2.1.) Dies trägt der Selbstbestimmung des Versicherten und den rechtlichen Vorgaben des Sozialgesetzbuches Rechnung.

Im Berichtszeitraum bemühten sich sowohl die AOK-Hamburg beim AOK-Bundesverband als auch wir im zuständigen Bund-Länder-Arbeitskreis um eine bundesweite Umsetzung dieses „Hamburger Modells". Während sich die Datenschutzbeauftragten im wesentlichen einig sind, macht der AOK-Bundesverband noch immer vor allem technische Probleme geltend. Die Datenschutzbeauftragten haben ihre technische Kompetenz für eine Beratung angeboten. Der im Bund-Länder-Arbeitskreis anwesende Vertreter des AOK-Bundesverbandes sagte eine weitere Erörterung im Bundesverband und eine Konkretisierung der technischen Probleme zu. Das vom Bundestag Anfang November 1999 beschlossene Gesundheitsreformgesetz 2000 machte im neuen §284 Abs. 4 SGB V den geschäftsstellenübergreifenden Zugriff auf Versicherten-Sozialdaten nun vom schriftlichen Einverständnis der betroffenen Person abhängig (siehe Kasten). Das Ergebnis der Verhandlungen im Bundesrat steht allerdings noch aus.

§284 Abs. 4 SGB V-E:

Geschäftsstellenübergreifend darf eine Krankenkasse ohne schriftliches Einverständnis des Versicherten nur auf die Daten zugreifen, die zur Feststellung des Versichertenverhältnisses und der Mitgliedschaft erforderlich sind. Darüber hinausgehende Zugriffe auf Sozialdaten des Versicherten sind nur der für diesen Versicherten zuständigen Geschäftsstelle zu ermöglichen, soweit der Versicherte nicht schriftlich diesem Zugriff durch weitere oder alle Geschäftsstellen der Krankenkasse eingewillligt hat. Die Einwilligung muß den Zweck des Zugriffs auf die Sozialdaten nach Satz 2 und die Dauer der Aufbewahrungsfrist enthalten.

1.2 Servicegewinn: Der Kunde erhält zusätzliche Leistungen

Sowohl die rasante Entwicklung auf dem Gebiet der Technik als auch die gestiegenen Serviceanforderungen in allen Bereichen haben dazu geführt, daß einerseits die bereits bestehenden Angebote deutlich verbessert und andererseits völlig neue Ideen verwirklicht werden sollen.

1.2.1 Videoüberwachung von Kinderspielplätzen

Eine Hamburger Wohnungsgesellschaft hatte Planungsentwürfe vorgelegt, nach denen in einem Neubaugebiet auf dem dortigen Kinderspielplatz Kameras installiert werden sollten. Die detailscharfen Aufnahmen der dort spielenden Kinder sollten in das lokale Kabelfernsehnetz der in dem Gebiet befindlichen Haushalte eingespeist werden.

Servicegewinn

Das Vorhaben hätte für die Eltern von Kleinkindern den unbestreitbaren Vorteil, daß sie die Kinder nicht mehr begleiten müssen und dennoch wissen, was ihr Nachwuchs in jedem Augenblick auf dem Spielplatz tut. Mütter und Väter würden in die Lage versetzt, ihre Zeit „doppelt“ zu nutzen. Sie könnten, ohne ihre Kinder aus den Augen zu verlieren, nebenher Haus- oder Berufsarbeit erledigen. Verkäufer und Vermieter von Wohnungen, die diesen Aspekt in ihre Werbung aufnehmen, würden unter Umständen viel Erfolg bei Familien mit kleinen Kindern haben. Aber auch andere potentielle Kunden, wie z.B. ältere Personen, könnten sich einen erhöhten Sicherheitsgewinn durch derartige Einrichtungen versprechen, die auch den zunehmenden Vandalismus bekämpfen helfen könnten.

Datenschutzrisiko

Bei all diesen Vorteilen für die Betroffenen darf jedoch nicht außer Acht gelassen werden, daß erhebliche Einschränkungen für die Persönlichkeitsrechte zu befürchten sind. Die Kinder können auf dem Spielplatz bei ständiger und totaler Kontrolle nicht mehr unbeobachtet spielen. Darüber hinaus können auch größere Kinder und Dritte auf dem Spielplatz von jedem Haushalt des Gebietes aus beobachtet werden. Das bedeutet, daß jederzeit von vielen Personen ohne Kenntnis und konkrete Einwilligung der Betroffenen eine Kontrolle über die Geschehnisse auf dem Spielplatz ausgeübt werden könnte. Nicht ausgeschlossen ist daher auch die Stigmatisierung von Kindern, die normale Streitereien austragen und bei etwaigen Handgreiflichkeiten beobachtet werden können. Ebenso könnte die Kabelübertragung mißbräuchlich zur Vorbereitung krimineller Aktionen genutzt werden. Zwar war von den Planern vorgesehen, die Bilder nur direkt zu übertragen und an zentraler Stelle keine Aufzeichnungen zu machen. Es wäre den angeschlossenen Haushalten jedoch ohne weiteres möglich, Videoaufzeichnungen mit den damit verbundenen Mißbrauchsmöglichkeiten zu fertigen.

Rechtlich ist davon auszugehen, daß neben den Datenschutzbestimmungen jedenfalls §22 Kunsturhebergesetz (KunstUrhG) gilt. Danach dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.

Schutzmaßnahmen

Man kann durchaus davon ausgehen, daß diejenigen, die in das Gebiet ziehen und den vorgesehenen Service gutheißen oder sogar bewußt in Anspruch nehmen möchten, auch ihre generelle Einwilligung in die Videoübertragung erteilen. Es ist jedoch nicht auszuschließen, daß sich selbst die Eltern kleinerer Kinder nicht über die Tragweite dieser Entscheidung im Klaren sind. Insbesondere wird wohl nicht berücksichtigt werden, daß nicht nur sie, sondern auch jeder andere Haushalt ihr Kind – und das auch bei nicht gewünschten Verhaltensweisen – beobachten kann.

Bei der Überlegung, welche Schutzmaßnahmen hierbei aus datenschutzrechtlicher Sicht gefordert werden können, sind nur Lösungen denkbar, die sich als weltfremd und daher nicht konsequent durchführbar erweisen:

Hinweisschilder: Auf dem öffentlich zugänglichen Spielplatz werden auch andere Kinder spielen, für die nicht die Einwilligung in die Videoübertragung vorliegt. In diesen Fällen würde auf jeden Fall ein Verstoß gegen §22 KunstUrhG vorliegen. Das kann auch nicht dadurch umgangen werden, daß deutliche Hinweisschilder auf sichtbare Kameras aufmerksam machen. Die Hinweisschilder würden zum einen die erforderliche Einwilligung nicht ersetzen, zum anderen könnten aber auch gerade Kinder deren Bedeutung nicht erfassen und nicht selbständig in die Übertragung einwilligen.

Einwilligung: Nur die theoretisch denkbare, aber praktisch undurchführbare Einholung der Einwilligung der außerhalb der Anlage wohnenden Eltern könnte hier Abhilfe schaffen. Auch ein Ausschluß von der Benutzung des Spielplatzes wird angesichts der Tatsache, daß die Bewohnerkinder auch Besucher mitbringen, nicht möglich sein.

Fallweise Aktivierung der Kameras: Ein Ein- und Ausschalten der Kameras je nach Vorliegen rechtswirksamer Einwillungen ist theoretisch denkbar, erscheint praktisch jedoch ebenfalls realititätsfremd. Jede andere Ausgestaltung aber muß als Verstoß gegen §22 KunstUrhG angesehen werden und ist damit unzulässig.

Aufgrund unserer Hinweise hat die Wohnungsgesellschaft mitgeteilt, daß sie ihr Vorhaben zunächst zurückstellt und nur datenschutzkonform nach Abstimmung mit uns umsetzen wird.

1.2.2 Kundenzentren in der Bezirksverwaltung

Auch in den Kundenzentren der Bezirksämter wird dem Bürger durch die Zusammenfassung verschiedener Aufgaben an einem Ort ein zusätzlicher Service angeboten.

Servicegewinn

Grundidee eines Kundenzentrums der Bezirksverwaltung ist es, möglichst viele Verwaltungsleistungen aus einer Hand anzubieten. Die Bürger sollen nicht mehr gezwungen sein, auf weiten Wegen mit viel Zeitaufwand unterschiedliche Angebote wahrzunehmen oder auch Pflichten zu erledigen.

Das Bezirksamt Hamburg-Nord hat im Rahmen eines Projekts bereits Anfang des Jahres 1998 ein Kundenzentrum eingerichtet, in dem von einem Sachbearbeiter an einem Arbeitsplatz folgende Verwaltungsangelegenheiten erledigt werden können:

- Meldewesen, Wohngeld, Unterhaltssicherung und Erziehungsgeld
- Erledigung von Kirchenaustritten (bisher Standesamt)
- Verlängerung von Schwerbehindertenausweisen (bisher Sozialamt)
- Namens- und Anschriftenänderungen von Kfz-Scheinen (bisher Landesbetrieb Verkehr)
- Ausgabe von Fischereischeinen und Angelkarten (bisher Wirtschafts- und Ordnungsamt)
- Beglaubigung elektronischer Signaturen (neu)
- Umweltberatung
- Verkauf von Radwanderkarten und Kartenmaterial auf CD-ROM (bisher Kataster- und Vermessungsamt).

Nach dem Vorbild des Kundenzentrums Hamburg-Nord sollen noch bis Ende 1999/Anfang 2000 weitere Kundenzentren in Altona, Wandsbek, Bergedorf und Harburg eröffnet werden. Insgesamt haben sich die Bezirksämter zum Ziel gesetzt, mittelfristig in allen Regionen (Kerngebiete, Ortsamtsbereiche, Einzugsbereiche großer Ortsdienststellen) Bürgerservice-Einrichtungen mit erweitertem Leistungsangebot vorzusehen. Auf jeden Fall soll aber bis 2001 jeweils mindestens ein Kundenzentrum pro Bezirk verwirklicht werden.

Obwohl nicht jeder Bürger, der eine der dort angebotenen Leistungen in Anspruch nehmen möchte, gleichzeitig auch andere nutzt, ist die räumliche Zusammenfassung verschiedenster Leistungen sicherlich aus Gründen der Bürgerfreundlichkeit positiv zu bewerten.

Datenschutzrisiko

Die Bündelung von Verwaltungsleistungen an einem Ort birgt jedoch die Gefahr, daß die Mitarbeiter der Kundenzentren umfassenderen Zugriff auf die Daten der Bürger erhalten, als dies bei der räumlichen und fachlichen Trennung der Zuständigkeiten der Fall wäre. Zwar kann man davon ausgehen, daß die Bearbeiter aufgrund der jeweils für das einzelne Sachgebiet einschlägigen Rechtsgrundlage tätig werden. Die Möglichkeiten eines Mißbrauchs der Datenbestände erhöhen sich jedoch deutlich.

Darüber hinaus war es bisher sogar in den sensiblen Bereichen wie Wohngeld, Unterhaltssicherung oder Erziehungsgeld für den Bürger kaum möglich, im Kundenzentrum mit dem zuständigen Sachbearbeiter ein unbelauschbares Gespräch zu führen.

Schutzmaßnahmen

Insbesondere in Fällen, in denen die Bürger schwierige finanzielle und persönliche Verhältnisse darlegen, sind hohe Anforderungen an die Einhaltung der Vertraulichkeit zu stellen. Sowohl das Senatsamt für Bezirksangelegenheiten als auch das Bezirksamt Hamburg-Nord haben auf unsere Kritik reagiert.

Das Senatsamt hat im „Rahmenkonzept zur Errichtung von Kundenzentren" festgelegt, daß die besonders sensiblen Bereiche Wohngeld, Erziehungsgeld und Unterhaltssicherung weiterhin spezialisiert im Fachamt betreut werden sollen. Außerdem wird im Kundenzentrum Hamburg-Nord das Angebot an die „Kunden", ihre Angelegenheit mit dem zuständigen Sachbearbeiter in einem gesonderten Raum zu besprechen, durch deutliche Hinweisschilder und die Planung von zwei neuen separaten Besprechungsräumen umgesetzt.

Technisch realisierbar sind auch örtliche und fachliche Zugriffsbeschränkungen in den EDV-Systemen, die nur durchbrochen werden dürfen, wenn der Bürger ausdrücklich damit einverstanden ist. In Betracht kommt auch die Aufzeichnung von Zugriffslegitimationen in jedem Einzelfall. Insbesondere haben wir gefordert, daß unzulässige Datentransfers und Datenabgleiche ausgeschlossen und die Prinzipien der Mandantenfähigkeit (siehe Kasten) des Systems eingehalten werden. Damit verbunden sind möglicherweise eingeschränkte Zugriffsrechte für die einzelnen Sachbearbeiter und die Protokollierung des lesenden Zugriffs, um damit der Gefahr zu begegnen, daß unzulässigerweise Informationen aus verschiedenen Systemen zusammengeführt werden.

Mandantenfähige Informationssysteme

Ein wesentliches Kriterium für die Zulässigkeit der Verarbeitung personenbezogener Daten ist das Erforderlichkeitsprinzip: Daten dürfen nur dann verarbeitet werden, wenn dies zur Erfüllung der Aufgabe bzw. zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist. Die Umsetzung dieses Prinzips durch konkrete technische und organisatorische Maßnahmen ist um so wichtiger, je umfassender die Datenmengen sind, auf die arbeitsteilig zugegriffen wird, und je größer die Sensibilität der Daten ist. Bei Datenbankanwendungen, die auf einer unternehmens- oder behördenweit zentralen Datenhaltung basieren, kommt diesem Konzept besondere Bedeutung zu. Der Zugriff auf die Daten muß entsprechend der arbeitsteiligen Abgrenzung eingeschränkt werden, etwa nach örtlicher Zuständigkeit bestimmter Zweigstellen oder Ämter, nach Zuständigkeit anhand der Namen – z.B. für die Anfangsbuchstaben A bis E der Nachnamen – oder anderer Merkmale der gespeicherten Personen. Systeme, die eine solche Abgrenzung ermöglichen, werden als *mandantenfähig* bezeichnet.

Aus technischer Sicht kommt eine Umsetzung dieser Maßnahme auf zwei Ebenen in Betracht: Zum einen kann die Mandantenfähigkeit auf der Ebene der Anwendung durch eine entsprechende Programmierung gewährleistet werden, zum anderen können Mechanismen direkt auf der Ebene des Datenbanksystems genutzt werden. Letzteres ist aus Gründen der Sicherheit und der Antwortzeiten zu bevorzugen (weitere Details siehe 13. TB, 3.9).

1.3 Servicegewinn: Der Kunde erhält Leistungen bequemer

Online-Dienste und Internet ermöglichen neue Dienstleistungen, etwa die elektronische Abwicklung von Behördenkontakten und von Kauf- und Zahlungsvorgängen, und ersparen den Kunden damit Wege und Zeit.

1.3.1 Kfz-Zulassung über das Internet

Die An- und Abmeldung von Kraftfahrzeugen ist bislang für die Bürgerinnen und Bürger ein zeitaufwendiges Geschäft. Trotz des Einsatzes automatisierter Verfahren müssen sie z.T. mehrere Stunden in Kfz-Zulassungsstellen zubringen.

Servicegewinn

Durch Nutzung des Internet wäre es möglich, daß Anträge online gestellt und Gebühren elektronisch bezahlt werden. Die Kunden müßten lediglich zum Abholen der Papiere und der Kfz-Kennzeichen persönlich erscheinen. Dabei könnten auch individuelle Wünsche (z.B. „Wunschkennzeichen“) berücksichtigt werden. In Hamburg wird ein derartiges Verfahren bereits für bestimmte Großkunden (Kfz-Händler) praktiziert, die die Fahrzeugdaten per E-Mail an das Landesamt für Informationstechnik (LIT) senden. Diese Daten stehen dann der Zulassungsstelle zur weiteren Bearbeitung zur Verfügung.

Von seiten des Autohandels ist zudem vorgeschlagen worden, daß Autohäuser und Zulassungsdienste online auf die Computer-Systeme der Kfz-Zulassungsstellen zugreifen können, Zulassungsdaten in die Computer der Behörde eingeben und anschließend die Unterlagen für die Zulassung ausfertigen und den Kunden aushändigen. Die Unternehmen würden die Kundendaten erheben, überprüfen (z.B. durch Anfrage beim Melderegister und beim Kraftfahrt-Bundesamt) und im eigenen Bereich speichern. Nach der Online-Registrierung bei der Zulassungsstelle würden sie die Fahrzeugpapiere bedrucken, abstempeln, die Kennzeichen plakettieren und beides den Kunden aushändigen. Sie würden ferner die Versicherungsbestätigung überprüfen, Gebühren erheben und mit der Zulassungsstelle abrechnen.

Datenschutzrisiko

Geht es allein um die elektronische Übermittlung von Anträgen an die Zulassungsstellen, bestehen Risiken für die Vertraulichkeit und Authentizität: Wenn personenbezogene Daten über das Internet übertragen werden, können sie – da das Internet standardmäßig keine Sicherheitsmechanismen enthält – bei der Übertragung zwischen dem Computer des Kunden und dem Behördencomputer abgehört, verfälscht oder unterdrückt werden. Zudem bereitet die zweifelsfreie Feststellung der Identität der Kommunikationspartner Schwierigkeiten. Nicht zu vernachlässigen ist darüber hinaus, daß derartige Verwaltungsverfahren Schnittstellen der behördlichen Computer zum Internet voraussetzen, wodurch zwangsläufig zusätzliche Risiken für die Sicherheit der behördlichen Datenverarbeitung entstehen.

Wenn darüber hinaus der gesamte Zulassungsvorgang von privaten Autohäusern übernommen würde, liefe dies auf eine – rechtlich zweifelhafte – Privatisierung eines bisher hoheitlich betriebenen Verwaltungsverfahrens hinaus mit der datenschutzrechtlichen Konsequenz, daß private Stellen einen Online-Zugriff auf behördliche Register erhielten. Die Firmen unterlägen im Hinblick auf die geschäftliche Verwertbarkeit der auf diese Weise zugänglichen Daten einem kaum lösbaren Interessenkonflikt. Ferner würde die ohnehin schon schwierige datenschutzrechtliche Überwachung zusätzlich erschwert.

Schutzmaßnahmen

Die Übermittlung der Antragsdaten an die Zulassungsstelle, die für das Zulassungsverfahren voll verantwortlich bleibt, erscheint aus datenschutzrechtlicher Sicht vertretbar, wenn die oben beschriebenen Risiken durch geeignete Schutzmaßnahmen weitgehend ausgeschlossen werden: Die Abwicklung behördlicher Kommunikation mit den Kundinnen und Kunden der Verwaltung über das Internet setzt stets eine Sicherheitsinfrastruktur voraus, mit der sowohl die Vertraulichkeit der verarbeiteten Daten als auch die Authentizität der Kommunikationspartner sichergestellt werden kann. Kernstücke einer derartigen Sicherheitsinfrastruktur wären kryptographische Verschlüsselungsverfahren und Mechanismen der digitalen Signatur.

Solange derartige Mechanismen noch nicht zur Verfügung stehen, muß sich die elektronische Unterstützung von Verwaltungsleistungen über das Internet für den Bürger darauf beschränken, daß Formulare im Internet zum Abruf bereitgestellt werden. Lediglich soweit ein Dienst auf wenige Kommunikationspartner beschränkt werden kann (etwa Autofirmen bzw. Kfz-Zulassungsdienste), können die Sicherheit und Authentizität der Kommunikation auch ohne digitale Signaturen sichergestellt werden (z.B. durch Verwendung von Benutzerkennungen und Paßwörtern, Einrichtung geschlossener Benutzergruppen).

Zur Sicherung der behördlichen Datenverarbeitung ist es zudem erforderlich, daß die internen Netzwerke durch Firewall-Systeme vom Internet abgeschottet werden. Ferner sind zusätzliche Sicherheitsmaßnahmen auf denjenigen Behörden-Computern erforderlich, auf die aus dem Internet zugegriffen werden kann.

Dagegen sind keine Maßnahmen ersichtlich, die die oben beschriebenen Bedenken gegen die Kfz-Zulassung durch Autohäuser ausräumen würden. In diesem Sinne hat sich auch der Bundesbeauftragte für den Datenschutz aufgrund einer Umfrage bei den Landesbeauftragten geäußert.

1.3.2 Elektronisches Bezahlen

Kunden, die über das Internet Dienstleistungen in Anspruch nehmen oder Waren bestellen, sind zur Zeit bei der Bezahlung weitgehend auf konventionelle Verfahren (Rechnung bzw. Abbuchung von Bank- bzw. Kreditkartenkonten) angewiesen. Dies ist einer der Gründe, warum sich elektronische Dienstleistungen bislang nicht in dem erwarteten Umfang haben durchsetzen können. Mit dem Datenschutz bei elektronischem Geld hat sich der Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder hinsichtlich der Anwendungsmöglichkeiten und Einsatzfelder näher befaßt (S. 34ff. in: Landesbeauftragter für den Datenschutz Mecklenburg-Vorpommern (Hrsg.), Datenschutzfreundliche Technologien 1998).

Servicegewinn

Electronic Commerce wird voraussichtlich der Durchbruch gelingen, wenn Bestell- und Bezahlvorgänge auf einfache Art technisch miteinander verknüpft und speziell ohne „Medienbruch“ abgewickelt werden können. Dies gilt gleichermaßen für größere Beträge, die etwa bei der elektronischen Bestellung von Waren fällig werden (Makro Payments), und für elektronisches „Kleingeld“, das insb. beim Abruf elektronischer Informationen zunehmende Bedeutung erhalten wird (Mikro Payments). Sowohl für Makro- als auch für Mikro Payments ist die Geldkarte des deutschen Kreditwesens als Bestandteil der EC-Karte ein interessanter Ansatz.

Um mit der Geldkarte im Internet bezahlen zu können, muß der Kunden-PC jedoch mit einem Chipkartenleser ausgestattet sein, mit dem das Guthaben auf dem Geldkartenchip gelesen und Beträge über das Internet auf ein entsprechendes Händlerterminal und dort auf eine Händlerkarte gebucht werden können. Das entsprechende Verfahren wurde 1999 vom Zentralen Kreditausschuß freigegeben. Trotz der Betragsgrenzen (derzeit können bis zu 400 DM als Guthaben auf der Geldkarte geladen werden) kann erwartet werden, daß dieses Verfahren an Bedeutung gewinnen wird, da allein in Deutschland mehr als 50 Millionen EC-Karten im Umlauf sind.

Datenschutzrisiko

Sowohl die Warenbestellung als auch ihre Bezahlung über das Internet bergen Risiken für die Vertraulichkeit der übertragenen Daten in sich (vgl. auch 3.3.1). Beim elektronischen Handel besteht zudem die Gefahr, daß unsichere Verfahren direkten wirtschaftlichen Schaden auslösen. Zudem wäre es datenschutzrechtlich sehr bedenklich, wenn sowohl das Verhalten der Kunden im Netz (z.B. das „Schmökern" in einem elektronischen Katalog) als auch ihr Zahlungsverhalten personenbezogene Spuren hinterlassen, die zu Verhaltensprofilen zusammengeführt werden können.

Schutzmaßnahmen

Während konventionelle elektronische Zahlungsverfahren wie beispielsweise Electronic Cash, Lastschriftverfahren oder Kreditkartenverfahren dazu führen, daß die Kunden den Händlern gegenüber zumindest ihre Kontronummer und Bankleitzahl und somit u.U. auch ihre Identität offenbaren müssen, bieten neuere elektronische Zahlungsverfahren die Chance, daß der Kunde – wie beim Barkauf in der realen Welt – anonym bleiben kann. Dies gilt zumindest für reine Teledienste, bei denen keine Lieferanschrift zwecks Auslieferung bestellter Waren erforderlich ist.

Mit anonymen oder pseudonymen Bezahlverfahren läßt sich die Vorgabe aus §4 Abs. 1 Teledienstedatenschutzgesetz realisieren, wonach der Diensteanbieter dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen hat. Dies gilt u.a. auch für die Geldkarte, bei der der Kunde seine Identität gegenüber dem Händler nicht offenbaren muß. Damit die Anonymität auch gegenüber den Kreditinstituten gewährleistet ist, sollte das deutsche Kreditwesen zum einen auf die im Hintergrund gespeicherten Schattenkonten verzichten, die es ermöglichen, jede mit der Geldkarte getätigte Transaktion nachzuvollziehen. Zum anderen sollten die Banken und Sparkassen verstärkt Geldkarten ohne Personenbezug („White Cards") herausgeben. Es wäre dann allein die Entscheidung des Kunden, entweder die Geldkartenfunktion der personengebundenen EC-Karte oder eine anonyme White Card einzusetzen (16.TB 21.2).

1.4 Ausblick

Die Frage „Mehr Service – weniger Datenschutz?" richtet sich nicht nur an den Kunden und seine Entscheidungsfreiheit. Nicht selten hat gerade der Anbieter bzw. die datenverarbeitende Stelle selbst ein Interesse daran, daß neue technische Möglichkeiten umgesetzt werden. Der Servicegewinn für den Kunden wird jedenfalls dann eher zur Nebensache, ja zum „Köder", wenn sich der Anbieter von den neuen Möglichkeiten vor allem eigene Rationalisierungseffekte verspricht.

So wurde bei der gemeinsamen Datenbank für alle Ausländerdienststellen die „partielle Allzuständigkeit" und der Zugriff aller Sachbearbeiter auf sämtliche Daten eingeführt, um die Verwaltungsabläufe zu erleichtern und aufwendige technische Vorkehrungen zur Mandantenfähigkeit des Systems (s.o. Kasten) zu vermeiden. Der Servicegewinn ist dabei eher ein „Abfallprodukt". Etwas ähnliches gilt auch für die geschäftsstellenübergreifenden Zugriffe bei der AOK: Wäre der Kundenwille das vorherrschende Motiv, würde sich der AOK-Bundesverband nicht so schwer tun, diesen tatsächlich zu ermitteln und sicherheitstechnisch umzusetzen. Die Bürgerzentren in den Bezirksämtern versprechen Rationalisierungseffekte und folgen dem Motto „Kundenorientierung", ohne konkret den Bedarf nach den zusammengelegten Verwaltungsaufgaben ermittelt zu haben. Bei der Nutzung des Internet für die Kfz-Zulassung schließlich haben sicher beide Seiten Vorteile: die Zulassungsstelle und noch mehr der Kunde. Die elektronische Kfz-Zulassung zwischen Zulassungsstelle und Kfz-Händler hat allerdings den „Schönheitsfehler", daß der Händler der „ Kunde" ist, die übermittelten personenbezogenen Daten jedoch die des Autokäufers sind. In allen Fällen sind ungesicherte Datenübertragungen zu befürchten und zu vermeiden.

Die Frage nach dem Hauptnutznießer neuer Verfahren erklärt meist auch die sehr unterschiedliche Bereitschaft der datenverarbeitenden Stelle, datenschutzrechtliche und sicherungstechnische Rahmenbedingungen zu schaffen und dem Kunden selbst die Wahl zu lassen zwischen mehr Service und mehr Datenschutz. Aus Sicht des Grundrechts auf informationelle Selbstbestimmung sollte die Wahlfreiheit des Kunden Vorrang haben vor einem aufgedrängten, oft gar nicht genutzten Servicegewinn mit mehr oder weniger effektiven Sicherungsmaßnahmen. Das bedeutet ggf., daß der Kunde tatsächlich zwischen zwei Verfahren auswählen kann – dem alten sichereren bzw. Daten-"genügsamen" Verfahren, das aber umständlicher ist, und dem neuen riskanteren bzw. Daten-"hungrigeren" Verfahren, das dafür aber bequemer ist. Das Vorhalten zweier Verfahren – ggf. des alten und des neuen – nebeneinander ist jedoch vielfach nicht wirtschaftlich oder ablauftechnisch ausgeschlossen, so wie etwa beim Zugriff auf die Ausländerdatei. In diesen Fällen kann das gewünschte neue Verfahren nur eingeführt werden, wenn Datenschutz und Datensicherheit in angemessener Weise sichergestellt werden können.

Kann der Kunde frei zwischen verschiedenen Verfahren wählen wie beim elektronischen oder konventionellen Bezahlen oder bei der Auswahl zuständiger Geschäftsstellen, geht es vor allem um eine objektive Aufklärung über die jeweiligen Vor- und Nachteile einschließlich der mit den jeweiligen Lösungen verbundenen Datenschutzrisiken. Hier liegt auch eine Aufgabe der Datenschutz-Aufsichtsbehörden und der Verbraucherzentralen.

Richtige und ausreichende Information und Aufklärung müssen auch erfolgen, wenn die Einwilligung des Betroffenen die zusätzliche Datenverarbeitung rechtfertigen soll. Hier ist jeweils zu prüfen, ob die Betroffenen eine realistische Alternative haben, nein zu sagen, also die Einwilligung zu verweigern. An dieser Freiwilligkeit fehlt es, wenn sozialer Druck oder besondere Vergünstigungen die Einwilligung so sehr nahelegen, daß eine freie Willensentscheidung nicht gewährleistet erscheint (zur Einwilligungsproblematik siehe bereits ausführlich 14.TB, 1.2).

Insgesamt zeigen die vorstehenden Beispiele, daß die Euphorie über neue technische Möglichkeiten nicht in jedem Falle berechtigt ist. Vielmehr ist es eine datenschutzrechtliche wie gesellschaftspolitische Aufgabe, auch die Risiken und Nachteile für die informationelle Selbstbestimmung deutlich zu machen, sie der verantwortungsbewußten Abwägung der „Kunden" zugänglich zu machen und durchzusetzen, daß die datenverarbeitende Stelle sie technisch minimiert oder ausschließt.

Die Frage „Mehr Service – weniger Datenschutz?" eröffnet schließlich noch eine ganz andere Perspektive: mehr Service durch mehr Datenschutz ! Auch wenn viele Kunden Bequemlichkeit oder Zeitersparnis für wichtiger halten als zusätzlichen Datenschutz, steigt in der Gesellschaft das Bewußtsein für die Gefahren einer ausufernden elektronischen Datenverarbeitung. Es liegt deswegen durchaus nahe, erhöhte technische Sicherheit oder eine Umwandlung von personenbezogener in anonyme / pseudonyme Datenverarbeitung als eigenen Service anzubieten (15.TB, 3.1). Software, die sichere Einweg-Verschlüsselungen (Pseudonymisierungen) oder Verschlüsselungen für die Datenübermittlung in besonders anwenderfreundlicher Form verspricht, kann eine zunehmende Nachfrage erwarten. So ermöglicht die oben erwähnte „White Card" das anonyme elektronische Bezahlen; die Anonymität des Bargeldverkehrs bietet aber – bei entsprechender Infrastruktur – den Servicegewinn, daß der Kunde auf das Sammeln passender Münzen für Automaten verzichten kann.

Die Datenschutzbeauftragten verstehen sich auch hier als technikfördernde Beratungsinstanz und Informationsstelle für mehr Service **und** mehr Datenschutz.

Datenschutzrecht und -technik

2. Neues Datenschutzrecht

2.1 EG-Datenschutzrichtlinie und Bundesdatenschutzgesetz

Die Umsetzung der Richtlinie kommt mittlerweile voran.

Über vier Jahre nach Annahme der EG-Datenschutzrichtlinie am 24. Oktober 1995 ist die Umsetzungsfrist längst überschritten. Die Europäische Kommission hatte deshalb bereits Deutschland gerügt, weil die Anpassung des nationalen Datenschutzrechts noch nicht in Kraft gesetzt wurde.

Die Novellierung des Bundesdatenschutzgesetzes hat immerhin wesentliche Fortschritte gemacht. Nach mehreren Referentenentwürfen noch in der Zeit der früheren Bundesregierung und verbesserten Entwürfen unter der jetzigen Bundesregierung wird das Bundeskabinett den Gesetzentwurf voraussichtlich spätestens im Januar 2000 beschließen.

Die Datenschutzbeauftragten haben in ihrer Sonderkonferenz vom 15. Juli 1999 insbesondere gefordert,

– Ausnahmeregelungen zu begrenzen, z.B. keine langen Übergangszeiträume vorzusehen und nicht vielfältige Ausnahmen für den Sicherheitsbereich einzuführen

– die technischen und organisatorischen Maßnahmen zur Datensicherheit mit einer Festlegung der Schutzzwecke zu modernisieren statt grundsätzlich am bisherigen Katalog von Einzelmaßnahmen festzuhalten

– öffentlichen und nicht-öffentlichen Bereich gleich zu gewichten, z.B. bei der Unabhängigkeit der Datenschutzbeauftragten und der Aufsichtsbehörde sowie deren effektiven Einwirkungsbefugnissen

– die Videoüberwachung wirkungsvoll zu beschränken statt sie für jede Art der Aufgabenerfüllung zuzulassen (siehe dazu 7.3.1 und 23.)

– die aufgrund der neueren Rechtsprechung entstandene Strafbarkeitslücke zu schließen, damit die unbefugten Zugriffe auf Daten strafbar bleiben, die nicht jeder Person ohne rechtlich geregelte Voraussetzung zugänglich sind (siehe 13.4).

Über diese Hauptpunkte hinaus gibt es eine Vielzahl von Änderungswünschen der Datenschutzbeauftragten. Auch der Düsseldorfer Kreis der Obersten Aufsichtsbehörden für den Datenschutz in der Wirtschaft hatte sich zum Gesetzentwurf sehr kritisch geäußert. Es bleibt abzuwarten, ob die angekündigte Umgestaltung des gesamten Gesetzes zu einer verständlichen, modernen und effektiven Datenschutzregelung in einer 2. Stufe wirklich zeitnah angegangen wird. Die Datenschutzbeauftragten werden sich an diesem wichtigen Vorhaben weiter aktiv beteiligen.

2.2 Hamburgische Datenschutzvorschriften

2.2.1 Hamburgisches Datenschutzgesetz

Der vorgesehenen Novellierung ist weitgehend zuzustimmen.

Zur Anpassung an die EG-Datenschutzrichtlinie ist auch das Hamburgische Datenschutzgesetz erneut zu novellieren. Nach intensiver Vorbereitung seitens der Justizbehörde mit unserer Beteiligung ist der Gesetzentwurf in der Behördenabstimmung. Wichtige Punkte gemäß der Richtlinie sind u.a.

– der besondere Schutz sensibler Daten

– die Einführung behördlicher Datenschutzbeauftragter

– die neue Regelung der Übermittlungen ins Ausland

– die Verbesserungen bei der Benachrichtigung der Betroffenen

– die Erweiterung hinsichtlich der Auskunfts- und Nachberichtspflichten

– das grundsätzliche Verbot automatisierter Einzelentscheidungen zur Persönlichkeits- und Verhaltensbewertung.

Dem Gesetzentwurf kann aus unserer Sicht weitgehend zugestimmt werden. Statt der nun vorgesehenen fakultativen Einführung behördlicher Datenschutzbeauftragter wäre allerdings eine Verpflichtung für alle Behörden vorzuziehen, wie im BDSG-Entwurf und in den meisten Landesdatenschutzgesetzentwürfen. Verschiedene Einzelpunkte haben wir in die Behördenabstimmung eingebracht und werden darauf ggf. in den bürgerschaftlichen Ausschußberatungen zurückkommen.

2.2.2 Bereichsspezifische Datenschutzvorschriften

Die neuen Rechtsvorschriften sind mit unserer Beteiligung überwiegend datenschutzfreundlich ausgestaltet worden.

Nach langem Vorlauf wurde schließlich die Datenschutzordnung der Hamburgischen Bürgerschaft vom Parlament am 14. Oktober 1999 beschlossen. Unsere Anregungen sind dabei fast vollständig übernommen worden. Statt der unzureichenden Vorschriften im Hamburgischen Datenschutzgesetz gibt es damit eine besondere Regelung über den Umgang mit personenbezogenen Daten bei der Wahrnehmung parlamentarischer Aufgaben.

Im Hamburgischen Ausführungsgesetz zur Insolvenzordnung vom 8. Juli 1998 waren anfänglich keine ausreichenden Datenschutzregelungen vorgesehen. In Abstimmung mit uns wurde dies aber noch rechtzeitig nachgeholt.

Das Hamburgische Sicherheitsüberprüfungsgesetz (HmbSÜG) vom 25. Mai 1999 ist in enger Abstimmung mit uns beraten und verabschiedet worden (vgl. 16. TB, 13.1). Es setzt, auch im Vergleich mit den Regelungen des Bundes und anderer Länder, in zentralen Punkten deutlich datenschutzfreundliche Aspekte.

Die Dezentralisierung der Ausländerbehörde mit der Errichtung einer gemeinsamen Ausländerdatenbank für alle bezirklichen Dienststellen und für die zentrale fachbehördliche Dienststelle machten den Erlaß einer Rechtsverordnung nach §11 a HmbDSG notwendig. Hieran wirkten wir ebenso mit wie an der entsprechenden Zuständigkeitsanordnung.

Zu den weiteren bereichsspezifischen Datenschutzregelungen gehört die erneute Änderung des Rundfunkstaatsvertrages mit unserer Beteiligung (siehe 3.10). Es fehlt noch eine Datenschutzvorschrift im Gesetz zur Einführung von Bürgerbegehren und Bürgerentscheid (siehe 4.2). Für unzulänglich halten wir die Neufassung der Berufsordnung für Hamburger Ärzte hinsichtlich des Praxisverkaufs und des Auskunftsrechts (siehe 17.5).

3. Informations- und Kommunikationstechnik/Neue Medien

3.1 FHHinfoNET

Das Mailing-System der hamburgischen Verwaltung muß so gestaltet werden, daß keine unvertretbaren Sicherheitsrisiken entstehen.

Unter der Bezeichnung FHHinfoNET bietet das Landesamt für Informationstechnik (LIT) seit Oktober 1998 den Betrieb eines neuen elektronischen Mailing-Systems für die hamburgische Verwaltung als Dienstleistung an. Unter einer einheitlichen Oberfläche werden folgende Funktionalitäten rund um die Uhr zur Verfügung gestellt:

– ein gemeinsames Adressverzeichnis der öffentlichen Verwaltung auf der Basis eines mit den Behörden und Ämtern abgestimmten Namenskonzeptes,

– das Versenden und Empfangen von Nachrichten (Mailing) auf der Basis von SMTP (Simple Mail Transfer Protocol) und von Teilnehmeradressen innerhalb und außerhalb der hamburgischen Verwaltung,

– die Führung eines elektronischen Terminkalenders,

– der Zugriff auf unterschiedlichste Informationen über allen Teilnehmerinnen und Teilnehmern zugängliche „Öffentliche Ordner“,

– der Zugriff auf die eigenen Postfächer und Terminkalender über einen Intranet-Zugang auch außerhalb des eigenen LAN von jedem angeschlossenen PC in der hamburgischen Verwaltung.

Bislang sind bereits etwa 12.000 Nutzerinnen und Nutzer in das FHHinfoNET aufgenommen worden. Nach den bisherigen Planungen sollen Ende des Jahres 2000 bereits 16.000 Postfächer eingerichtet sein. Fernziel ist, alle der derzeit etwa 25.000 PC-Arbeitsplätze in der FHH an dieses gemeinsame und einheitliche Kommunikationssystem anzuschließen.

Alle Mail-Server im FHHinfoNET befinden sich in den Räumlichkeiten des LIT. Sie werden ausschließlich vom LIT betrieben. Dies erfolgt in einem eigenen IP-Adreßraum, der von allen anderen bereits vorhandenen und durch Filtereinträge in den Routern gesicherten Kommunikationsbeziehungen im FHH-Netz getrennt ist. Die Mail-Server werden in einer eigenen Windows NT-Domäne zusammengefaßt. Zu dieser Domäne bestehen von den Domänen der Behörden und Ämter nur einseitige Vertrauensverhältnisse. Die Authentifizierung der Nutzerinnen und Nutzer erfolgt über die Eingabe von Benutzerkennung und Paßwort gegenüber der Anmeldedomäne von Windows NT in den jeweiligen Installationen der Behörden und Ämter.

Auf den Servern werden nur die erforderlichen Dienste gestartet. Das LIT hat sich wegen des entstehenden Mehraufwands gegen unseren Vorschlag, eine Portfilterung auf den Kopfstellenroutern vorzunehmen, entschieden. Als Gründe wurden die zu hohe Komplexität im Bereich der Administration und die wirtschaftlich nicht vertretbare Aufrüstung der für die Masse der Filtereinträge zu geringen Speicherkapazitäten genannt.

Seit kurzem stehen innerhalb des FHHinfoNET auch eine Verschlüsselung und die digitale Signatur von Nachrichten zur Verfügung. Mit diesem Dienst kann auch aus unserer Sicht die in den Durchführungsbestimmungen zur Telekommunikations-Richtlinie der hamburgischen Verwaltung geforderte Vertraulichkeit gewährleistet werden. Sensible personenbezogene Daten können per E-Mail versandt werden, wenn sie auf diesem Wege verschlüsselt werden.

Die Möglichkeit, daß Benutzerinnen und Benutzer des FHHinfoNET ihre elektronische Post von jedem beliebigen angeschlossenen Arbeitsplatz aus einsehen können („Web Access“), ist nicht frei von Risiken. Vor allem wird die Sicherheit der lokalen Netzwerke berührt, die mit dem Intranet verbunden sind, wenn die Authentifizierung gegenüber dem elektronischen Postamt (Mail-Server) des LIT unter demselben Paßwort erfolgt wie die lokale Authentifizierung am Arbeitsplatz der Nutzerinnen und Nutzer. Die Kunden sind vom LIT über die mit Web Access verbundenen Risiken ausdrücklich zu informieren und darauf hinzuweisen, daß insbesondere der Einhaltung der verbindlichen Paßwortvorgaben erhöhte Bedeutung zukommt (Beschränkung der Anmeldefehlversuche mit Sperrung der Benutzerkennung, regelmäßige Kontrolle auf unbefugte Zugriffe). Unserem Vorschlag, den Zugang über Web Access grundsätzlich zu unterbinden und nur bei tatsächlichem Bedarf auf Antrag freizuschalten, wurde nicht gefolgt, da man den hierfür erforderlichen Aufwand als zu hoch einschätzt.

Datenschutzrechtlich bedeutsam ist ferner die Kalenderfunktion. Die Benutzer müssen selbst darüber bestimmen können, wer in welchem Umfang Einsicht in ihre Terminkalender nehmen kann. Dies betrifft nicht nur Vorgesetzte und direkte Kollegen, sondern auch Dritte in anderen Behörden und Ämtern, die über Besprechungsanfragen erkennen können, ob man zu bestimmten Zeiten für gemeinsame Termine verfügbar ist oder nicht. Bei ungeplanter Abwesenheit dürfen Vorgesetzte oder Vertreter des betroffenen Postfachbenutzers keinen direkten Zugang auf die hier eingehende Post und die Inhalte aller vorhandenen Postfachordner bekommen. Es dürfen allenfalls eingehende Nachrichten weitergeleitet werden, damit sie nicht unbearbeitet bleiben. Die lokale Systemadminstration darf jedenfalls nicht das Paßwort ändern und weitergeben. Da davon nicht nur die elektronische Post, sondern aufgrund der Konfiguration in der FHH alle über das lokale NT-Paßwort erreichbaren Anwendungen und Daten betroffen sind, wäre eine solche Lösung unvertretbar.

Unter Federführung der Finanzbehörde werden zur Zeit Regeln für die elektronische Kommunikation (Benutzerregeln) erarbeitet. Sie sollen verbindliche Vorgaben für die Nutzung der elektronischen Post und Terminkalender enthalten. Daneben sind einige Änderungen in den bereits bestehenden Telekommunikationsregeln erforderlich. In beiden Fällen sind hierbei auch datenschutzrechtlich relevante Einzelheiten betroffen, so daß wir an diesem Prozeß beteiligt sind.

Durch Zufall wurden wir darauf aufmerksam, daß der Zugriff auf Protokolle mit Verbindungsdaten, die routinemäßig im FHHinfoNet erzeugt werden, allen Teilnehmern im FHH-Netz technisch möglich war. Auf unsere Anforderung hin wurde der Zugriff auf das erforderliche Maß eingeschränkt. Das LIT protokolliert sämtliche E-Mail-Sendungen hinsichtlich Absender, Empfänger, Nachrichtenlänge, Datum und Uhrzeit, sowohl im internen Verkehr als auch bei Nachrichten aus und in externe/n Netze/n (Internet, X.400). Diese Protokolle dienen der Fehlersuche, der Virenabwehr und Abrechnungszwecken. Bis zum Zeitpunkt unserer Überprüfung waren wesentliche Teile dieser Protokolle von jedem PC der hamburgischen Verwaltung aus zugreifbar, ohne daß dies durch Maßnahmen zur Zugriffssicherung oder der nachträglichen Erkennung erschwert worden wäre. Mittlerweile ist dieser Zustand abgestellt, so daß ein Zugriff auf die Protokolle nur nach entsprechender Authentisierung möglich ist und zudem unberechtigte Zugriffsversuche erkannt werden können. Der Kreis der Berechtigten wurde auf wenige Mitarbeiter im CCF (Competence Center FHHinfoNet im LIT) begrenzt. Nach unserem Kenntnisstand ist die Protokollierung im Bereich des E-Mail-Verkehrs daher nun datenschutzrechtlich unbedenklich.

3.2 Zentrale und dezentrale Virenkontrolle in der hamburgischen Verwaltung

Die Finanzbehörde und das LIT sind bemüht, die Verbreitung von Schadenssoftware im Datennetz der FHH technisch zu unterbinden. Die datenschutzrechtlichen Aspekte wurden mit uns erörtert.

Durch die im Berichtszeitraum erfolgte Öffnung des Datennetzes der FHH für E-Mail und Internet (WWW und ftp) für eine Vielzahl von Benutzern (siehe 3.1) sind auch die Gefahren durch Viren und Trojanische Pferde stark gestiegen. Wir haben auf dieses erhöhte Risiko mit entsprechenden Konzepten für den Betrieb von Windows NT reagiert (siehe 3.3). Neben einer solchen Maßnahme, die der Vertraulichkeit der Daten dient, ist ein möglichst frühzeitiges und umfassendes Erkennen von Viren von wesentlicher Bedeutung.

Das LIT hat dieser Tatsache einerseits durch die Einrichtung eines zentralen Virenscanners Rechnung getragen, der sämtlichen E-Mail-Austausch mit externen Netzen (Internet, X.400) auf bekannte Schadenssoftware überprüft. Andererseits werden die Exchange-Postfächer aller Benutzer in regelmäßigem Abstand automatisiert auf entsprechende Inhalte durchsucht. Eine Überprüfung bereits beim Versand FHH-interner E-Mails erfolgt aus technischen Gründen bislang nicht, ist aber geplant. Ebenso wenig erfolgt zurzeit ein zentraler Virenschutz bei der Nutzung des Internet (insbes. des World Wide Web). Die zentralen Virenschutzmaßnahmen sind daher in jedem Fall, wie auch seitens der Finanzbehörde betont, durch geeignete lokale Virenscanner zu ergänzen.

Neben der Technik spielen bei der Virenkontrolle organisatorische Aspekte eine wesentliche Rolle. Der Sicherheitsgewinn durch eine zentrale Überprüfung von E-Mails darf nicht zu erheblichen Nachteilen für den Datenschutz der Betroffenen oder zu einer unzulässigen Durchbrechung des Fernmeldegeheimnisses führen.

Aus diesem Grund verfährt das LIT wie folgt: bei Empfang einer E-Mail mit einem durch Viren infizierten Anhang von außen wird diese gelöscht; die Kommunikationspartner, das Competence Center FHHinfoNet im LIT (CCF) und die für Datensicherheit zuständige Stelle in der Finanzbehörde (FB) werden darüber informiert. Bei Versand einer infizierten E-Mail aus dem FHHinfoNet heraus erfolgt ebenfalls eine Benachrichtigung an die Kommunikationspartner, CCF, FB, sowie die örtlichen IuK-Verantwortlichen. Zudem wird das interne Postfach des Absenders für den weiteren Versand von Anhängen gesperrt, bis der Virus beseitigt wurde.

Die Verbindungsdaten, die dem CCF und der FB mitgeteilt wurden, werden nach Erledigung des Vorfalls (Bereinigung des Postfachs bzw. des PC) gelöscht. Die FB speichert dauerhaft lediglich statistische Angaben über das Virenaufkommen.

Wir halten diese organisatorischen Regelungen für datenschutzrechtlich akzeptabel. Verbesserungswürdig ist jedoch der Umfang der zentralen Virenkontrolle, die zumindest den Internet-Verkehr im Rahmen der Nutzung des World Wide Web sowie den FHH-internen Versand von E-Mails einschließen sollte.

3.3 Infrastrukturansatz durch Windows NT

Die Verfügbarkeit von Internet-Diensten am Arbeitsplatz führt zu Sicherheitsrisiken, die durch Installation zweier Arbeitsumgebungen unter Windows NT reduziert werden können.

Seit Anfang des Jahres 1999 hat grundsätzlich jeder Mitarbeiter der hamburgischen Verwaltung die Möglichkeit, sowohl elektronische Post (E-Mail) als auch Internetzugang (World Wide Web) am Arbeitsplatz-PC zu erhalten, ohne daß im Einzelfall die Notwendigkeit eines derartigen Anschlusses begründet werden muß. Langfristig soll nach dem Willen des Senats an jedem der derzeit etwa 25.000 Bildschirmarbeitsplätze eine umfassende technische Infrastruktur zur Verfügung gestellt werden; dies gilt auch für sämtliche Sachbearbeiter in den Bezirksämtern – sei es in der Erziehungs- oder Sozialhilfe.

Die Umsetzung dieses Infrastrukturansatzes wird seit einiger Zeit von zahlreichen Behörden in Hamburg mit großem Aufwand vorangetrieben. Beispielsweise können Mitarbeiter der Schuldnerberatung seit Ende des Jahres elektronische Post auch im Internet verschicken, Mitarbeiter der Fachlichen Leitstelle Erziehungsgeld können das World Wide Web (www) nutzen. Mittlerweile haben nach Einschätzung des LIT bislang ca. 12 000 Mitarbeiter in den verschiedensten Dienststellen ein eigenes elektronisches Postfach und davon fast 3.000 auf das www Zugriff.

Die Anbindung von Büroarbeitsplätzen an das Internet bringt gravierende Sicherheitsrisiken mit sich: Sogenannte Trojanische Pferde können als Bestandteil von ausführbaren Programmen (beispielsweise Bildschirmschoner, die vom Benutzer zusätzlich auf das System geladen werden), als Anhängsel von selbstextrahierenden Dateien, als Anlage von Elektronischer Post oder in Form von Java-Applets, Javascript-Code oder ActiveX-Controls auf den PC geladen werden, ohne daß deren Qualität und Herkunft kontrolliert werden kann. Werden solche Trojanischen Pferde von den eingesetzten Virenscannern nicht erkannt, besteht die Gefahr, daß beispielsweise Arbeitsplatz-PC aus dem Internet ferngesteuert und Dateien mit sensiblem Inhalt unbemerkt als Anhang von elektronischer Post an beliebige Internetadressen versendet werden. Beispielsweise steht mit der neueren Version des Hacker-Programms „Back Orifice“ mittlerweile ein sehr funktionales Werkzeug zur Fernsteuerung von Windows NT zur Verfügung, dessen Quellcode kostenlos aus dem Internet geladen werden kann. Es ist daher zu erwarten, daß in nächster Zeit verschiedenste Varianten von Back Orifice auftreten werden, die nicht mehr in ihrer Gesamtheit von den eingesetzten Virenscannern erkannt werden.

Die zunehmende Verbreitung von Windows NT hat der Hamburgische Datenschutzbeauftragte zum Anlaß genommen, Sicherheitsmaßnahmen für den Einsatz von Windows NT zu formulieren, die auch den genannten Risiken Rechnung tragen. Dieses Sicherheitskonzept findet sich auch in einer Broschüre wieder, die der Hamburgische Datenschutzbeauftragte zusammen mit dem Landesbeauftragten für den Datenschutz in Bremen herausgegeben hat.

Ein wesentlicher Bestandteil des NT-Sicherheitskonzepts ist ein Vorschlag zur Einrichtung von zwei getrennten Arbeitsumgebungen auf einem NT-Client. In der sogenannten Produktionsumgebung soll ausschließlich auf Client-Server-Anwendungen einschließlich Textverarbeitung zugegriffen werden, während die sogenannte Transportumgebung für die Internet-Dienste E-Mail und www zur Verfügung steht. Durch diese Trennung wird verhindert, daß zeitgleich auf sensible Serverdaten und auf beliebige Internetadressen zugegriffen werden kann. Das Konzept sieht weiterhin vor, daß Programme in der Transportumgebung ausführlich getestet werden, ohne hierdurch die Sicherheit der Produktionsumgebung zu beeinträchtigen. Ausführbare Programme – entweder als exe-Datei, als Anlage von E-Mail, als Java-Code oder als ActiveX-Control – sollen nur in Ausnahmefällen nach ausgiebigem Test der Programme oder bei vertrauenswürdigem Urheber von der Transport- in die Produktionsumgebung übertragen werden. Damit aus der Transportumgebung nicht direkt auf die Daten der Produktionsumgebung zugegriffen werden kann, sind jedoch zwei unterschiedliche NT-Benutzerkennungen erforderlich. Der Benutzer muß zwischen den jeweiligen Arbeitsumgebungen bzw. NT-Kennungen wechseln. Unser Vorschlag der zwei Arbeitsumgebungen wurde bislang von der Finanzbehörde nicht aufgegriffen. Die Finanzbehörde hat ausgeführt, daß gegenwärtig in der Verwaltung kein Verfahren bekannt sei, das mit Daten arbeitet, deren Sicherheit eine Trennung von Arbeitsumgebungen mit den damit zusammenhängenden Einschränkungen verlangen würde. Es wurde lediglich auf eine umfangreiche Virenkontrolle verwiesen, die sicherstellen soll, daß keine bösartigen Programme installiert und ausgeführt werden.

Eine Virenkontrolle stößt jedoch an ihre Grenzen. Zum einen können nur solche Trojanischen Pferde gefiltert werden, die den Herstellern von Virenscannern bekannt sind. Trojanische Pferde, die individuell entwickelt werden, um Behörden der FHH zu attackieren, bleiben unentdeckt. Zum anderen kann die Zeitspanne von der Entdeckung eines Standard-Trojaners bis hin zur flächendeckenden Installation des aktualisierten Virenscanners in der hamburgischen Verwaltung durchaus beträchtlich sein.

Angesichts der Sicherheitsrisiken, die trotz Virenkontrolle mit der Verfügbarkeit von Internet-Diensten an jedem Arbeitsplatz verbunden sind, halten wir es für erforderlich, den Zugriff auf lokal verfügbare personenbezogene Daten aus dem Internet heraus zu unterbinden. Die vorgeschlagene Trennung der Arbeitsumgebungen ist eine geeignete Maßnahme zur Reduzierung dieser Risiken. Der Hamburgischen Datenschutzbeauftragte begrüßt es, daß die Diskussion in der hamburgischen Verwaltung intensiver geführt werden soll – wie von der Finanzbehörde angekündigt. Sofern bei Anwendungen mit hohem Schutzbedarf keine Maßnahmen über die bisherigen Grundschutzmaßnahmen hinaus getroffen werden, sollte an solchen Bildschirmarbeitsplätzen lieber vollständig auf Internet-Dienste einschließlich elektronischer Post verzichtet werden.

3.4 Prüfung des UNIX-Rechenzentrums des LIT

Bei der Prüfung des UNIX-Rechenzentrums im Landesamt für Informationstechnik (LIT) wurden Mängel beim administrativen Zugriff festgestellt und inzwischen behoben.

Das LIT betreibt mehrere UNIX-Server und stellt diese anderen Behörden für zentrale Anwendungen zur Verfügung. Verschiedene Verfahren mit teilweise sensiblen personenbezogenen Daten sind dort im Einsatz, z.B. PROJUGA (Projekt Jugendamtsautomation) und MESTA (Mehrländer-Staatsanwaltschafts-Automation, siehe 14.1). Wir haben dieses Rechenzentrum geprüft und dabei neben einigen Mängeln ein im Wesentlichen zufriedenstellendes Datensicherheitsniveau angetroffen.

Zum Prüfzeitpunkt erfolgte die Administration der UNIX-Maschinen durch verschiedene Benutzer der entsprechenden Abteilung und des Leitstandes unter einer einzigen Kennung für den Super-User „root“. Da sich dies auf insgesamt acht Personen erstreckte, haben wir vorgeschlagen, individuelle Kennungen für den administrativen Zugang einzurichten. Dieser Anregung wurde gefolgt. Zudem wurden die im Rahmen der Systemverwaltertätigkeit übertragenen Daten durch den Einsatz des Produkts SSH (Secure Shell) gegen unberechtigte Zugriffe im Inhouse-Netz des LIT geschützt. Die Kenntnisnahme von Passwörtern durch Unberechtigte wurde dadurch wesentlich erschwert.

Weitere Verbesserungen betrafen die zur Verfügung gestellten Netzwerkdienste, die auf das erforderliche Maß reduziert wurden, und die Löschung nicht benötigter Benutzerkonten, die in Absprache mit den Kunden des UNIX-RZ durchgeführt wurde.

3.5 Kooperation bei der Datenschutzkontrolle

Die Datenschutzbeauftragten von Hamburg und Schleswig-Holstein haben eine Vereinbarung über die Zusammenarbeit bei der datenschutzrechtlichen Kontrolle der Landesrechenzentren getroffen.

Im Juli 1999 haben Hamburg und Schleswig-Holstein ein Verwaltungsabkommen unterzeichnet, das eine länderübergreifende Kooperation auf dem Gebiet der Informations- und Kommunikationstechnik (IuK) beinhaltet. Die Vereinbarung sieht eine enge Zusammenarbeit der jeweiligen IuK-Dienstleister, dem Landesamt für Informationstechnik (LIT) in Hamburg und der Datenzentrale des Landes Schleswig-Holstein (DZSH) in Kiel-Altenholz, vor. Die Großrechneranwendungen beider Länder werden zukünftig nur noch in Hamburg betrieben, Druckausgaben einschließlich Papiernachbearbeitung und Versand werden nur noch in der DZSH erfolgen. Durch diese Konzentration von Kernfunktionen der beiden Rechenzentren sollen in den kommenden Jahren Einsparungen in Millionenhöhe erzielt werden.

Diese Kooperation darf nicht zu einer Absenkung von Datenschutzstandards führen. Die Bürgerinnen und Bürger von Hamburg und Schleswig-Holstein sollen sich auch in Zukunft darauf verlassen können, daß ihre personenbezogenen Daten gesetzeskonform und nachprüfbar sicher verarbeitet werden. Die Datenschutzbeauftragten von Hamburg und Schleswig-Holstein haben deshalb im Oktober 1999 selbst eine Vereinbarung getroffen, durch die gewährleistet wird, daß die Datenschutzkontrolle auch im Rahmen der länderübergreifenden Zusammenarbeit des LIT und der DZSH weiterhin effektiv ausgeübt wird. Sie beabsichtigen, bei der Bearbeitung von Eingaben und bei der Durchführung von Prüfungen eng und arbeitsteilig zusammenzuarbeiten. Anforderungen an die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung in den betroffenen Bereichen werden sie gemeinsam formulieren und ihrer Kontrolltätigkeit zugrunde legen.

3.6 Evaluation des Informations- und Kommunikationsdienste-Gesetzes (IuKDG)

Das Evaluationsverfahren hat die Datenschutzbestimmungen im Multimediarecht weitgehend bestätigt.

Am 1. August 1997 ist das Informations- und Kommunikationsdienste-Gesetz (IuKDG) zeitgleich mit dem Mediendienste-Staatsvertrag (MDStV) in Kraft getreten. Beide Gesetze enthalten – weitgehend übereinstimmende – Regelungen über den Datenschutz bei interaktiven Diensten (vgl. 16.TB, 3.5 und unsere Broschüre „Datenschutz bei Multimedia und Telekommunikation“).

Der Deutsche Bundestag hatte bei der Verabschiedung des IuKDG die Bundesregierung aufgefordert, die Entwicklung bei den neuen Informations- und Kommunikationsdiensten zu beobachten und darzulegen, ob und gegebenenfalls in welchen Bereichen Anpassungs- bzw. Ergänzungsbedarf bestehe, und hierüber spätestens zwei Jahre nach Inkrafttreten des Gesetzes zu berichten. Dabei sollten auch die Erfahrungen der Länder mit der Umsetzung des Mediendienste-Staatsvertrages Berücksichtigung finden. Im einzelnen sollte auch darauf eingegangen werden, welche Auswirkungen der Teledienstedatenschutz auf das Nutzerverhalten und die wirtschaftliche Entwicklung bei den neuen Diensten hat.

Im Rahmen des Evaluationsprozesses, der unter Federführung des Bundesministeriums für Wissenschaft und Forschung (BMWF) stattfand, wurden auch die Fragen des Datenschutzes bearbeitet. Im Arbeitskreis „Datenschutz“, an dem der Hamburgische Datenschutzbeauftragte beteiligt war, standen die Erfahrungen mit der Umsetzung des neuen Datenschutzkonzeptes im Mittelpunkt, vor allem

• der Systemdatenschutz (Datenvermeidung, anonyme und pseudonyme Nutzungsmöglichkeiten),

• das Datenschutzaudit und

• die Datenschutzaufsicht.

Aus Sicht der Datenschutzbeauftragten und der Datenschutzaufsichtsbehörden haben sich die Datenschutzbestimmungen für Tele- und Mediendienste im wesentlichen bewährt. Allerdings bestehen nach wie vor Umsetzungsdefizite, denen sich die Datenschutzaufsichtsbehörden durch eine koordinierte und intensivierte Prüf- und Beratungstätigkeit angenommen haben.

Inzwischen hat die Bundesregierung ihren Bericht vorgelegt (Bundestags-Drs. 14/1191 vom 18. Juni 1999). Darin wird festgestellt, daß angesichts der kurzen Zeitperiode, die seit Inkrafttreten der Rechtsvorschriften vergangen ist, zwar eine abschließende Beurteilung der Datenschutzbestimmungen noch nicht möglich sei; gleichwohl könne jedoch festgestellt werden, daß die Wirtschaft Ansätze und Initiativen entwickelt habe, die den Vorgaben des Gesetzes Rechnung trügen. Wesentliche Bestimmungen aus dem Tele- und Mediendienstерecht (insb. zum Systemdatenschutz und zum Datenschutzaudit) sollen bei der Novellierung des Bundesdatenschutzgesetzes berücksichtigt werden (vgl. 2.1).

3.6.1 Systemdatenschutz

§3 Abs. 4 TDDSG:

„Die Gestaltung und Auswahl technischer Einrichtungen für Teledienste hat sich an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen."

§4 Abs. 1 TDDSG:

„Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren."

Der „Systemdatenschutz" ist eine der wesentlichen Datenschutzinnovationen, die sowohl in das Teledienstedatenschutzgesetz (TDDSG – Art. 2 IuKDG) als auch in den MDStV Eingang gefunden haben: Bereits bei der Gestaltung der technischen Systeme (und nicht erst bei ihrer Anwendung) soll die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach Möglichkeit vermieden bzw. auf ein Mindestmaß begrenzt werden. Konkret sollen Dienste so gestaltet werden, daß sie auch anonym oder unter Pseudonym genutzt werden können.

Die Prüf- und Beratungspraxis der Datenschutzaufsichtsbehörden hat allerdings gezeigt, daß insbesondere hinsichtlich der Erhebung und Speicherung von Nutzungsdaten, aber auch bezüglich der Informationen der Nutzer noch erhebliche Defizite bestehen. So werden bei vielen Angeboten – entgegen den Bestimmungen aus §6 TDDSG bzw. §15 MDStV – Nutzungsdaten detailliert gespeichert (vgl. 16.TB, 3.6.1).

Wir haben ferner auf das Problem hingewiesen, daß im Internet eine sichere Authentifizierung der Nutzer – aber auch der Anbieter – von Telediensten nicht in ausreichendem Maße gewährleistet ist. Dieses Defizit kann dazu führen, daß Unberechtigte Kenntnis von personenbezogenen Daten erhalten (etwa Kreditkartennummern im Rahmen von Zahlungsvorgängen).

Zudem erweist es sich zunehmend als ein Hindernis sowohl für den Datenschutz als auch für die geschäftliche Nutzung des Internet, daß ohne zusätzliche Schutzmaßnahmen die Vertraulichkeit der Datenübertragung nicht sichergestellt ist. Aus diesem Grunde haben wir angeregt, Projekte zur Entwicklung von Sicherheitsinfrastrukturen (insb. anonyme/pseudonyme Nutzung; Verschlüsselungsverfahren) verstärkt zu fördern und die bereits verfügbaren Mittel zur Verbesserung der Sicherheit der Datenübertragung auch zu nutzen.

Die Bundesregierung hat dazu ausgeführt, daß sich die entsprechenden Verfahren weitgehend noch in der Entwicklungs- und Erprobungsphase befänden. Im übrigen hat die Bundesregierung angekündigt, daß die Novelle zum Bundesdatenschutzgesetz auch Bestimmungen zum Systemdatenschutz, insb. zur Datenvermeidung, enthalten soll. Im HmbDSG gibt es eine entsprechende Regelung (§5 Abs.4) bereits seit 1997.

3.6.2 Datenschutzaudit

§17 MDStV

„Zur Verbesserung von Datenschutz und Datensicherheit können Anbieter von Mediendiensten ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen lassen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt."

Datenschutzaudit ist ein Verfahren, in dem überprüft und bescheinigt wird, inwieweit Unternehmen datenschutzkonform handeln. Dazu sollen Maßstäbe etabliert werden, die es dem Verbraucher ermöglichen, Angebote und Unternehmen hinsichtlich ihrer Datenschutzvorkehrungen zu bewerten und die datenschutzfreundlichsten Angebote auszuwählen. Es wird also angestrebt, die unternehmerische Selbstverantwortung der datenverarbeitenden Stellen für den Datenschutz zu stärken. Das Datenschutzaudit trägt auch der Tatsache Rechnung, daß die Datenschutzaufsichtsbehörden kaum in der Lage sind, über alle datenverarbeitenden Stellen eine ständige gründliche Kontrolle auszuüben.

Ferner wird berücksichtigt, daß die Globalisierung der Informations- und Kommunikationstechnik der Reichweite nationaler Datenschutzregelungen enge Grenzen setzt. Vor allem im Hinblick auf diese zunehmende Internationalisierung der Teledienste haben wir uns dafür ausgesprochen, das bereits im MDStV vorgesehene Datenschutzaudit auch in das TDDSG aufzunehmen. Damit würden die Bemühungen verschiedener Anbieter zur Datenschutz-Zertifizierung (d.h. zu einer nachprüfbaren Bescheinigung über die Gewährleistung des Datenschutzes – vgl. 16. TB 3.7) unterstützt. Im Rahmen des Datenschutzaudit könnten Qualitätsnormen definiert und umgesetzt werden, die auf internationaler Ebene datenschutzkonformen Angeboten und Anbietern einen Wettbewerbsvorteil verschaffen.

Während der Evaluation des IuKDG haben sich nahezu alle Beteiligten – auch die Wirtschaftsverbände und Unternehmen – positiv zur Einführung des Datenschutzaudit geäußert. Entsprechende Regelungen sind bereits im Brandenburgischen Datenschutzgesetz enthalten. Die Bundesregierung hat zudem angekündigt, daß bei der BDSG-Novelle eine Vorschrift zum Datenschutzaudit aufgenommen werden soll.

3.6.3 Datenschutzaufsicht

§8 TDDSG

„(1) §38 des Bundesdatenschutzgesetzes findet mit der Maßgabe Anwendung, daß die Überprüfung auch vorgenommen werden darf, wenn Anhaltspunkte für eine Verletzung von Datenschutzvorschriften nicht vorliegen.

(2) Der Bundesbeauftragte für den Datenschutz beobachtet die Entwicklung des Datenschutzes bei Telediensten und nimmt dazu im Rahmen seines Tätigkeitsberichtes nach §26 Abs. 1 BDSG Stellung."

§18 Abs. 1 Satz 2 MDStV

„Die nach den allgemeinen Datenschutzgesetzen des Bundes und der Länder zuständigen Kontrollbehörden überwachen für ihren Bereich die Einhaltung der Bestimmungen nach §§12 bis 16."

§91 Abs. 4 TKG

„Soweit für die geschäftsmäßige Erbringung von Telekommunikationsdiensten Daten von natürlichen oder juristischen Personen erhoben, verarbeitet oder genutzt werden, tritt bei den Unternehmen an die Stelle der Kontrolle nach §38 des Bundesdatenschutzgesetzes eine Kontrolle durch den Bundesbeauftragten für den Datenschutz entsprechend den §§21 und 24 bis 26 Abs. 1 bis 4 des Bundesdatenschutzgesetzes."

Für Multimediadienste, sowohl bei Tele- als auch bei Mediendiensten, sind übereinstimmend die Aufsichtsbehörden nach den allgemeinen Datenschutzgesetzen (für den privaten Bereich: die Länderaufsichtsbehörden nach §38 BDSG) zuständig. In Hamburg wird die Datenschutzaufsicht sowohl für den privaten als auch für den öffentlichen Bereich durch den Hamburgischen Datenschutzbeauftragten wahrgenommen.

Allerdings liegt die Aufsicht hinsichtlich der technischen Telekommunikationsverbindungen, die den Multimediadiensten zugrunde liegen, nach §91 Abs. 4 Telekommunikationsgesetz (TKG) beim Bundesbeauftragten für den Datenschutz (BfD).

Diese unterschiedlichen Aufsichtsmodelle für Multimediadienste und für Telekommunikationsdienste sind während des Gesetzgebungsverfahrens zum IuKDG zum Teil auf Skepsis gestoßen.

Wir haben das BMWF während des Evaluationsverfahrens darauf hingewiesen, daß sich die Zuordnung der Datenschutzaufsicht für Medien- und Teledienste zu den nach allgemeinem Datenschutzrecht zuständigen Aufsichtsbehörden bewährt hat. Diese Aufsichtsregelung hat für die meisten Anbieter zur Konsequenz, daß für sie insoweit nur eine Aufsichtsbehörde zuständig ist. Daneben besteht für die zugrundeliegenden technischen Telekommunikationsverbindungen die Aufsicht durch den BfD.

Die Anwendungsprobleme des Telekommunikations-, Mediendienste- und Teledienstesrechtes konnten in enger Kooperation der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzaufsichtsbehörden für den nichtöffentlichen Bereich befriedigend geklärt werden. Zu diesem Zweck sind ein IuK-Kooperationskreis der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzaufsichtsbehörden und eine Arbeitsgruppe Telekommunikation, Tele- und Mediendienste des Düsseldorfer Kreises eingerichtet worden. Beide Arbeitskreise werden vom Berliner Datenschutzbeauftragten geleitet. Damit ist eine länderübergreifend einheitliche Aufsichtspraxis sichergestellt.

3.6.4 Anwendbarkeit des deutschen Datenschutzrechts

Sowohl über das Internet als auch auf anderer technischer Basis angebotene Tele- und Mediendienste wenden sich an einen globalen Nutzerkreis. Dabei kann der Betrieb der technischen Infrastruktur, die Bereitstellung der Inhalte und die Kundenbetreuung in verschiedenen Staaten stattfinden.

Entscheidend für die Anwendbarkeit deutschen Datenschutzrechts sind die tatsächlichen Umstände der Datenverarbeitung. Gleichwohl ist es datenschutzrechtlich zu begrüßen, wenn international tätige Unternehmen hinsichtlich des Angebots, das sich an deutsche Nutzer wendet, von sich aus das deutsche Datenschutzrecht anwenden.

§2 TDDSG

„Im Sinne dieses Gesetzes sind ... „Diensteanbieter“ natürliche oder juristische Personen oder Personenvereinigungen, die Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln...“

Selbst wenn der deutsche Nutzer den Vertrag über die Inanspruchnahme eines Tele- oder Mediendienstes mit einem ausländischen Unternehmen schließt und das deutsche Unternehmen in rein technischem Sinne einen Zugang zur Nutzung des Dienstes nicht vermittelt, ist im Sinne eines möglichst effektiven Grundrechtsschutzes der Nutzer das „Bereithalten eines Dienstes zur Nutzung“ (§2 TDDSG, §3 MDStV) weit auszulegen. Aus Sicht des Nutzers ist also das deutsche Unternehmen als Anbieter des Medien- bzw. Teledienstes anzusehen, wenn es die Akquisition neuer deutscher Kunden betreibt, an der Verwaltung der Nutzerdaten mitwirkt und die deutschsprachigen Inhalte des Dienstes redaktionell zu verantworten hat.

3.7 Orientierungshilfe für Tele- und Mediendienstanbieter

Die Orientierungshilfe für Anbieter von Tele- und Mediendiensten soll die Umsetzung der Datenschutzvorschriften des Multimediarechts erleichtern.

Bei der Beratung von Firmen, die Tele- und Mediendienste anbieten, und durch Eingaben von Nutzern solcher Angebote ist uns deutlich geworden, daß hinsichtlich der Interpretation der gesetzlichen Vorgaben des Teledienstedatenschutzgesetzes und des Mediendienste-Staatsvertrags (vgl. 3.6) und ihrer technischen Umsetzung erhebliche Unsicherheiten bestehen. Wir haben deshalb eine Orientierungshilfe erarbeitet, die anhand von praktischen Beispielen die Rechtslage erläutert und Tips zur Umsetzung der datenschutzrechtlichen Vorgaben gibt.

Die Orientierungshilfe hat nicht den Anspruch, alle Rechtsfragen zu beantworten, die im Zusammenhang mit interaktiven Diensten stehen. Nicht betrachtet werden

• die reine Transportebene, auf der die jeweiligen Dienste aufsetzen. Hierfür sind die Bestimmungen des Telekommunikationsrechts, insb. das Telekommunikationsgesetz (TKG) einschlägig;

• die Datenverarbeitung auf der Inhalts- bzw. Anwendungsebene, soweit Tele- bzw. Mediendienste lediglich zur Verbindungssteuerung eingesetzt werden (z.B. zur Abwicklung von Vertragsverhältnissen, etwa bei Bank- und Versicherungsgeschäften; hier ist bezüglich der Zulässigkeit der Verarbeitung personenbezogener Daten §28 BDSG anzuwenden).

Die Orientierungshilfe beschränkt sich also auf die mittlere Ebene, d.h. auf die für Online-Dienste und das Internet typische logische Interaktion zwischen Nutzer und Anbieter.

Behandelt werden unter anderem folgende Fragen:

• Wie kann sichergestellt werden, daß der Nutzer den Verantwortlichen für ein Angebot kennt?

• Auf welche Weise und zu welchem Zeitpunkt muß der Anbieter über die Verarbeitung von Bestands- und Nutzungsdaten unterrichten und wie umfassend muß die Unterrichtung sein?

• Unter welchen Umständen dürfen Cookies verwendet werden und wie ist der Nutzer darüber zu informieren?

• Wie kann der Anbieter die Unterrichtung des Nutzers nachweisen?

• Wann muß der Anbieter eine Einwilligung des Nutzers einholen und wie ist die Einwilligungserklärung zu gestalten?

• Welche Grenzen hat die Einwilligung?

• Wann müssen anonyme und pseudonyme Nutzungsmöglichkeiten vorgesehen werden und welche Anforderungen sind an derartige Angebote zu stellen?

• Über welche Daten kann der Nutzer beim Anbieter Auskunft verlangen und wie sind die Auskunftsrechte technisch zu realisieren?

Die Orientierungshilfe wird im Jahr 2000 im Rahmen der Neuauflage unserer Broschüre zum Multimediarecht veröffentlicht und ist darin im Internet unter <www.hamburg.datenschutz.de> abrufbar.

3.8 Prüfung eines Online-Dienstes

Der Hamburgische Datenschutzbeauftragte hat einen ausländischen Online-Dienst mit einem deutschen Tochterunternehmen geprüft. Werden Abrechnungsdaten von der deutschen Unternehmenstochter an die ausländische Obergesellschaft übermittelt, müssen die Unternehmen eine verbindliche vertragliche Vereinbarung treffen, um die Wahrung des Fernmeldegeheimnisses sicherzustellen.

Der geprüfte Online-Dienst bietet Angebote in verschiedenen Sprachen an. Das umfangreiche deutschsprachige Angebot richtet sich vor allem an deutsche Nutzer. Zudem wird der Zugang zum Internet vermittelt. Die Rechner, auf denen die Benutzerverwaltung abgewickelt wird, und auch die Server, auf denen die Inhalte verwaltet werden, befinden sich in den USA. Die deutsche Tochtergesellschaft hat die redaktionelle Verantwortung für die deutschsprachigen Inhalte des Dienstes, beteiligt sich an der Verwaltung der Mitgliederdaten der deutschen Kunden und wirkt an der Abrechnung ihrer Nutzungsentgelte mit.

3.8.1 Registrierung neuer Kunden

Der Online-Dienst wirbt mit der Möglichkeit, daß sich neue Kunden online registrieren lassen. Dabei nutzt der Kunde eine Zugangssoftware, die (zumeist auf CD-ROM) in großer Auflage öffentlich verbreitet wird. Im Rahmen des Registrierungsprozesses hatte der neue Kunde verschiedene Angaben zu seiner Identität und zum gewünschten Abrechnungsverfahren zu machen. Die Eingabe der Daten erfolgte nach Installation der Zugangssoftware zunächst offline, d.h. ohne Telekommunikationsverbindung zu dem Diensteanbieter. Während der Prozedur wurde jedoch eine Online-Verbindung aufgebaut, und die Angaben wurden einer Plausibilitätsprüfung unterzogen.

Zudem wurden die Nutzerangaben mit einer Datenbank des Anbieters abgeglichen, in der die Namen und Kontonummern der derzeitigen und früherer Kunden gespeichert sind. Sofern eine Kontonummer bereits verwendet wurde, wurde der Registrierungsprozeß abgebrochen. Damit wurden bereits vor Abschluß der Registrierung personenbezogene Daten erhoben.

Das Verfahren war im Prüfungszeitraum so gestaltet, daß die Kunden erst zum Ende der Registrierungsprozedur – also nach Beendigung der Plausibilitätsüberprüfungen und nach dem Online-Abgleich der Kontodaten – über das Verfahren der Datenverarbeitung und die Datenschutzregelungen informiert und zur Zustimmung aufgefordert wurden. Dies widersprach der Vorgabe aus §3 Abs. 5 TDDSG, wonach der Nutzer vor der Erhebung seiner personenbezogenen Daten zu informieren ist.

§3 Abs. 5 TDDSG

„Der Nutzer ist vor der Erhebung über Art, Umfang, Ort und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten. Bei automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, ist der Nutzer vor Beginn dieses Verfahrens zu unterrichten..."

Mit der inzwischen zugesagten Änderung des Verfahrens wird das Registrierungsverfahren zukünftig den datenschutzrechtlichen Vorschriften entsprechen.

Im Hinblick auf die bei der Online-Registrierung erhobenen Daten bestanden zunächst Zweifel hinsichtlich ihrer Erforderlichkeit und damit an der Zulässigkeit der Erhebung und an der anschließenden Verarbeitung und Nutzung.

§5 Abs. 1 TDDSG

„Der Diensteanbieter darf personenbezogene Daten eines Nutzers erheben, verarbeiten und nutzen, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses mit ihm über die Nutzung von Telediensten erforderlich sind (Bestandsdaten)."

Wir hatten die Erforderlichkeit der Datemverarbeotimg für die Probemitgliedschaft und für die reguläre Mitgliedschaft zunächst gesondert beurteilt. Nach den Aussagen in der damaligen Kundenwerbung sollte die Probemitgliedschaft es den Nutzern ermöglichen, den Dienst gratis und frei von Verpflichtungen (insb. ohne Kaufzwang) zu testen. Für diesen Zweck waren Angaben zur Zahlungsweise und zur Kontoverbindung nicht erforderlich. Zudem hatte der Dienst die Möglichkeit, die Daten zur Zahlungsweise im Rahmen des ohnehin stattfindenden schriftlichen Bestätigungsverfahrens nach Abschluß der Online-Registrierung nachzuerheben. Die Erhebung dieser Daten bereits bei der Online-Registrierung für die Probemitgliedschaft erschien somit datenschutzrechtlich zweifelhaft.

Der Dienst hat jedoch inzwischen erklärt, daß ein Vertrag zustande komme, sobald der Kunde die Nutzungsbedingungen elektronisch akzeptiert habe. Eine bestimmte Zeit könne der Kunde den Dienst umsonst nutzen, danach muß er bezahlen. Es liege jedoch ein einheitliches Vertragsverhältnis vor. Wenn der Kunde innerhalb der Freistunden den Vertrag nicht kündige, werde der Vertrag automatisch kostenpflichtig. Dementsprechend sei eine rechtliche Unterscheidung in ein Probevertragsverhältnis und ein „richtiges“ Vertragsverhältnis nicht möglich.

Diese Argumentation ist vertretbar. Dementsprechend haben wir die Datenerhebung und -speicherung ganzheitlich betrachtet. Für die rechtliche Beurteilung ist insofern auch die Notwendigkeit der Datenspeicherung zur Abrechnung der entgeltpflichtigen Nutzung des Dienstes einzubeziehen. Hierfür ist es erforderlich, daß der Dienst auch die Angaben über die Bankverbindung bzw. die Kreditkartennummern seiner Kunden erhebt und speichert. Die Erhebung und Speicherung der Daten zur Kontoverbindung bereits zu Beginn der kostenfreien Probephase war dementsprechend datenschutzrechtlich zulässig.

3.8.2 Übermittlung von Kundendaten

Auch wenn das amerikanische und das deutsche Unternehmen demselben Konzern zugehören, handelt es sich datenschutzrechtlich um zwei speichernde Stellen. Eine Datenverarbeitung im Auftrag (§11 BDSG) scheidet im vorliegenden Fall aus, weil das US-Unternehmen seinen Sitz nicht im Geltungsbereich des BDSG hat und somit Dritter im Sinne von §3 Abs. 9 BDSG ist. Jede Weitergabe personenbezogener Daten zwischen den Unternehmen ist dementsprechend als Übermittlung anzusehen.

Soweit im Rahmen des Dienstes Nutzungsdaten erhoben und gespeichert werden, erfolgt dies allein durch das amerikanische Unternehmen. Diese Daten werden also nicht von dem deutschen Unternehmen an das amerikanische Unternehmen übermittelt.

§3 Abs. 5 BDSG

„Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten (Empfänger) in der Weise, daß

a) die Daten durch die speichernde Stelle an den Empfänger weitergegeben werden oder

b) der Empfänger von der speichernden Stelle zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft“

Soweit allerdings im Rahmen des Inkassoverfahrens und für die Mitgliederbetreuung Daten über Zahlungsvorgänge deutscher Kunden von dem deutschen Unternehmen an das amerikanische Unternehmen übertragen werden (z.B. indem diese Daten online in der Mitgliederdatenbank gespeichert werden), handelt es sich um eine Datenübermittlung des deutschen an das US-Unternehmen im Sinne von §3 Abs. 5 Nr. 3 BDSG. Umgekehrt werden von dem amerikanischen Unternehmen Daten an das deutsche Unternehmen übermittelt, wenn das deutsche Unternehmen auf die in der Mitgliederdatenbank gespeicherten Daten lesend zugreift. Gegenstand der Übermittlung sind jedoch in beiden Fällen Bestands- und Abrechnungsdaten, nicht jedoch Nutzungsdaten.

Vor dem Hintergrund des Art. 25 der EG-Datenschutzrichtlinie bestehen zwar Zweifel, inwieweit in den USA als Bestimmungsland der Datenübermittlung des deutschen Unternehmens ein angemessenes Schutzniveau gegeben ist. Allerdings ist der Datenempfänger zugleich Vertragspartner der Betroffenen, die mit ihrer Zustimmung zu den Nutzungsbestimmungen auch ihre Einwilligung in die Datenverarbeitung durch das amerikanische Unternehmen gegeben haben. Die Übermittlung begegnet von daher keinen datenschutzrechtlichen Bedenken.

Art. 25 EG-Datenschutzrichtlinie

„(1) Die Mitgliedstaaten sehen vor, daß die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

(2) Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen berücksichtigt. ...“

Hinsichtlich der Abrechnungsdaten, die an das amerikanische Unternehmen übermittelt werden, fehlt allerdings noch die in §6 Abs. 4 TDDSG und §15 Abs. 4 MDStV geforderte vertragliche Regelung zwischen dem deutschen und dem amerikanischen Unternehmen.

§6 Abs. 4 TDDSG

„Hat der Diensteanbieter mit einem Dritten einen Vertrag über die Abrechnung des Entgelts geschlossen, so darf er diesem Dritten Abrechnungsdaten übermitteln, soweit es für diesen Zweck erforderlich ist. Der Dritte ist zur Wahrung des Fernmeldegeheimnisses zu verpflichten.“

Wir haben deshalb vorgeschlagen, daß beide Unternehmen eine verbindliche vertragliche Vereinbarung treffen, die die Wahrung des Fernmeldegeheimnisses absichert. Wir haben ferner angeregt, auch die Verantwortlichkeit für die Daten und die Sicherstellung eines angemessenen Datenschutzniveaus vertraglich zu regeln.

3.9 ePost

Die Versendung von Daten, die der ärztlichen Schweigepflicht unterliegen, mit dem elektronischen Service ePost bedarf der Einwilligung der Betroffenen. Die elektronische Übertragung personenbezogener Daten in öffentlichen Netzen muß verschlüsselt erfolgen.

Die Deutsche Post AG bietet vor allem Geschäftskunden den elektronischen Service ePost an. Dabei handelt es sich um die Kombination verschiedener Dienste:

• Der Kunde liefert die Daten auf Datenträger oder online bei der Deutschen Post AG bzw. bei einem ihrer „Vertriebspartner“ für den ePost-Dienst an. Bei der online-Anlieferung handelt es sich um einen Teledienst. Da es sich bei den Nutzern des Dienstes üblicherweise nicht um natürliche Personen, sondern um Unternehmen handelt, fallen auf dieser Ebene im Regelfall keine personenbezogenen Nutzerdaten an.

• Die Daten werden durch die Post bzw. ihre Vertriebspartner entsprechend den Vorgaben des Kunden formatiert und zur ePost-Station übertragen, bei der sie ausgedruckt und kuvertiert werden sollen. Diese Tätigkeiten entsprechen der Funktion von Letter-Shops und sind – soweit dabei personenbezogene Daten verarbeitet werden – als Auftragsdatenverarbeitung zu qualifizieren. Dies gilt auch für die Archivierung der Versanddaten auf CD-ROM, die zusätzlich angeboten wird.

• Die fertigen Briefsendungen werden im üblichen Briefverteilverfahren den Adressaten zugestellt; dabei handelt es sich um einen Postdienst.

3.9.1 Erforderlichkeit der Einwilligung

Der Düsseldorfer Kreis der Obersten Aufsichtsbehörden für den Datenschutz beschäftigte sich mit den Voraussetzungen für die Nutzung von ePost für den Versand von Arztrechnungen durch privatärztliche Verrechnungsstellen (PV). Zu klären war, ob der Versand von Arztrechnungen mittels ePost eine unbefugte Offenbarung besonders geschützter Geheimnisse darstellt, die gemäß §203 StGB strafbar ist.

Zunächst war zu klären, ob die Daten, die der ärztlichen Schweigepflicht unterliegen, bei Nutzung von ePost offenbart werden. Zwar ist die Kenntnisnahme der Daten durch die Deutsche Post AG nicht beabsichtigt; allerdings kann auch nicht ausgeschlossen werden, daß bei Produktionsfehlern in verschiedenen Phasen des Verarbeitungsprozesses Mitarbeiter der Post Kenntnis von den Inhalten erhalten (etwa bei Papierstau im Drucker oder bei Fehlern in einer Kuvertiermaschine). Bei derartigen Fehlern würden die Daten Postmitarbeitern offenbart werden.

Der Bundesbeauftragte für den Datenschutz hat die Auffassung vertreten, daß das gesamte ePost-Verfahren (mit Ausnahme der Archivierung) als neuartige Postdienstleistung zu bewerten ist. Postmitarbeiter, die bei Störungen Kenntnis von den Daten erhielten, seien deshalb an das Postgeheimnis gebunden. Eine unbefugte Offenbarung liege nicht vor (17.TB des BfD, 29.3.3).

Demgegenüber ist der Düsseldorfer Kreis mit uns der Auffassung, daß die Nutzung von ePost durch PV zum Versand von Arztrechnungen zu einer unzulässigen Offenbarung der geheimzuhaltenden Patientendaten führen könne.

3.9.2 Prüfung eines ePost-Partnerunternehmens

Die Deutsche Post AG arbeitet zur Erbringung des ePost-Dienstes mit Partnerunternehmen zusammen. Deren Aufgabe besteht in der Akquisition von Kunden und in der Vorverarbeitung von Daten, die von den Kunden angeliefert werden. Wir haben ein derartiges Unternehmen geprüft, das personenbezogene Daten im Auftrag der Kunden verarbeitet.

Die Kunden übertragen ihre Daten (Formulare und Versandlisten) im Regelfall online per ISDN an das geprüfte Unternehmen. Die Daten werden durch das Unternehmen hinsichtlich der Formatierungskonventionen für den ePost-Dienst überprüft und ggf. nachbearbeitet und anschließend per Datenleitung an die ePost-Station der Post übertragen. Die Daten werden bei dem Transport über die Telekommunikationsverbindung vom Kunden an das Unternehmen verschlüsselt, wobei individuelle, mit den jeweiligen Kunden vereinbarte Schlüssel verwendet werden. Zur Verschlüsselung wurde ein paßwortgeschütztes Komprimierungsverfahren verwendet, das als schwach einzuschätzen ist, weil die Verschlüsselung mit verhältnismäßig geringem Aufwand aufzuheben ist. Inzwischen bietet das Unternehmen seinen Kunden jedoch ein sicheres kryptographisches Verschlüsselungsverfahren an.

Die Datenübertragung des Unternehmens an die Post erfolgte überwiegend unverschlüsselt.

Wir haben angeregt, nicht nur die Verbindung zwischen dem Kunden und dem Unternehmen, sondern auch die Datenübertragung von dem Unternehmen an die ePost-Station durch kryptographische Verschlüsselung zu sichern. Die Prüfung hat im übrigen keine Hinweise auf Verstöße gegen datenschutzrechtliche Vorschriften ergeben.

3.10 Änderung des Rundfunkstaatsvertrags

Mit dem Vierten Rundfunkänderungsstaatsvertrag wird der Datenschutz bei Rundfunkprogrammen neu geregelt und weitgehend mit den Datenschutzbestimmungen für Tele- und Mediendienste harmonisiert.

Bei der Übertragung von Rundfunkprogrammen kommt zunehmend digititale Technik zum Einsatz. Diese Innovation ermöglicht nicht nur eine Vervielfachung der gleichzeitig übertragenen Programme; sie gestattet auch gänzlich neue Programmformen und neue Zugriffs- und Abrechnungsverfahren. Zwar ist der Rückkanal derzeit weder im Kabel- noch im Satellitenfernsehen realisiert; durch Kombination dieser Verteiltechniken mit bestehenden „schmalbandigen“ Kommunikationsdiensten (ISDN, Telefon) wird jedoch bereits heute ein gewisser Grad an Interaktivität ermöglicht. Insbesondere im Bezahlfernsehen (Pay TV) sind bereits interaktive Bestell- und Abrechnungsverfahren realisiert, bei denen personenbezogene Daten der Nutzer erhoben und verarbeitet werden. Insofern besteht bereits jetzt die Gefahr, daß das Fernsehverhalten registriert wird und im nachhinein festgestellt werden kann, welcher Nutzer wann welche Sendungen gesehen hat (vgl. 15.TB, 5.1).

Zudem nimmt – durch Einsatz neuer Kompressions- und Übertragungsverfahren – die Übertragungsleistung schmalbandiger Telekommunikationstechnik in starkem Maße zu, so daß auch auf diesem Wege Ton- und Bewegtbildübertragungen möglich werden, die in ihrer Qualität kaum noch hinter herkömmlichen Fernseh- und Hörfunkprogrammen zurückbleiben. Bereits nach geltendem Recht können bestimmte Dienste, die zunächst wegen mangelnder Relevanz für die Bildung der öffentlichen Meinung als Mediendienste eingestuft wurden, bei zunehmender Reichweite und Bedeutung zu Rundfunk werden. Vor diesem Hintergrund war es dringend geboten, die Datenschutzregelungen für den Rundfunk dem inzwischen erreichten Standard für interaktive Tele- und Mediendienste anzupassen (vgl. 3.6).

Dies wird mit dem Vierten Rundfunkänderungsstaatsvertrag geschehen, der voraussichtlich am 1. April 2000 in Kraft treten wird. Im Mittelpunkt der neuen Bestimmungen steht das Recht des Nutzers, sich unbeobachtet und ohne Registrierung seines Nutzungsverhaltens zu informieren und unbeobachtet einzelne Programmangebote in Anspruch zu nehmen. Die Regelungen sollen insofern nicht allein das Recht auf informationelle Selbstbestimmung gewährleisten, sondern darüber hinaus auch die Informationsfreiheit nach Art. 5 Abs. 1 Grundgesetz.

Besonderen Stellenwert besitzen in diesem Zusammenhang die Bestimmungen zum „Systemdatenschutz“ (vgl. auch 3.6.1). Gemäß §47 Abs. 5 Rundfunkstaatsvertrag (RStV) haben sich die Gestaltung und die Auswahl technischer Einrichtungen für die Veranstaltung und den Empfang von Rundfunk an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen. Bereits durch die Gestaltung der Systemstrukturen soll damit die Erhebung, Verarbeitung und Nutzung personenbezogener Daten vermieden und die Selbstbestimmung der Nutzer sichergestellt werden. Dies kann z.B. durch eine dateneinsparende Organisation der Übermittlung, der Abrechnung und Bezahlung sowie der Abschottung von Verarbeitungsbereichen unterstützt werden.

Diese Regelung wird ergänzt durch die Verpflichtung der Veranstalter in §47a Abs. 1 RStV, dem Nutzer die Inanspruchnahme einzelner Angebote und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Nutzungsprofile sind gemäß §47a Abs. 4 RStV nur bei der Verwendung von Pseudonymen zulässig. Dabei dürfen die unter einem Pseudonym erfaßten Nutzungsprofile nicht mit den Daten über den Träger des Pseudonyms zusammengeführt werden.

Nutzungsdaten, d.h. diejenigen personenbezogenen Daten, die während der Inanspruchnahme von Rundfunk entstehen, sind frühestmöglich, spätestens nach Ende der jeweiligen Nutzung zu löschen, soweit sie nicht zu Abrechnungszwecken erforderlich sind. Personenbezogene Daten über Suchschritte (etwa in einem interaktiven Programmführer), die in Hinblick auf Nutzerverhalten und Konsumentenwünsche von Bedeutung sind, sind nach Beendigung der Nutzung des Programmangebots unmittelbar zu löschen.

Die Abrechnungsdaten sind zu löschen, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind. Nutzerbezogene Abrechnungsdaten, die für die Erstellung von Einzelnachweisen erforderlich sind, müssen im Grundsatz spätestens 80 Tage nach Versendung des Einzelnachweises gelöscht werden.

Dabei sind die Abrechnungen so zu gestalten, daß sie grundsätzlich nicht erkennen lassen, welche Programmangebote im einzelnen in Anspruch genommen wurden. Mit dieser Vorschrift soll verhindert werden, daß aufgrund der aufgeschlüsselten Abrechnung personenbezogene Nutzerprofile entstehen und von Dritten (z. B. Mitbenutzer, Betriebsangehörige) eingesehen werden können. Nur wenn der Nutzer einen Einzelnachweis verlangt, darf die Abrechnung über die Inanspruchnahme von einzelnen Programmangeboten aufgeschlüsselt werden.

Im Sinne der Transparenz der Datenverarbeitung ist der Nutzer vor der Erhebung seiner personenbezogenen Daten umfassend zu unterrichten. Nur so kann sich der Nutzer einen angemessenen Überblick über die Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten verschaffen. Der Transparenz dient auch die Vorgabe, daß der Nutzer über die Weiterschaltung zu einem anderen Veranstalter unterrichtet wird. Ohne eine derartige Vorschrift könnten weder das Auskunftsrecht des Nutzers noch eine datenschutzrechtliche Aufsicht wirksam wahrgenommen werden.

Schließlich gewährt der Rundfunkstaatsvertrag dem Nutzer nicht nur hinsichtlich der unter seinem Namen, sondern auch zu den unter Pseudonym gespeicherten Daten ein umfassendes Auskunftsrecht.

Wie bereits der Mediendienstestaatsvertrag enthält nun auch §47e RStV eine Vorschrift zum Datenschutz-Audit (vgl. 3.6.2) , d.h. Veranstalter können ihr Datenschutzkonzept und ihre technischen Einrichtungen von unabhängigen Gutachtern prüfen und das Prüfungsergebnis veröffentlichen lassen. Die Möglichkeit des Datenschutz-Audits richtet sich in erster Linie an die Veranstalter, die bei der Konzeption ihres Angebots datenschutzrechtliche Belange berücksichtigen wollen. Dem kann z.B. durch die Schaffung von Gütesiegeln Rechnung getragen werden.

3.11 Sonstiges

Innerhalb des Netzes der hamburgischen Verwaltung wird zum ersten Mal ein virtuelles privates Netzwerk (VPN) für die Verschlüsselung von Daten auf dem Übertragungsweg eingesetzt.

Das Landesamt für Informationstechnik (LIT) richtet erstmals ein „virtual private network“ (VPN) innerhalb des IP-Netzes der Freien und Hansestadt Hamburg ein. Das Projekt sieht die Verknüpfung von insgesamt 18 Standorten der Steuerverwaltung mit dem FDDI-Ring des LIT über 2 Mbit/s-Leitungen als Ersatz für die bisher genutzten 64 Kbit/s-Standleitungen vor. Die ersten für das Tunneling erforderlichen neuen Router – DES-Verfahren mit 56 Bit Schlüssellänge, 168 Bit sind beantragt – wurden bereits installiert und in Betrieb genommen. Wir begrüßen ausdrücklich diesen ersten Ansatz zur physikalischen Verschlüsselung von Daten im Netz der hamburgischen Verwaltung und hoffen, daß er sich zukünftig auch auf andere sensible Bereiche ausdehnen läßt.

Einzelne Probleme des Datenschutzes im öffentlichen Bereich

4. Parlamentsspezifischer Datenschutz, Wahlen und Volksabstimmungen

4.1 Aktenvorlage an den Parlamentarischen Untersuchungsausschuß „Vergabe und Kontrolle von Aufträgen und Zuwendungen durch die Freie und Hansestadt Hamburg“

Die Anonymisierung von Daten mit streng persönlichem Charakter muß auch in den vorgelegten Stiftungsakten umfassend sichergestellt werden.

Nachdem wir anläßlich eines Beratungsgesprächs mit dem Arbeitsstab des Untersuchungsausschusses in den vorgelegten Akten der Behörde für Arbeit, Gesundheit und Soziales (BAGS) in größerer Zahl sensible personenbezogene Daten festgestellt hatten, führten wir im September 1999 eine umfangreiche Kontrolle dieser Akten in den Räumen des Arbeitsstabes durch. Unsere Prüfung ergab, daß die BAGS in erheblichem Umfang Unterlagen, die einen streng persönlichen Charakter aufwiesen, mit entsprechenden Hinweisen für den Untersuchungsausschuß aus den Akten entnommen oder anonymisiert hatte. Die danach personenbezogen an den Ausschuß übermittelten Daten, insbesondere Angaben zu Höhe und Zeitraum von Fördermitteln und Zuschüssen, erfüllten in der Regel nicht das gesetzliche Merkmal „streng persönlich“.

In einigen Fällen gingen aus den Akten jedoch sehr sensible Daten, die der engeren Persönlichkeits- und Intimsphäre der Betroffenen zuzurechnen waren, mit Personenbezug hervor. In einer Stiftungsakte fanden wir eine Übersicht für den Zeitraum 1978 – 1996 mit den Namen sowie Aufnahme- und Entlassungsdaten von rund 400 Klientinnen, die sich einer sozialtherapeutischen Nachsorge unterzogen hatten. Weitere Stiftungsakten vermittelten personenbezogen Aufschluß über körperliche und geistige Erkrankungen (z.B. Aids, Diabetes, Krebs, spastische Behinderung), über Alkoholismus, Eheprobleme und Suizidgefahr.

Wir legten der BAGS dringend nahe, diese Daten in Abstimmung mit dem Arbeitsstab des Untersuchungsausschusses umfassend zu anonymisieren. Die BAGS hat zugesagt, sich des Problems umgehend anzunehmen und in ihre Prüfung sämtliche an den Ausschuß übersandten Stiftungsakten einzubeziehen.

Hinsichtlich der disziplinar- und strafrechtlich bedeutsamen Vorgänge in Akten über Vormundschaften und Pflegschaften hat die Justizbehörde mit dem Arbeitsstab geklärt, daß der Untersuchungsausschuß diese Akten bis auf weiteres nicht anfordern wird.

4.2 Bürgerbegehren und Bürgerentscheide

Der Datenschutz bei Bürgerbegehren und Bürgerentscheiden bedarf dringend klarer rechtlicher Grundlagen.

Durch Volksentscheid vom 27. September 1998 wurden Bürgerbegehren und Bürgerentscheid als Ausprägungen direkter Demokratie auf Bezirksebene eingeführt. Nach §8 a Abs. 1 des Bezirksverwaltungsgesetzes (BezVG) können die Bürgerinnen und Bürger eines Bezirkes in allen Angelegenheiten, in denen die Bezirksversammlung Beschlüsse fassen kann, einen Bürgerentscheid beantragen (Bürgerbegehren). Ausgenommen vom Bürgerbegehren sind Personalentscheidungen und Beschlüsse über den Haushalt.

§8 a BezVG enthält keine Vorschriften über den Datenschutz. Er beinhaltet – anders als der seinerzeit von der Bürgerschaft zur Abstimmung vorgelegte Gesetzentwurf – auch keine Ermächtigung an den Senat, Einzelheiten des Verfahrens und damit auch den Datenschutz durch Rechtsverordnung verbindlich zu regeln. Deshalb ist für die bei Bürgerbegehren und Bürgerentscheiden erhobenen personenbezogenen Daten keine Zweckbindung gewährleistet, die eine anderweitige Nutzung der Daten, z.B. für allgemeine politische Arbeit oder für kommerzielle Werbung, ausschließt. Die ein Bürgerbegehren tragenden Initiativen sind weder in den Anwendungsbereich des Hamburgischen Datenschutzgesetzes (HmbDSG) einbezogen, noch gilt für ihre Unterschriftenlisten das Bundesdatenschutzgesetz (BDSG). Die Vorschriften über den Datenschutz bei Volksinitiativen, Volksbegehren und Volksentscheiden können weder unmittelbar noch entsprechend herangezogen werden.

Das Senatsamt für Bezirksangelegenheiten (SfB) und die Behörde für Inneres (BfI) haben wir frühzeitig und nachdrücklich auf den Regelungsbedarf hingewiesen. Der Senat lehnt es ab, die im Wege der Volksgesetzgebung beschlossene Vorschrift des §8 a BezVG um datenschutzrechtliche Regelungen zu ergänzen. Deshalb haben wir uns nach einem Gespräch mit dem Trägerkreis „Mehr Demokratie e.V.“, der den Volksentscheid vom 27. September 1998 initiiert hatte, im September 1999 unmittelbar an die Bürgerschaft gewandt. Ob die Fraktionen in der Bürgerschaft unser Anliegen aufgreifen werden, ist noch offen.

Das SfB hat uns im Oktober 1999 den Entwurf einer Dienstvorschrift für die Durchführung von Bürgerbegehren und Bürgerentscheiden in den Bezirken zur Stellungnahme zugeleitet. Wir haben dem SfB gegenüber unterstrichen, daß eine verwaltungsinterne Dienstvorschrift nicht die erforderliche gesetzliche Grundlage für den Datenschutz ersetzen kann. Daneben haben wir Verbesserungen in einzelnen Punkten vorgeschlagen, z.B. zur Berücksichtigung melderechtlicher Auskunftssperren bei den Unterschriftenlisten, zum Abstimmungsgeheimnis und zur Aufstellung von Abstimmungskabinen.

Diese Anregungen hat das SfB nur in geringem Umfang berücksichtigt. Für eine datenschutzgerechte Fassung der Unterschriftenlisten, so das SfB, fehle es an der erforderlichen Rechtsgrundlage. Den Initiatoren könne eine bestimmte Ausgestaltung der Unterschriftenlisten nicht verbindlich vorgeschrieben werden. Gleichwohl legt das SfB durch Dienstvorschrift zwingende inhaltliche Mindesterfordernisse für Unterschriftenlisten fest, von deren Beachtung die Gültigkeit der geleisteten Unterschriften abhängen soll; dies halten wir für inkonsequent. Wir werden uns in weiteren Gesprächen mit dem Trägerkreis „Mehr Demokratie e.V.“ dafür einsetzen, daß trotz der ablehnenden Haltung des SfB dem Datenschutz in der Praxis bei Unterschriftenlisten stärker Rechnung getragen wird.

Ferner fehlt es für die Prüfung der abgegebenen Unterschriften und die Feststellung der Abstimmungsberechtigung mit Hilfe des IuK – Verfahrens Meldewesen (MEWES) an einer Rechtsgrundlage.

5. Umweltschutz

5.1 Hamburgisches Bodenschutzgesetz

Bei Eingriffen in das informationelle Selbstbestimmungsrecht und bei Abweichungen von Bestimmungen des Datenschutzgesetzes kann nicht auf bereichsspezifische datenschutzrechtliche Regelungen verzichtet werden.

Bei der behördlichen Abstimmung über den Entwurf zum Hamburgischen Bodenschutzgesetz wurde von einer Behörde u.a. die Forderung erhoben, auf die bereichsspezifischen datenschutzrechtlichen Regelungen weitgehend zu verzichten und stattdessen auf die geltenden Bestimmungen des Hamburgischen Datenschutzgesetzes zu verweisen.

Dieser Forderung konnten wir nicht folgen. Die vorgesehenen datenschutzrechtlichen Regelungen weichen teilweise von den Bestimmungen des Hamburgischen Datenschutzgesetzes ab. Der Eingriff in das Recht auf informationelle Selbstbestimmungsrecht sowie das Gebot der Normenklarheit und der Bestimmtheit machen es erforderlich, für die Bürgerinnen und Bürger klare und eindeutige datenschutzrechtliche Regelungen zu fassen.

Nach derzeitigem Kenntnisstand gehen wir davon aus, daß das im Jahre 1998 eingeleitete behördliche Abstimmungsverfahren in einigen Monaten abgeschlossen sein wird.

5.2 Sonstiges

Bei den Novellierungen des Hamburgischen Naturschutzgesetzes, des Hamburgischen Abwassergesetzes und des Hamburgischen Wassergesetzes sollen ebenfalls die bisher fehlenden bereichsspezifischen datenschutzrechtlichen Regelungen soweit wie erforderlich getroffen werden. Die einzelnen behördlichen Abstimmungsverfahren waren allerdings bis Redaktionsschluß noch nicht abgeschlossen.

6. Sozialdaten

6.1 Zusammenarbeit von Sozialleistungsträgern mit Strafverfolgungsbehörden

Die ersten Erfahrungen zeigen, daß sich die Zusammenarbeit weiterhin in engen Grenzen hält.

Am 7. August 1998 ist mit dem Ersten Gesetz zur Änderung des Medizinproduktegesetz eine Änderung des §68 SGB X in Kraft getreten. Danach ist es Sozialleistungsträgern erlaubt, insbesondere die Polizei auf deren Ersuchen zu informieren, wenn sich ein Bürger bei ihnen aufhält bzw. für wann er einen Termin dort vereinbart hat. Wesentlicher Zweck der Vorschrift ist es, daß ein von der Polizei oder Staatsanwaltschaft gesuchter Bürger beim Sozialleistungsträger verhaftet oder festgenommen werden kann. Allerdings hat der Gesetzgeber eine Begrenzung auf die mit Haftbefehl gesuchten Personen nicht vorgenommen. Deshalb kann sich die Polizei auch zur Erfüllung aller ihrer Aufgaben der Sozialleistungsträger bedienen. In der Begründung zur Gesetzesänderung heißt es wörtlich:

> „Mit der Regelung wird klargestellt, daß die Sozialleistungsträger beispielsweise der Polizei auf Ersuchen den derzeitigen oder künftigen Aufenthalt eines Leistungssuchenden mitteilen dürfen. Es kann nicht hingenommen werden, daß eine polizeilich gesuchte Person die Sozialverwaltung aufsuchen und aufgrund unterschiedlicher Auffassungen in der Praxis darauf vertrauen kann, daß die Polizei von dem Besuch nichts erfährt. Außerdem wird konkretisiert, daß die Behörde den derzeitigen oder künftigen Aufenthalt dann übermitteln darf, wenn das Ersuchen nicht länger als sechs Monate zurückliegt."

Um Unsicherheiten bei diesem neuen Verfahren in der praktischen Umsetzung zu begegnen, hat das Landessozialamt in enger Abstimmung mit der Justizbehörde, der Behörde für Inneres, dem Senatsamt für Bezirksangelegenheiten und uns eine Arbeitshilfe erarbeitet, die seit dem 29. Januar 1999 allen Bediensteten in den Sozialdienststellen zur Verfügung steht. Das Landessozialamt will die gemachten Erfahrungen zu gegebener Zeit auswerten und prüfen, ob Änderungen der Arbeitshilfe erforderlich sind.

Parallel dazu haben wir die Bezirksämter und weitere Sozialleistungsträger, die unserer Kontrolle unterliegen, gebeten, im ersten Quartal 1999 eingehende Ersuchen nach §68 SGB X statistisch zu erfassen und uns darüber zu berichten. Die uns vorliegenden Ergebnisse zeigen folgendes:

• Bei den jeweiligen Sozialleistungsträgern gingen durchweg weniger als zehn Ersuchen ein.

• Die meisten Ersuchen wurden von der Polizei an die Sozialleistungsträger gerichtet und gelegentlich auch von den Gerichten, Staatsanwaltschaften und Justizvollzugsanstalten.

• In den meisten Fällen wurde gefragt nach Namen, Geburtsdatum/-ort, derzeitiger Anschrift und Name/Anschrift des Arbeitgebers. An zweiter Stelle interessierte der derzeitige bzw. künftige Aufenthaltsort des Hilfeempfängers.

• Am häufigsten wurde die Anfrage damit begründet, daß die gesuchte Person wegen eines vorliegenden Haftbefehls zur Fahndung ausgeschrieben war. Aber auch nicht alltägliche Gründe wurden genannt. So fragte eine polizeiliche Verkehrsstaffel bei einer Betriebskrankenkasse nach dem aktuellen Aufenthaltsort des Betroffenen; Hintergrund war die gerichtlich angeordnete Beschlagnahme eines Führerscheins. Da der Betroffene an seinem Wohnsitz nicht angetroffen wurde, hatte sich die Polizei zunächst an den ihr bereits bekannten Arbeitgeber gewandt. Von dort erfuhr sie, daß der Betroffene zur Kur sei, man wisse jedoch nicht wo. Die Betriebskrankenkasse des Unternehmens, die für die Kosten der Kur aufkomme, könne hierzu Auskunft geben. Daraufhin erfolgte die Anfrage bei der Krankenkasse, die als aktuellen Aufenthaltsort im Sinne von §68 Absatz 1 Satz 1 SGB X die Anschrift der Kurklinik mitteilte.

Nach dem Ergebnis der Umfrage haben wir derzeit keine Veranlassung, das Verfahren einer vertieften datenschutzrechtlichen Überprüfung zu unterziehen. Allerdings werden wir die weitere Entwicklung der Praxis beobachten und ggf. ergänzende datenschutzrechtliche Hinweise zum Umgang mit den Ermittlungsersuchen geben.

6.2 Pädagogische Betreuung im eigenen Wohnraum (PBW)

Es bestehen große Unsicherheiten darüber, welche Informationen das Sozialamt für die Antragsbearbeitung benötigt.

In der Zeit vom 1. Januar bis zum 31. August 1999 wurde im Ortsamt Billstedt im Rahmen eines Pilotprojektes eine neue Form der Bearbeitung von Anträgen auf pädagogische Betreuung im eigenen Wohnraum (PBW) erprobt. Wir hatten Gelegenheit, das Projekt zu begleiten.

Bei PBW handelt es sich um eine „Sonstige Hilfe“ nach §40 Abs. 1 Bundessozialhilfegesetz (BSHG), also um eine Hilfe, die nicht explizit in dieser Bestimmung aufgeführt ist. PBW ist eine pädagogisch orientierte ambulante Maßnahme, die geistig Behinderten, Sinnesbehinderten sowie körperlich und mehrfach Behinderten helfen soll, in ihrer eigenen Häuslichkeit selbständig und möglichst unabhängig von öffentlichen Hilfen zu leben. Zweck ist nicht die laufende Übernahme von Tätigkeiten für den behinderten Menschen, sondern Anleitung zur Selbsthilfe. Eine Globalrichtlinie der Behörde für Arbeit, Gesundheit und Soziales enthält die entsprechenden Rahmenvorgaben für das Verfahren.

PBW soll

• eine stationäre Unterbringung verhindern,

• die Entwicklung von Selbständigkeit fördern,

• die Mobilität und Orientierung am Wohnort herstellen,

• die Gestaltung des sozialen und Arbeitsumfelds fördern,

• dem behinderten Menschen helfen, sein Wohnumfeld und seine Freizeit zu gestalten.

Ein wesentliches Element für die neue Aufgabenwahrnehmung ist der Reha-Gesamtplan nach §46 BSHG, der zwar schon länger vorgeschrieben, aber bislang kaum Praxis ist. An seiner Erstellung soll der Betroffene bzw. sein Betreuer teilnehmen. Bewilligungen von PBW-Leistungen sollen zukünftig nur erfolgen, sofern damit auch Zielvorgaben verbunden werden. Nach Ablauf vereinbarter Fristen ist die Zielerreichung zu überprüfen und entweder eine Verlängerung der Maßnahme zu bewilligen oder eine andere, geeignetere Leistung.

Die Erstellung des Reha-Gesamtplanes wurde im Projekt EDV-mäßig unterstützt. Im wesentlichen wurden dabei schematische Fähigkeitsprofile erstellt und eine Kompetenzeinstufung vorgenommen (z.B. Fähigkeit und Hilfebedarf bei der Wohnraumbeschaffung). Das EDV-Verfahren lieferte automatisiert einen Vorschlag für Hilfebedarfe, der als Grundlage für eine Bedarfsplanung in Form eines Bewertungsrasters diente. Zusätzlich bestand die Möglichkeit, kurzfristige Ziele als Freitext festzuhalten. Wir haben verlangt, daß die EDV-Unterstützung lediglich als Hilfsmittel für die Hilfeplanung eingesetzt werden darf. Es muß dabei bleiben, daß eine Entscheidung erst nach genauer Ansehung eines jeden Einzelfalles – unter Gesamtwürdigung der jeweiligen persönlichen Gegebenheiten – zu erfolgen hat. Da dies verfahrensmäßig sichergestellt worden ist, haben wir insoweit auch keine Sorge, daß der Einsatz des EDV-Verfahrens zu – unzulässigen – automatisierten Einzelfallentscheidungen führt.

Im Rahmen des Pilotprojektes wurde auch das Instrument der Betreuungskonferenz erprobt, um in Anlehnung an die Erziehungskonferenz aus dem Kinder- und Jugendhilfebereich (vgl. §36 SGB VIII) die Kompetenz des Hilfebedürftigen sowie Art und Umfang der Hilfe im Zusammenwirken aller beteiligten Stellen mit dem Hilfebedürftigen gemeinsam zu ermitteln. Die gemeinsame Entscheidungsfindung in der Betreuungskonferenz begegnet keinen grundsätzlichen datenschutzrechtlichen Bedenken, denn es liegt im Interesse des Hilfebedürftigen, daß nicht nur Experten über die zu ergreifenden Maßnahmen entscheiden. Vielmehr hat der Hilfebedürftige durch seine Teilnahme an der Betreuungskonferenz die Möglichkeit, die eigene Sichtweise seiner Lebenssituation deutlich zu machen und damit zu einer Entscheidung beizutragen, die am besten seinen persönlichen Lebensumständen gerecht wird. Außerdem wird dadurch die Transparenz des Entscheidungsprozesses verbessert.

Es kommt allerdings darauf an, daß sowohl die Durchführung als auch die Dokumentation der Betreuungskonferenz so abläuft, daß weder Persönlichkeitsrechte des Betroffenen gefährdet werden noch beteiligte Experten unzulässigerweise Daten über den Betroffenen offenbaren. Dies bedeutet im einzelnen:

• Mangels einer spezialgesetzlichen Bestimmung, die eine Offenbarung personenbezogener Daten des Betroffenen durch Sozialarbeiter bzw. Sozialpädagogen oder Ärzte in der Betreuungskonferenz zulässt, muß die Einwilligung des Betroffenen zur Weitergabe der Sozialdaten an die Betreuungskonferenz – und damit an einen größeren Personenkreis – eingeholt werden. Ansonsten ist zu befürchten, daß sich die Sozialarbeiter bzw. Sozialpädagogen und Ärzte nach §203 Abs. 1 StGB strafbar machen.

• Nach dem Erforderlichkeitsprinzip ist auch zu erwägen, ob nicht ein Austausch in kleiner Runde zunächst ausreicht. Das Ergebnis einer solchen Vor-Erörterung im kleinen Kreis könnte anschließend zusammengefaßt in der Betreuungskonferenz dargestellt werden.

• Soweit Sozialdaten mit dem Einverständnis des Betroffenen in der Betreuungskonferenz mitgeteilt werden, sollte darauf hingewiesen werden, daß diese Angaben den Einschränkungen nach §76 SGB X und der Zweckbindung nach §78 SGB X unterliegen.

• Dem Sozialhilfesachbearbeiter ist die Teilnahme an der Betreuungskonferenz in jedem Fall zu ermöglichen, da er über den Hilfeantrag zu entscheiden hat. Dies gilt für Vorgesetzte nur dann, sofern im Einzelfall bereits vorher erkennbar ist, daß sie in den Entscheidungsprozeß eingebunden sein werden. Steht dies nicht fest, darf dieser Personenkreis nicht teilnehmen, weil ansonsten die Gefahr besteht, daß der Kreis zu groß wird.

• Über das Ergebnis der Betreuungskonferenz sollte ein Protokoll angefertigt werden, das nur die für die Entscheidungsfindung erforderlichen Angaben enthält. Es ist darauf zu verzichten, die Beratungsinhalte im einzelnen wiederzugeben. Vielmehr reicht es aus, Gesprächsergebnisse zusammenzufassen.

Im übrigen hat sich im Verlauf des Projektes gezeigt, daß es ein Spannungsverhältnis zwischen den begutachtenden Stellen (z.B. dem Gesundheitsamt oder den Freien Trägern) und dem Sozialamt als Kostenträger gibt. Dieses Spannungsverhältnis ist auch aus anderen Sozialleistungsbereichen bekannt und rührt insbesondere daher, daß nicht immer deutlich ist, welche Angaben der Kostenträger für die Entscheidung über den Antrag auf eine Sozialleistung tatsächlich benötigt. So wurde uns berichtet, daß das Sozialamt darauf bestehe, umfangreiche medizinische und sozialpädagogische Stellungnahmen über die Person des Antragstellers zu erhalten. Nicht in jedem Fall sei erkennbar gewesen, daß die Stellungnahmen in einem derartigen Umfang auch für die Antragsbearbeitung erforderlich seien.

Um für alle Beteiligte eine tragfähige Lösung zu erarbeiten, haben wir deshalb vorgeschlagen, zunächst einmal gemeinsam den Versuch zu unternehmen, die für das Sozialamt als Kostenträger erforderlichen Angaben zu definieren. Wir waren uns dabei darüber im klaren, daß dies nicht beim ersten Anlauf zufriedenstellend gelingen kann. Dennoch haben wir an dem Vorschlag festgehalten, weil von der Antwort auf die Frage, was das Sozialamt tatsächlich wissen muß, die Qualität des Berichtswesens der übermittelnden Stellen ganz wesentlich abhängt. Leider wurde dieser Punkt im Projekt nicht weiter diskutiert, sondern lediglich der Behörde für Arbeit, Gesundheit und Soziales zur Stellungnahme vorgelegt. Erst nach mehrmaliger Erinnerung erhielten wir die Mitteilung, daß der Umfang der erforderlichen Detailinformationen allein vom Einzelfall abhänge. Es lasse sich also keine abschließende Liste erstellen. Im Einzelfall könnten dafür auch medizinische Diagnosen und Prognosen über die Entwicklung erforderlich sein. Im übrigen gehe die Behörde für Arbeit, Gesundheit und Soziales davon aus, daß die Zusammenarbeit der an der Hilfe beteiligten Dienststellen und deren Rolle im Verfahren einvernehmlich zwischen der Behörde für Arbeit, Gesundheit und Soziales und dem Senatsamt für Bezirksangelegenheiten geregelt werde.

Diese Reaktion ist unter zwei Gesichtspunkten unbefriedigend. Zum einen war es niemals unsere Absicht, eine abschließende Liste der erforderlichen Angaben zu erarbeiten. Es kann selbstverständlich lediglich nur darum gehen, die erforderlichen Informationen unter übergeordneten Gesichtspunkten zu definieren. Zum anderen erachtet es die Behörde für Arbeit, Gesundheit und Soziales offensichtlich nicht für notwendig, uns an dieser Fachdiskussion zu beteiligen. Wir haben deshalb die Behörde gebeten, ihren Standpunkt noch einmal zu überdenken, zumal vorgesehen ist, künftig in allen Sozialämtern Anträge auf PBW-Leistungen so zu bearbeiten, wie es im Rahmen des Projektes in Billstedt ausprobiert wurde.

6.3 Projekt Sozialhilfe-Automation (PROSA)

Das neue PROSA-Verfahren darf die Sicherheit der Sozialdaten nicht gefährden.

Seit unserer letzten Berichterstattung (vgl. 16. TB, 6.3) hat die Praxis gezeigt, daß zusätzliche Anforderungen an das PROSA-Verfahren zu verwirklichen sind. Im Online-Betrieb werden derzeit bis zu 35 Millionen Datenbankzugriffe mit ca. 1 Million Transaktionen täglich abgesetzt. Mit dem Verfahren werden ca. 145.000 aktive Fälle bearbeitet, im Jahre 1998 wurden über die verschiedenen Verfahrensteile weit über 1 Milliarde DM ausgezahlt.

Die Komplexität der Fälle macht die Darstellung im gegenwärtigen Verfahren mit der Vielzahl von Masken unkomfortabel. Individuell einstellbare Fallübersichten sind mit der bisherigen Technik nicht möglich. Für eine komplette elektronische Akte fehlt die Möglichkeit, Dokumente zu scannen und in die Datenbank zu schreiben. Außerdem soll die Integration einer modernen Textverarbeitung sowie weiterer Komponenten von Microsoft-Office erfolgen. Wegen dieser vielfältigen neuen Anforderungen heißt das neue Projekt OPEN-PROSA, also ein PROSA, das offen für die verschiedensten Erweiterungen sein soll. Wir sind vom Senatsamt für Bezirksangelegenheiten (SfB) von Beginn an eng in diese Entwicklung eingebunden worden.

Das SfB plant in einem ersten Schritt zunächst einen Technikaustausch, also im wesentlichen den Wechsel der Endgeräte von Terminal auf PC. Mit dem Abschluß des Technikaustausches wird für November 2000 gerechnet, wobei zwischenzeitlich der Betrieb des Basisverfahrens weitergehen soll.

Bereits in diesem frühen Planungsstadium haben wir den an jedem Sachbearbeiterplatz vorgesehenen Einsatz von E-Mail- und Internet-Funktionalität unter Hinweis auf den Infrastrukturansatz durch Windows NT problematisiert (vgl. 3.3). Wir sehen mit der Einführung dieser Funktionalitäten eine nicht zu unterschätzende Gefährdung der besonders schützenswerten Sozialdaten. Das SfB will hierüber zunächst keine eigene Entscheidung treffen, sondern die weiteren Gespräche zwischen der Finanzbehörde und uns abwarten. Insbesondere soll abgewartet werden, wie die Finanzbehörde das Schutzniveau unter Windows NT für sensible Daten weiter beurteilt.

Daneben haben wir angesprochen, daß nach unseren Prüferfahrungen die Vorgaben des SfB zur Systemadministration wohl für die einzelnen Bezirksämter nicht unbedingt durchgängig verbindlich sind. Um eine einheitliche Praxis zu erreichen, will das SfB deshalb bei sich bietender Gelegenheit eine gemeinsame Besprechung mit den IuK-Verantwortlichen der Bezirksämter unter unserer Beteiligung veranstalten.

Sollten sich im Hinblick auf den Datenschutz bei der Entwicklung von PROSA zu OPEN-PROSA zusätzliche Probleme ergeben, werden wir darauf in unserem nächsten Bericht eingehen.

6.4 Online-Zugriffe des Rechnungshofs auf Sozialdaten

Der hohe Sicherheitsstandard für Sozialdaten muß auch bei einem Online-Zugriff des Rechnungshofs gewährleistet sein.

Nach einer Vereinbarung aus dem Jahre 1995 auf Grund von §79 Abs. 2 SGB X besteht für den Rechnungshof die Möglichkeit, sich Daten des Dialogverfahrens Projekt Sozialhilfeautomation (PROSA) durch lesenden Zugriff für Prüfzwecke übermitteln zu lassen. Bisher wurden die abgerufenen Daten ausschließlich an zwei hierfür definierten Endgeräten in gesonderten Räumen des Rechnungshofes sichtbar gemacht. Der Rechnungshof hat den Wunsch geäußert, die von PROSA für Prüfzwecke zur Verfügung gestellten Daten direkt am Arbeitsplatz den an den Prüfungen beteiligten Prüferinnen und Prüfern verfügbar zu machen. Dadurch entstehen Risiken für die im Netz verarbeiteten personenbezogenen Sozialhilfedaten, die in keinem angemessenen Verhältnis zu dem damit verfolgten Zweck stehen.

Wir haben in der Diskussion um die Einrichtung von Online-Zugriffen des Rechnungshofs auf Daten der hamburgischen Verwaltung nicht bestritten, daß sich der Rechnungshof im Rahmen seiner gesetzlich geregelten Auskunftsansprüche auch des Online-Zugriffs auf automatisiert geführte Datenbestände bedienen kann. Dabei hat jedoch aus datenschutzrechtlicher Sicht immer eine Abwägung mit den schutzwürdigen Belangen der Betroffenen zu erfolgen. Gerade die im Sozialhilfeverfahren verarbeiteten personenbezogenen Daten sind derart sensibel, daß für die Sachbearbeitung in den Sozialdienststellen ein hoher technischer und organisatorischer Aufwand für Maßnahmen zur Datensicherung und Datenschutzkontrolle getroffen werden muß. So wurden beispielsweise physikalisch getrennte Netze geschaffen, d.h. der Datenverkehr im Sozialbereich läuft nicht zwangsläufig über die Verkabelung, auf der auch die sonstige Bürokommunikation in den Bezirken erfolgt. Electronic Mail und direkter Zugriff auf das Internet am Arbeitsplatz der Sachbearbeiter ist wegen des damit verbundenen, nicht restlos beherrschbaren Risikos für die Sicherheit der Sozialdaten entweder überhaupt nicht oder nur mit zwei voneinander unabhängigen Benutzerumgebungen möglich. Dieser hohe Sicherheitsstand muß auch vom Rechnungshof gewährleistet werden.

Die Problematik hat weiter an Bedeutung gewonnen, weil der Rechnungshof auch auf das IuK-Verfahren Projekt Jugendamts-Automation (PROJUGA) in gleicher Weise zu Prüfzwecken lesend zugreifen möchte. Hierfür ist zwischen dem Rechnungshof und dem Senatsamt für Bezirksangelegenheiten am 1. November 1998 eine Vereinbarung nach §79 Abs. 2 SGB X geschlossen worden. Dabei ist seitens des Senatsamtes für Bezirksangelegenheiten versäumt worden, uns bereits vor Abschluß – wie es das Gesetz vorsieht – zu informieren und in die Verhandlungen mit einzubeziehen. Das Senatsamt für Bezirksangelegenheiten hat dieses Versäumnis inzwischen ausdrücklich bedauert.

Die geschlossene Vereinbarung sieht allerdings vor, uns bei der Realisierung von automatisierten Verfahren zum Abruf von Daten aus dem Dialogverfahren PROJUGA frühzeitig einzubeziehen. Hierfür gab es bislang noch keine Veranlassung, weil der Rechnungshof noch nicht den automatisierten Abruf von Daten aus PROJUGA für Prüfzwecke benötigt hat.

In Anbetracht dieser Entwicklung haben wir das Senatsamt für Bezirksangelegenheiten gebeten, gemeinsam mit dem Rechnungshof und uns das weitere Vorgehen bei Online-Zugriffen des Rechnungshofs auf Sozialdaten insgesamt grundsätzlich abzustimmen. Leider mußte ein bereits anberaumtes erstes Treffen kurzfristig vom Rechnungshof abgesagt und auf das Jahr 2000 verschoben werden. Wir gehen jedoch davon aus, daß eine Verfahrensänderung hinsichtlich des Online-Zugriffs auf PROSA und die Realisierung eines Online-Abrufverfahrens für PROJUGA erst dann stattfinden wird, wenn die Angelegenheit abschließend zwischen allen Beteiligten geklärt ist.

6.5 Hamburgisches Erziehungsgeldverfahren (HErz)

Bei der Prüfung des Hamburgischen Erziehungsgeldverfahrens wurden zahlreiche Mängel sowohl im Bereich der Fachlichen Leitstelle als auch im Bezirksamtsbereich festgestellt.

Im Berichtszeitraum haben wir das neue Hamburgische Erziehungsgeldverfahrens (HErz) geprüft. Gegenstand der Prüfung war sowohl die Fachliche Leitstelle im Senatsamt für Bezirksangelegenheiten (SfB) als auch die Sachbearbeitung im Bezirksamt Eimsbüttel. Dabei wurden folgende Datenschutzdefizite festgestellt:

1. HErz ersetzt im Gegensatz zu dem Sozialhilfeverfahren PROSA keine traditionellen Akten; vom Bürger vorzulegende Bescheinigungen über Mutterschaftsbezüge, Beschäftigungsverhältnisse und Verdienstbescheinigungen werden auch weiterhin ausschließlich in der Akte aufbewahrt. Wir haben problematisiert, daß die gesetzlichen Aufbewahrungsfristen von 6 Jahren auch auf das EDV-Verfahren abgebildet werden müssen. Dieser Forderung wurde entsprochen.

2. Die PC der Fachlichen Leitstelle bildeten zusammen mit zahlreichen anderen PC der IuK-Abteilung des SfB ein gemeinsames physikalisches Subnetz. Da die Daten im Netz der IuK-Abteilung broadcastorientiert übertragen werden, bestand die Gefahr, daß die Daten von Mitarbeitern der IuK-Abteilung des SfB mitgelesen werden. Dies ist besonders problematisch, da nicht nur die Anwendungsdaten zwischen den Client der Fachlichen Leitstelle und dem Server im Landesamt für Informationstechnik (LIT) unverschlüsselt übertragen werden, sondern auch die HErz-Paßwörter zur Authentisierung gegenüber dem Host. Aufgrund unserer Kritik wurde die Datenübertragung bei der IuK-Abteilung des SfB inzwischen auf Switching-Technologie umgestellt.

3. Die Problematik broadcastorientierter Datenübertragung gilt auch für das geprüfte Bezirksamt Eimsbüttel. Hier werden zwar teilweise bereits Switches eingesetzt. Ein Gesamtkonzept für den Einsatz von Switches soll aber erst entwickelt werden.

4. Die bisher von der Fachlichen Leitstelle herausgegebenen technisch-organisatorischen Vorgaben zur Umsetzung des technischen Konzepts in den Bezirksämtern sind zu unverbindlich. Dies gilt insbesondere für den Einsatz von Windows NT. Das SfB teilt diese Kritik und hat zugesagt, die Vorgaben in Zusammenarbeit mit den IuK-Abschnitten der Bezirke so bald wie möglich zu vereinheitlichen.

5. Die Fachliche Leitstelle verfügt über NT-Rechner, die mit Diskettenlaufwerken ausgestattet sind. Ebenso steht umfassende E-Mail-Funktionalität zur Verfügung. Da von diesen Rechnern aus auf sämtliche Daten des Erziehungsgeld-Verfahrens zugegriffen werden kann, haben wir in Anlehnung an das von uns vorgeschlagene NT-Grundschutzkonzept dem SfB empfohlen, zwei getrennte Arbeitsumgebungen auf den NT-Rechnern der Fachlichen Leitstelle einzurichten. Diese Empfehlung wurde mit Hinweis auf die Stellungnahme der Finanzbehörde verworfen (vgl. 3.3).

6. Auf den NT-Rechnern der Fachlichen Leitstelle ist SMS (System Management Server) installiert, das den Remote-Zugriff auf diesen Rechner ermöglicht. SMS war so konfiguriert, daß der Remote-Zugriff nicht ausdrücklich vom Mitarbeiter der Leitstelle freigegeben werden mußte. Der aktuelle Remote-Zugriff wurde zwar symbolhaft auf der Taskleiste von Windows NT angezeigt. Den Mitarbeiterinnen und Mitarbeitern der Fachlichen Leitstelle war jedoch nicht bekannt, daß die Möglichkeit eines Remote-Zugriffs überhaupt existierte. Aufgrund unserer Kritik wurde SMS inzwischen so konfiguriert, daß der Anwender den SMS-Zugriff auf sein Endgerät explizit freigeben muß und er dies auch visuell erkennen kann.

7. Auf einem der im Bezirksamt geprüften NT-Rechner waren sowohl der lokale Registry-Editor als auch das Programm TUN Net in vollem Funktionsumfang verfügbar. Mit Hilfe von TUN Net können sicherheitskritische Internetdienste wie beispielsweise telnet, ftp, ping, wall aufgerufen werden. Beide Programme wurden inzwischen für die Sachbearbeiter gesperrt.

8. Die Sachbearbeiter in den Bezirksämtern müssen sich sowohl gegenüber Windows NT als auch gegenüber dem HErz-Verfahren authentisieren. Dies ist aus datensicherheitstechnischer Sicht problematisch, da sich der Benutzer zwei Paßwörter merken muß, ohne daß hiermit die Sicherheit des Gesamtsystems erhöht wird. Diese Situation führt aus unserer Erfahrung in aller Regel dazu, daß entweder auf allen Ebenen gleiche Paßwörter benutzt oder die verschiedenen Paßwörter aufgeschrieben werden. Wir haben daher ein Single-Logon-Verfahren empfohlen, das die beiden Authentisierungsebenen synchronisiert.

9. Sämtliche NT-Rechner wurden im Bezirksamt Eimsbüttel von 5 Mitarbeitern der IuK-Abteilung über die Standardkennung administriert. Hierdurch bestand nicht nur das Risiko, daß das verwendete Gruppenpaßwort einem größeren Personenkreis bekannt wird. Es besteht auch das Problem, daß die Standardkennung zum Ziel von Angriffen per Paßwortgenerator wird. Auf unsere Anregung hin wurden individuelle Systemverwalterkennungen eingerichtet.

6.6 Prüfung in der Schwerbehindertenabteilung des Versorgungsamtes

Die festgestellten Mängel hätten nicht auftreten müssen, wenn wir in üblicher Weise an der Vorbereitung des neuen EDV-Verfahrens beteiligt worden wären.

Das bisherige Schwerbehinderten-Dialogverfahren wurde am 1. Juli 1999 durch eine moderne DV-Lösung in Client/Server-Architektur abgelöst, ohne daß wir Gelegenheit hatten, das neue Verfahren abschließend datenschutzrechtlich zu beurteilen. Zwar hatte uns das Versorgungsamt zunächst einige Materialien zur Verfügung gestellt, die Gegenstand einer gemeinsamen Erörterung waren. Unsere sich daran anschließenden ergänzenden Anfragen wurden dann aber vom Versorgungsamt entweder überhaupt nicht oder nur sehr zögerlich behandelt. Insbesondere war es nicht möglich, uns eine Verfahrensbeschreibung zur Verfügung zu stellen. Wegen unserer regelmäßigen Praxis, allein wegen Mängeln im Beteiligungsverfahren nicht von der Möglichkeit einer Beanstandung nach §25 Abs. 1 HmbDSG Gebrauch zu machen, haben wir auch in diesem Fall davon abgesehen. Eine datenschutzrechtliche Prüfung des neuen Verfahrens war nach dieser Vorgeschichte allerdings zwingend.

Die Prüfung wurde im letzten Quartal des Jahres 1999 durchgeführt. Die Schwerbehindertenabteilung des Versorgungsamtes hat sich unter neuer Leitung fristgerecht zu unserem Prüfprotokoll geäußert, so daß wir in der Lage waren, eine Bewertung der Prüfergebnisse vorzunehmen. Wegen des Zeitablaufs können wir aber nachfolgend nur unsere festgestellten Datenschutzdefizite darstellen, ohne daß uns bis zum Redaktionsschluß eine Reaktion des Versorgungsamtes vorliegen konnte.

– Der Server des unter Windows NT laufenden Verfahrens ist eingebunden in die Domäne der Behörde für Arbeit, Gesundheit und Soziales (BAGS). Langfristig ist geplant, für den Bereich Soziales und Gesundheit jeweils eine eigene Domäne zu bilden. Sämtliche BAGS-Kennungen können derzeit noch domänenweit aufgerufen werden, ohne daß hierfür eine funktionale Notwendigkeit besteht. Um den damit einhergehenden Risiken entgegenzutreten, haben wir gefordert, möglichst eine eigene Domäne für jedes Amt der BAGS einzurichten.

– Die Daten werden in komprimierter, nicht verschlüsselter Form über das FHH-Netz zu einer NT-Workstation in der BAGS exportiert, um von dort in unverschlüsselter Form per ISDN zur ePost-Zentrale nach Hannover übermittelt zu werden. Die ePost, ein Dienstleistungsangebot der Deutschen Post AG, erledigt bestimmte Druckaufträge auf der Grundlage von vertraglichen Rahmenbedingungen, die zentral von der BAGS geschaffen worden sind. In Anbetracht der Sensibilität der Daten, die hierbei transportiert werden, haben wir eine Verschlüsselung der Datensätze auf der gesamten Wegstrecke sowohl innerhalb des FHH-Netzes als auch im Netz der Telekom verlangt.

– Das FHH-Netz wird zudem benötigt für die Übermittlung von Daten der Schwerbehindertenabteilung an die Rechtsabteilung des Versorgungsamtes, die auf einem MVS-Host gespeichert werden. Die Kommunikation wird von dem MVS-Host angestoßen. Der Anschluß des Versorgungsamtes an das FHH-Netz erfolgt über Router; die IP-Pakete werden auf dem Router nach IP-Adressen gefiltert. Zusätzlich ist eine Filterung der Router nach TCP/IP-Diensten erforderlich.

– In dem neuen Verfahren existiert kein Internetzugang und in der Regel auch keine E-Mail-Funktionalität. Die Mitarbeiter haben lediglich Zugriff auf den Web-Server der BAGS. In Anbetracht des Infrastrukturansatzes unter Windows NT (vgl. 3.3) haben wir darauf gedrungen, auch künftig keine E-Mail-Funktionalität und keinen Internetzugang auf Arbeitsplatzrechnern mit Zugriff auf sensible personenbezogene Daten zuzulassen.

Ein umfassendes Sicherheitskonzept für den Einsatz von Windows NT fehlt bislang in der BAGS. Die Prüfung im Versorgungsamt hat uns Gelegenheit gegeben, auf dieses Defizit aufmerksam zu machen und die Erarbeitung eines solchen Konzeptes zu verlangen.

6.7 Informationsverarbeitung in der Pflege bei pflegen & wohnen

pflegen & wohnen hat schließlich doch noch konstruktiv auf unsere Kritik reagiert.

Die bisherige Pflegedokumentation von pflegen & wohnen war von uns nachhaltig kritisiert worden (vgl. 15. TB, 6.3, 16. TB, 6.6). Im Kern ging es uns darum, nur die Sammlung solcher Daten vorzusehen, die auch tatsächlich pflegerelevant sind.

Nachdem pflegen & wohnen fast ein halbes Jahr lang nicht auf unsere Kritik reagiert hatte, teilte uns das Unternehmen Ende Januar 1999 mit, daß nicht zuletzt unsere Feststellungen dazu geführt haben, ein neues Verfahren zu installieren, mit dem die bisherigen Probleme der Pflegedokumentation und der Abrechnung mit den Bewohnern und Kostenträgern im Rahmen einer veränderten Organisationsstruktur und einer neuen IT-Landschaft gelöst werden sollen. Die konzeptionellen Arbeiten, die in enger Abstimmung mit den Pflegeeinrichtungen und einem externen Dienstleister durchgeführt wurden, sind inzwischen abgeschlossen. Als Ergebnis liegt jetzt ein Datenkatalog vor, der die verschiedenen Aspekte des SGB XI, des Haftungsrechts und der Pflegeanforderungen berücksichtigen soll. Sobald über den Einsatz eines geeigneten Softwareproduktes entschieden und die Anpassung des Tools an die Besonderheiten von pflegen & wohnen erfolgt ist, soll die Produktion voraussichtlich im Laufe des Jahres 2000 aufgenommen werden.

Mit pflegen & wohnen besteht Einvernehmen darüber, daß die Informationssammlung im Sinne einer ganzheitlichen Pflege anzulegen ist und nur die pflegerelevanten Daten umfassen darf. Wir hatten Gelegenheit, das Anforderungsprofil für die zukünftige Informationsverarbeitung in der Pflege durchzusehen und mit pflegen & wohnen zu erörtern. Folgende Zwischenergebnisse wurden erreicht:

– Das Vorhalten von Bildschirmmasken zur Erfassung von Daten, die nicht benötigt werden, birgt latent die Gefahr, daß eine nicht erforderliche und somit unbefugte Erfassung von Daten erfolgt, und sei es nur aus Unwissenheit des Anwenders. Wir haben daher empfohlen, als Maßnahme der Speicher- und Organisationskontrolle die nicht genutzten Programmteile auszublenden, so daß ihre Nutzung für die einzelnen Anwender praktisch nicht möglich ist. pflegen & wohnen hat zugesagt, dies im neuen Verfahren zu berücksichtigen. Als erste Maßnahme wurde veranlaßt, daß nur examinierte Pflegekräfte zur Eingabe der Daten berechtigt sind.

– Leseberechtigung für alle Daten, die in dem System gespeichert sind, soll jede Pflegekraft erhalten. Je nach Tätigkeitsbereich und Zuständigkeit werden dann abgestufte Berechtigungen zur Verarbeitung der Daten erteilt. Dies entspricht dem datenschutzrechtlichen Standard.

– pflegen & wohnen hat aufgrund unserer entsprechenden Hinweise jetzt eine Archivierungsfunktion vorgesehen, die eine separierte Ablage inaktueller Daten ermöglicht, auf die nur bei Bedarf nach vorheriger Aktivierung zugegriffen werden kann. Dadurch werden unkontrollierte Zugriffe auf Daten, die laufend nicht mehr benötigt werden, verhindert. Dies entbindet pflegen & wohnen jedoch nicht von der Pflicht, für eine ordnungsgemäße Löschung der Daten nach Ablauf der Aufbewahrungsfristen zu sorgen.

– Der bisherige Umfang von personenbezogenen Auflistungen ist reduziert worden, nachdem sich herausgestellt hat, daß teilweise auch aggregierte Auswertungen den angestrebten Zweck erfüllen. Die jetzt noch vorgesehenen personenbezogenen Auflistungen werden zur Aufgabenerfüllung der Pflegekräfte benötigt.

– Die Anzahl der aus fachlicher Sicht für die Pflege erforderlichen Daten ist insgesamt geringer geworden. Lediglich bei wenigen Datenfeldern hatten wir Zweifel an deren Erforderlichkeit und haben empfohlen, auf die Angaben zu verzichten oder ergänzende Erläuterungen zu geben. pflegen & wohnen hat dies zugesagt. Ansonsten konnten unsere Fragen zur Notwendigkeit einzelner Datenfelder schlüssig beantwortet werden.

– pflegen & wohnen hat sich bei der Erstellung des Datenkatalogs im wesentlichen an Vorgaben des Medizinischen Dienstes der Krankenversicherung (MDK) orientiert. Danach gibt es elf Ausprägungen der Aktivitäten des täglichen Lebens (ATL), die sozusagen in übergeordneter Weise den Grad der Unterstützung und der Pflegebedürftigkeit bestimmen und der Erstellung des Ist-Zustandes dienen. Darunter erfolgt die weitere Gliederung anhand zahlreicher Unterpunkte, die sich nach bereits realisierten Modellen und nach der Literatur definieren.

Aktivitäten des täglichen Lebens (ATL)

- ATL 1:Vitale Funktionen aufrechterhalten.
- ATL 2:Sich situativ anpassen können.
- ATL 3:Für Sicherheit sorgen können.
- ATL 4:Sich bewegen können.
- ATL 5:Sich pflegen und kleiden können.
- ATL 6:Essen und trinken können.
- ATL 7:Ausscheiden können.
- ATL 8:Sich beschäftigen können.
- ATL 9:Kommunizieren können.
- ATL 10:Ruhen und schlafen können.
- ATL 11:Soziale Bereiche des Lebens sichern können.

– Aus datenschutzrechtlicher Sicht ist bemerkenswert, daß die Angaben mit dem Betroffenen oder mit Angehörigen bzw. Betreuern gemeinsam erhoben werden sollen. Dies soll nur in den Fällen anders gehandhabt werden, in denen weder der Pflegebedürftige zur Mitwirkung in der Lage ist noch Angehörige bzw. Betreuer zur Verfügung stehen. Dann sind die Pflegekräfte befugt, die Datenfelder ohne weitere Mitwirkung auszufüllen.

– E-Mail- oder Internet-Funktionalitäten sind in diesem System nicht vorgesehen. Von daher hatten wir keine Veranlassung, unsere Hinweise zum Infrastrukturansatz durch Windows NT (vgl. 3.3) zu vertiefen.

– Über ein Fernwartungskonzept wurde noch nicht abschließend entschieden. pflegen & wohnen strebt erfreulicherweise an, die Fernwartung in jedem Fall nur ohne personenbezogene Daten zuzulassen.

Insgesamt hat sich die Angelegenheit zum Ende des Berichtszeitraumes positiv entwickelt, sodaß wir hoffen, in absehbarer Zeit eine Informationsverarbeitung in der Pflege bei pflegen & wohnen vorzufinden, die auch den datenschutzrechtlichen Anforderungen genügt.

6.8 Neukonzeption der Kindertagesbetreuung (KTB)

Die Interessen der Eltern und der Kinder sind nicht gefährdet.

Im Rahmen des Projektes Jugendamts-Automation (PROJUGA) wurde im Berichtszeitraum unter Federführung des Senatsamtes für Bezirksangelegenheiten ein neues Konzept für den Bereich Kindertagesbetreuung entwickelt. In diesem Verfahren gibt es innerhalb der Programme keine Unterscheidung mehr zwischen Kindertagesbetreuung und Tagespflege. Beide Bereiche werden gleich behandelt. Technisch handelt es sich um ein neues PROJUGA-Modul, mit dem im wesentlichen sowohl die Beitragsrechnung bei der Unterbringung in Kindertageseinrichtungen als auch die Vermittlung von Plätzen in Tageseinrichtungen geleistet werden kann. Für die Gewährung von Unterhaltsvorschüssen wird weiterhin auf das hierfür bereits vorhandene PROJUGA-Modul zurückgegriffen.

Das neue KTB-Verfahren soll langfristig zu einer Vereinfachung und Vereinheitlichung der Abläufe nach dem Teilnahmebeitragsgesetz (TnBG) und dem Kindergartenförderungsgesetz (KGFG) führen. Angestrebt wird, die Regelungen des KGFG in absehbarer Zeit im TnBG aufgehen zu lassen. Dieses scheint auch dringend erforderlich zu sein, weil bislang die Regelungslandschaft im Bereich der Tagesunterbringung für sehr verwandte Sachverhalte leider unerfreulich unübersichtlich ist. So sind neben den landesrechtlichen Bestimmungen des TnBG und des KGFG auch noch die maßgeblichen bundesrechtlichen Regelungen des SGB VIII zu beachten (§§22 ff. und §§90 ff.).

Wir haben während unserer Beteiligung an der Einführung des neuen KTB-Verfahrens Einvernehmen über Art und Umfang der Datenverarbeitung erzielen können, wobei allerdings die Diskussion über Statistik- und Steuerungsdaten breiteren Raum einnahm. In den bezirklichen Dienststellen sollen Daten aus dem KTB-Modul in anonymisierter Form an das Amt für Jugend weitergeleitet werden, um den Planungs- und Steuerungsauftrag des Amtes im Hinblick auf die Bereitstellung eines angemessenen und flächendeckenden Versorgungsangebotes an Kindergarten- und Kindertagesheimplätzen für alle Bevölkerungs- und Nachfragegruppen gewährleisten zu können. Außerdem sollen dadurch die notwendigen Ressourcen in der Haushaltsplanung und in der Mittelfristigen Aufgabenplanung bereitgestellt werden. Hiergegen bestehen aus datenschutzrechtlicher Sicht grundsätzlich keine Bedenken.

Allerdings bestand die Gefahr, daß die Anonymität nicht in jedem Fall gewährleistet werden konnte, weil die Informationen einer zu kleinen Basisgruppe entnommen werden sollten. So wurde beispielsweise zunächst daran gedacht, Baublöcke als kleinste regionale Abgrenzung vorzusehen. Aufgrund unserer Hinweise ist das Senatsamt für Bezirksangelegenheiten gemeinsam mit dem Amt für Jugend zu dem Schluß gekommen, daß der Baublock in den statistischen Daten entbehrlich ist, wenn bei der Aufbereitung dieser Daten das statistische Gebiet und der Ortsteil mitgeliefert werden. Damit wurde unseren Bedenken entsprochen.

Ein weiterer Erörterungspunkt war der Umgang mit der vorgesehenen Einführung eines bedingten Rechtsanspruchs auf eine geförderte Betreuungsleistung. Einem Kind soll dann ein solcher bedingter Rechtsanspruch eingeräumt werden, wenn beide Elternteile berufstätig sind oder sich in einer Ausbildung befinden oder das alleinerziehende Elternteil berufstätig ist oder sich in einer Ausbildung befindet. Im Rahmen des neuen Systems werden Berechtigungsscheine für Betreuungsleistungen durch die bezirklichen Jugendämter ausgegeben. Die Eltern lösen diese Leistungsberechtigung dann bei einer Tageseinrichtung ihrer Wahl ein. Der Berechtigungsschein enthält – neben Daten, die auf den früher verwendeten Bewilligungsbescheiden angegeben waren – zusätzlich die Angabe „bedingter Rechtsanspruch: ja/nein“.

Da bereits bisher der Bewilligungsbescheid mit den Angaben zum Teilnahmebeitrag der Eltern dem Träger bzw. der Tageseinrichtung vorgelegt werden mußte, ergab sich durch die Einführung des Berechtigungsscheins keine qualitative Änderung. Die gegenüber dem bisherigen Verfahren neu hinzugekommene Angabe zum bedingten Rechtsanspruch umfaßt so viele unterschiedliche denkbare Fallgestaltungen, daß es nicht ohne weiteres möglich ist, auf den ersten Blick eindeutige Informationen über die soziale bzw. berufliche Situation der Eltern bzw. Elternteile zu erhalten. Da eine Beeinträchtigung schutzwürdiger Interessen der Betroffenen insoweit nicht zu befürchten ist, kann darauf verzichtet werden, dieses Datum für den Träger bzw. die Tageseinrichtung unkenntlich zu machen.

Wir werden zum einen beobachten, wie sich das neue KTB-Modul in der Praxis bewährt. Zum anderen werden wir unter datenschutzrechtlichen Aspekten die Zusammenführung unterschiedlicher Regelungen zur Kindertagesbetreuung in Hamburg begleiten.

6.9 Sonstiges

– Zum Thema „Mehr Service – weniger Datenschutz?“ ist die bisherige Praxis der Rentenversicherungsträger, sich die Versichertendaten gegenseitig ohne Einwilligung der Versicherten zugänglich zu machen, nach Kritik der Datenschutzbeauftragten geändert worden (vgl. 16. TB, 6.1). Der Verband Deutscher Rentenversicherungsträger (VDR) hat eine EDV-technische Möglichkeit geschaffen, die den Zugriff auf Versichertendaten bei einer anderen Rentenversicherungsanstalt unterbindet. Etwaigen Widersprüchen Versicherter gegen die Einrichtung der bundesweiten Zugriffsmöglichkeit durch unzuständige Rentenversicherungsträger kann entsprochen werden. Dies ist ein wesentlicher Schritt hin zu mehr Kundenfreundlichkeit und Datenschutz.

– Im Berichtszeitraum haben wir eine Betriebskrankenkasse einer allgemeinen datenschutzrechtlichen Überprüfung unterzogen und ergänzende Einzelfragen mit dem Landesverband Nord der Betriebskrankenkassen erörtert. Dabei zeigte sich insgesamt eine große Aufgeschlossenheit gegenüber den datenschutzrechtlichen Erfordernissen. Obwohl die Prüfergebnisse bei Redaktionsschluß noch nicht abschließend behandelt waren, kann bereits jetzt festgestellt werden, daß sich kein Mitglied der Betriebskrankenkasse um die Sicherheit seiner dort gespeicherten Daten Sorgen machen muß.

7. Personaldaten

7.1 Telearbeit

Ein Modellversuch zur Erprobung alternierender Telearbeit in der hamburgischen Verwaltung hat ergeben, daß die mit dieser Arbeitsform verbundenen Risiken für den Datenschutz durchaus beherrschbar sind.

Im Oktober 1998 begann unter Federführung der Finanzbehörde ein Modellversuch zur Erprobung der alternierenden Telearbeit in der hamburgischen Verwaltung. Die daran beteiligten 13 Mitarbeiterinnen und Mitarbeiter haben die Möglichkeit, ihre Arbeit zum Teil vom häuslichen Arbeitsplatz aus zu erledigen. Mindestens 20 % der Arbeitszeit müssen jedoch auch weiterhin in der Dienststelle geleistet werden.

Die häuslichen Arbeitsplätze wurden mit ausschließlich für diesen Zweck beschafften PC ausgestattet und über ISDN mit dem Netz der hamburgischen Verwaltung verbunden. Die am Pilotversuch teilnehmenden Mitarbeiterinnen und Mitarbeiter können auf diesem Wege Dienstleistungen des Landesamtes für Informationstechnik (LIT) in Anspruch nehmen (E-Mail, Internetzugang) sowie auf die Rechner in ihren jeweiligen Behörden und Ämtern zugreifen. Durch besondere technische Sicherheitsmaßnahmen – u.a. wird für jede Verbindung ein VPN (Virtual Private Network) eingerichtet (siehe 3.11) – ist gewährleistet, daß ein Zugriff auf das Verwaltungsnetz nur über die ausgelieferten PC erfolgen kann.

Über den Modellversuch erstattet die Finanzbehörde dem Senat Anfang des Jahres 2000 einen Bericht, der Aufschluß darüber geben wird, inwieweit sich Telearbeit bewährt hat und unter welchen Voraussetzungen die hamburgische Verwaltung zukünftig alternierende Telearbeit für ihre Mitarbeiterinnen und Mitarbeiter anbieten wird. Zur Zeit finden Verhandlungen mit den Gewerkschaften über den Abschluß einer Vereinbarung nach §94 des Personalvertretungsgesetzes statt, deren Ergebnisse im Abschlußbericht mit Berücksichtigung finden sollen.

Wir sind von vornherein an diesem Projekt beteiligt worden. Einer unserer Mitarbeiter nimmt als Anwender an dem Modellversuch teil. Die hierbei gewonnenen Erfahrungen sind in ein Datenschutzkonzept eingeflossen, das die Finanzbehörde erstellt und mit uns abgestimmt hat. Es enthält verbindliche Vorgaben für die Einrichtung und Nutzung von Telearbeitsplätzen. Die in der hamburgischen Verwaltung für IuK-Anwendungen und Telekommunikation bereits vorhandenen Richtlinien und Bestimmungen gelten uneingeschränkt auch für die Telearbeit. Der Arbeitgeber/Dienstherr ist für die Einhaltung der Regelungen zur technischen und organisatorischen Datensicherung und die Gewährleistung des Datenschutzes verantwortlich. U.a. sind folgende Mindestanforderungen zu erfüllen:

• Der Telearbeitsplatz ist gegen die unbefugte Nutzung durch Dritte – wie z.B. Familienangehörige – abzusichern. Neben den üblichen Authentifizierungsverfahren darf deshalb die Speicherung sensibler personenbezogener Daten auf dem Rechner oder auf Datenträgern am Telearbeitsplatz nur verschlüsselt erfolgen. Es müssen sichere Aufbewahrungs- und Transportmöglichkeiten für Akten, Unterlagen und Datenträger vorhanden sein.

• Die Konfiguration der Anschlußkomponenten ist auf fest vorgegebenen Rechneradressen vorzunehmen. Die Kommunikation zwischen dem Telearbeitsplatz und dem Netz der Verwaltung darf nur über das Firewall-System des LIT und nur verschlüsselt erfolgen. Unberechtigte Anschlußnummern, IP-Adressen und Diensteanforderungen sind durch entsprechende Filtereinstellungen zurückzuweisen

• Die jeweilige Dienststelle hat in unregelmäßigen Abständen Überprüfungen zur Kontrolle der Datensicherheit der Telearbeitsplätze durchzuführen. Für Revisionszwecke sind abgewiesene Anmeldeversuche in entsprechenden Protokolldateien festzuhalten. Diese dürfen nicht zur Leistungskontrolle benutzt werden. Die Datensätze sind nach 3 Monaten zu löschen.

Auch dem Hamburgischen Datenschutzbeauftragten ist Gelegenheit zur datenschutzrechtlichen Überprüfung des Telearbeitsplatzes zu geben. Dies soll jedoch grundsätzlich in den Diensträumen der Behörde erfolgen, wohin der Telearbeiter die von ihm zu Hause genutzte Hard- und Software für diesen Fall zu bringen hat. Wir haben uns bereits vor Jahren in Zusammenhang mit der Verwendung privater PC durch Lehrer (11. TB, 9.2) gegen eine Prüfung in privaten Räumlichkeiten ausgesprochen.

11. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten 1992, Seite 81:

„Auf eine Regelung, die uns auch gegen den Willen der Lehrer berechtigt, in deren Privaträumen eine datenschutzrechtliche Kontrolle vorzunehmen, haben wir bewußt verzichtet. In einer Zeit, in der staatliche Stellen zunehmend bemüht sind, in die Privatsphäre der Bürger eindringen zu dürfen, halten wir es für unangebracht, ein solches Recht einem Datenschutzbeauftragten einzuräumen.“

An dieser Auffassung halten wir in Abwägung des Grundrechts auf Unverletzlichkeit der Wohnung und unseren gesetzlich geregelten Kontrollbefugnissen unverändert fest.

Trotz der Vielzahl von möglichen technisch-organisatorischen Maßnahmen darf nicht vergessen werden, daß im Zentrum aller Sicherheitsbemühungen die Mitarbeiterin bzw. der Mitarbeiter selbst stehen muß. Der verantwortliche Umgang mit Daten und Datenverarbeitungssystemen ist immer die erste Regel, um Mißbrauch und Schäden vorzubeugen. Doch dies ist kein spezielles Problem der Telearbeit, sondern der Datenverarbeitung insgesamt. Deshalb spricht aus datenschutzrechtlicher Sicht nichts gegen Telearbeit – sofern sie sicher gestaltet wird.

7.2 Neues Rechnungswesen (NERE) bei pflegen & wohnen

Bei der Prüfung des Neuen Rechnungswesens bei pflegen & wohnen haben wir Schwachstellen bei SAP R/3, dem Personalverwaltungsmodul HR und dem eingesetzten Betriebssystem Windows NT bemängelt.

Im Jahr 1999 hat der Hamburgische Datenschutzbeauftragte das Neue Rechnungswesen bei pflegen & wohnen geprüft, da der Echtbetrieb für das neue Verfahren ohne vorherige Abstimmung mit unserer Dienststelle aufgenommen wurde. Ähnliche Abstimmungsprobleme hatte es bereits bei dem Verfahren Dokumentation in der Pflege mit pflegen & wohnen gegeben (vgl. 15. TB, 6.3; 16.TB, 6.6; 17. TB, 6.7). Gegenstand der Prüfung waren das SAP R/3-Basissystem, das Modul HR sowie Windows NT als Client-Server-Plattform.

SAP R/3

Bei der Prüfung des R/3-Basissystems fielen einige SAP-spezifische Schwachstellen auf, die bei der Prüfung von SAP-Systemen immer wieder zu beobachten sind (vgl. 16. TB, 3.3). Zum einen konnte im Produktivsystem unter einer Kennung die Editierberechtigung für ABAP/4-Programme aufgerufen werden. Da über die Editierberechtigung die in den Programmen implementierten Sicherheitsmechanismen außer Kraft gesetzt werden können, wurde diese Berechtigung gelöscht. Außerdem war bei der Kennung SAPCPIC nicht das Initialpaßwort verändert worden.

Zum anderen waren den für das SAP-Verfahren zuständigen Operatoren im AK Eilbek sehr weitgehende Zugriffsrechte für die ABAP/4-Entwicklung und die Pflege von Standard-Systemprofilen eingerichtet worden. Auch externe Berater hatten Zugriff auf Produktivdaten. Pflegen & wohnen hat daraufhin die Profile für die Operatoren geändert. Den externen Beratern sollen die Berechtigungen mit Beendigung des Einführungsprozesses entzogen werden.

Zudem fiel auf, daß die für Fernwartungszwecke benötigte Remoteco-Kennung aktiviert war. Um die Gefahr zu reduzieren, daß der Fernwartungszugang von Außenstehenden mißbräuchlich genutzt wird, wurde die Kennung deaktiviert; sie wird nunmehr nur noch für Fernwartungszwecke freigeschaltet.

Modul HR

Der Infotyp Aufenthaltsstatus des Moduls HR enthält zur Verwaltung von Personaldaten ausländischer Mitarbeiter Datenfelder zum Aufenthaltsstatus, zum Ablaufdatum der Aufenthaltserlaubnis, zum Ablaufdatum der Paßgültigkeit sowie ein Bemerkungsfeld. Da diese Daten aus unserer Sicht in der vorliegenden Form nicht gespeichert werden müssen, haben wir pflegen & wohnen gebeten, den Infotyp Aufenthaltsstatus entsprechend zu überarbeiten. Daraufhin hat pflegen & wohnen mitgeteilt, daß die Felder Aufenthaltsstatus und Bemerkungen zukünftig entweder aus der Datenerfassungsmaske ausgeblendet oder zumindest gesperrt werden.

Windows NT

Sowohl auf den Servern als auch auf den Client wird Windows NT als Betriebssystem eingesetzt. Das Gesamtunternehmen pflegen & wohnen bildet eine NT-Domaine; der Primary Domain Server steht in den Räumen des Dienstleitungszentrums Informationsverarbeitung von pflegen & wohnen. Sämtliche 3 SAP-Server sind dagegen im Rechenzentrum des AK Eilbek untergebracht.

Die Client-Server-Verbindung erfolgt über das X.25-Netz der FHH. Problematisch ist jedoch, daß sämtliche Daten unverschlüsselt übertragen werden; selbst die Paßwörter werden lediglich nach einem SAP-spezifischen Algorithmus komprimiert. Pflegen & wohnen hat den Einsatz zusätzlicher Verschlüsselungssysteme aus Kostengründen abgelehnt. Eine Verschlüsselung käme nach Auskunft von pflegen & wohnen erst in Betracht, wenn das LIT als Netzbetreiber entsprechende Techniken zur Verfügung stellt.

Darüber hinaus haben wir problematisiert, daß die NT- und SAP-Paßwörter nicht synchronisiert sind und sich jeder SAP-Benutzer sowohl gegenüber dem Betriebssystem als auch gegenüber SAP authentisieren muß. Aus diesem Grund haben wir die Installation eines Single-Logon-Verfahrens mit einem eigenen Authentisierungs-Server gefordert. Pflegen & wohnen hat zugesagt, entsprechende Authentisierungsmechanismen von Windows 2000 demnächst nutzen zu wollen.

Weiterhin fiel bei der Prüfung der NT-Infrastruktur auf, daß die NT-Administratoren mit umfangreichen Zugriffsrechten auf sämtliche Bürokummunikationsdaten ausgestattet waren. Pflegen & wohnen teilt in dieser Hinsicht unsere Kritik und plant die Verschlüsselung von Server-Daten. Die Paßwörter zum Entschlüsseln der Daten sollen dann nur den Anwendern, nicht jedoch den Systemverwaltern bekannt sein.

Darüber hinaus wurde auch bei pflegen & wohnen deutlich, daß NT-Systeme meistens nicht so konfiguriert sind, wie es aus Datenschutzsicht geboten erscheint. Weder war die Administratorkennung umbenannt worden noch wurde das Dechiffrieren der Paßwortdatei durch den Einsatz des Verschlüsselungsprogramms Syskey verhindert. Die Administratorkennung wurde daraufhin von pflegen & wohnen umbenannt; der Einsatz von syskey wird geprüft.

7.3 Mitarbeiterkontrolle

7.3.1 Videoüberwachung

Aufzeichnungen mit einer verdeckten Videokamera am Arbeitsplatz sind in der Regel nicht erlaubt.

Datenschutzfragen zur Videoüberwachung (siehe im übrigen 23.) stellen sich auch bei der Mitarbeiter-Kontrolle. Immer häufiger fragen Mitarbeiter nach der Zulässigkeit von videoüberwachten Arbeitsplätzen. Durch eine Videoüberwachung wird stets in das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) des davon betroffenen Personenkreises eingegriffen. Bei der Überwachung von Mitarbeitern ist der Arbeitsvertrag maßgebend, der jedoch nicht beliebig in Grundrechte eingreifen oder diese verletzen darf. Hierzu haben die Gerichte bereits einige Grundsätze festgelegt:

• Aufzeichnungen mit einer verdeckten Videokamera am Arbeitsplatz sind nur gerechtfertigt, wenn sie die einzige Möglichkeit für den Arbeitgeber sind, sein legitimes Interesse zu wahren und weniger weitreichende Mittel nicht zur Verfügung stehen.

• Der verfolgte Zweck, beispielsweise einer Diebstahlprävention, läßt sich effektiver mit Hilfe einer offenen Videokamera erreichen.

• Die mit einer verdeckten Videokamera unzulässig erlangten Aufzeichnungen unterliegen regelmäßig einem Beweisverwertungsverbot.

• Der Personal- bzw. Betriebsrat ist zu beteiligen.

7.3.2 Kontrolle am PC

Die Protokollierung der Benutzung von Datenverarbeitungssystemen darf nicht zur Leistungs- und Verhaltenskontrolle der Beschäftigten verwendet werden.

Von vielen Mitarbeitern wird befürchtet, daß sie bei ihrer Tätigkeit am PC ständig uneingeschränkt hinsichtlich ihres Verhaltens und ihrer Leistungen elektronisch kontrolliert werden können und dürfen. Diese Annahme, die auch von einigen Vorgesetzten geteilt wird, trifft aber nicht zu.

Alle Stellen, die personenbezogene Daten automatisiert verarbeiten, sind allerdings verpflichtet, die gesetzlich erforderlichen Maßnahmen zur Datensicherung zu treffen. Danach ist zu gewährleisten, daß ausschließlich befugte Personen Zugang zu Datenverarbeitungssystemen erhalten und diese allein auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Es muß auch nachträglich überprüft und festgestellt werden können, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind. Das Datenschutzrecht sieht folglich die Protokollierung der Rechnernutzung für jeden einzelnen zugriffsberechtigten Beschäftigten vor.

Die Auswertung dieser Protokolle (An- und Abmeldezeiten am System, gelesene und veränderte Datensätze) läßt grundsätzlich auch Rückschlüsse über die Leistung und das Arbeitsverhalten jedes einzelnen Benutzers zu. Aus diesem Grunde schreiben die Datenschutzgesetze des Bundes und der Länder aber ausdrücklich vor, daß Daten der Beschäftigten, die im Rahmen der Maßnahmen zur Datensicherung gespeichert werden, nicht zu anderen Zwecken, insbesondere nicht zur Verhaltens- und Leistungskontrolle, genutzt werden dürfen.

Die Protokollierung von Benutzeraktivitäten ist also zwar rechtlich zulässig. Unternehmen und Behörden haben sich jedoch an alle Vorgaben der Datenschutzgesetze zu halten und auch die Mitbestimmungsrechte zu wahren. Die Mitarbeitervertretungen sind an Automationsverfahren zu beteiligen. In Betriebs- oder Dienstvereinbarungen ist der Einsatz von EDV, insbesondere die Auswertung von Protokollierungsdaten, im einzelnen zu regeln. Die Rechtsprechung zum Arbeitnehmerdatenschutz ist dabei zu beachten.

§28 Abs. 7 HmbDSG	**§31 BDSG**
Soweit Daten der Beschäftigten im Rahmen der Maßnahmen zur Datensicherung nach §8 Abs. 2 gespeichert werden, dürfen sie nicht zu anderen Zwecken, insbesondere nicht zu Zwecken der Verhaltens- und Leistungskontrolle, genutzt werden.	Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

7.3.3 Telefonüberwachung

Das heimliche Mithören oder Mithörenlassen durch den Arbeitgeber bei Telefongesprächen des Arbeitnehmers ist im allgemeinen unzulässig.

Immer wieder werden wir nach den datenschutzrechtlichen Aspekten beim Telefonieren gefragt. Zu den Themen Mithörenlassen von Telefongesprächen des Arbeitnehmers durch den Arbeitgeber und Automatic-Call-Distribution liegen mittlerweile Entscheidungen des Bundesarbeitsgerichtes (BAG) und Bundesgerichtshofes (BGH) vor. Das BAG ist in einem Urteil von 1997 zu dem Ergebnis gekommen, daß das heimliche Mithörenlassen durch den Arbeitgeber bei Telefongesprächen des Arbeitnehmers im allgemeinen als unzulässig angesehen wird. Wer jemanden mithören lassen will, hat seinen Gesprächspartner vorher darüber zu informieren, weil andernfalls das Persönlichkeitsrecht des Gesprächspartners verletzt wird. Der BGH hat allerdings mehrfach angenommen, daß auch bei an sich unzulässigem Mithören von Telefongesprächen über die Verwertbarkeit stets aufgrund einer Interessen- und Güterabwägung im Einzelfall zu entscheiden sei.

In diesem Zusammenhang ist auch eine Entscheidung des Bundesverfassungsgerichtes zu erwähnen. Das Gericht hat bereits 1991 ausgeführt, daß Telefongespräche, die der Arbeitnehmer von seinem Dienstapparat aus führt, nicht von vornherein aus dem Schutz durch das allgemeine Persönlichkeitsrecht ausgenommen sind. Für die Beweisverwertung hat das Gericht ebenfalls auf eine Abwägung der gegensätzlichen Interessenlage abgestellt.

Das BAG hat allerdings bei Arbeitnehmern, die in einem Call-Center arbeiten, ein Mithören zugelassen. Danach kann der Betriebsrat mit dem Arbeitgeber eine Betriebsvereinbarung dahingehend schließen, daß bei Telefongesprächen des Arbeitnehmers mit einem Kunden zu Ausbildungszwecken mitgehört werden kann.

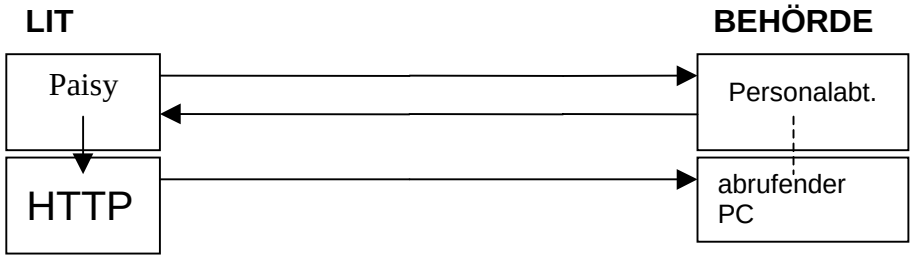
7.4 Personalcontrolling

Die datenschutzrechtlichen Fragen des Personalcontrolling sind geklärt.

Dezentrale personalwirtschaftliche Auswertungen wurden bereits ausführlich erörtert (siehe 16. TB, 7.2). Die datenschutzrechtlichen Fragen wurden nunmehr zum Abschluß des langjährigen Projektes PROPERS geklärt:

- Die **Kostenstellen** sind so zu gestalten, daß kein Rückschluß auf individuelles Verhalten und persönliche Merkmale von Mitarbeitern möglich ist.
- Die davon zu unterscheidenden **personenbezogenen Budgetdaten** dürfen für eine zweckgebundene Nutzung nach dem Erforderlichkeitsgrundsatz nur von Mitarbeiterinnen und Mitarbeiter der Personalabteilung und den nach §96 a Abs. 3 HmbBG beauftragten Personen genutzt werden. Dazu gehören auch Budgetverantwortliche, die die Behörde namentlich zu benennen hat und deren Aufgaben festzulegen sind. Andere Organisationseinheiten dürfen die Budgetdaten ausschließlich in anonymisierter Form erhalten.
- Ein weiterer wichtiger Gesichtspunkt ist die **sichere Übertragung** der personenbezogenen Budgetdaten. Das Verfahren ist so gestaltet, daß diese Daten auf einem Web-/HTTP-Server des Personalamtes im Landesamt für Informationstechnik zur Verfügung gestellt werden. Bei den Budgetdaten handelt es sich um einen Auszug aus den Paisy-Dateien, der in regelmäßigen Abständen neu erstellt wird. Ein Datensatz dieser Budgetdatei umfaßt ca. 28 Felder von ca. 1600 Feldern des Paisy-Datensatzes. Die Behörden aktivieren den Abruf, wobei jede Behörde nur auf ihre Berichtsdaten Zugriff hat.

Darstellung der Zugriffsberechtigung



Lediglich ein begrenzter Personenkreis bekommt Zugriff auf den Auswertungsserver des Personalamtes im LIT. Zu diesem Zweck erfolgt die Übermittlung verschlüsselt vom Web/HTTP-Server an einen von der Behörde bestimmten festzulegenden PC. Die IP-Adresse des abrufenden PC ist im Router beim LIT hinterlegt, um zu gewährleisten, daß der HTTP-Server nur von diesem bestimmten PC erreicht werden kann. Von dem abrufenden PC ist ein Zugriff auf die komplette Paisy-Datei nicht möglich.

- Für die Datenverarbeitung in der jeweiligen Behörde gilt:

• Die Behörde hat alle Grundschutzmaßnahmen und Vorgaben aus den allgemein verbindlichen Richtlinien bei PC´s am Arbeitsplatz einzuhalten.

• Die vom Server abgezogenen Daten dürfen nur dem berechtigten Personenkreis zugänglich sein.

• Der abrufende PC muß im Zugriff von Personen, die mit Aufgaben des Personalwesens betraut sind, stehen. Dies bedeutet, diese Person muß berechtigt sein, personenbezogene Personaldaten zu lesen.

• Werden personenbezogene Daten im Teilnetz der Behörde vom abrufenden PC zu PC´s anderer zugriffsberechtigter Personen weitergegeben, darf dies nur verschlüsselt erfolgen. Dafür bieten sich PGP oder E-Mail mit erweiterter Sicherheit im FHHInfoNet an.

7.5 Sonstiges

Weitere Themen zum Personaldatenschutz waren:

– Personalaktenführung in den Strafvollzugsanstalten

– Einführung von SAP/R3 bei verschiedenen Behörden und Landesbetrieben

– Stellenplanverfahren EPOS

– Neues Technikkonzept beim Arbeitsmedizinischen Dienst.

8. Finanzen und Steuern

8.1 Elektronischer Rechtsverkehr beim Finanzgericht

Das Finanzgericht Hamburg kommuniziert mit Steuerberatern, Anwälten und Finanzämtern auf elektronischem Wege. Die Daten werden verschlüsselt und digital signiert übertragen.

Seit dem 2. August 1999 nimmt das Finanzgericht Hamburg im Rahmen eines bundesweit einmaligen Modellversuchs von ausgewählten Steuerberatern und Rechtsanwälten Klagen und andere Schriftsätze per elektronischer Post entgegen. Diese werden von den Mitarbeiterinnen und Mitarbeitern des Finanzgerichts bearbeitet und ebenfalls per E-Mail an die betroffenen Finanzämter weitergeleitet. Die Klageerwiderungen werden auf gleichem Wege an das Gericht zurück gesandt. Durch die elektronische Kommunikation wird das gerichtliche Verfahren insgesamt rationeller und bürgerfreundlicher. Es werden vor allem aufwendige Aktentransporte vermieden und Portokosten eingespart. Es besteht eine Schnittstelle zu dem bisher schon für die Geschäftsstellen im PC-Netz des Finanzgerichts vorhandenen Automationsverfahren, so daß auch die Richter ihre Akten am Bildschirm verwalten können.

Der Modellversuch erfolgt in Zusammenarbeit mit der DATEV eG in Nürnberg. Diese stellt sowohl die zusätzlich erforderliche Hardware zur Verfügung (SmartCard, Lesegerät) als auch die Software für das Signieren und Verschlüsseln von Nachrichten zwischen dem Finanzgericht und den teilnehmenden Steuerberatern und Rechtsanwälten.

Es kommt ein hybrides Schlüsselverfahren zum Einsatz. Zunächst wird ein 56-Bit-Session- Key erzeugt, mit dem die gesamte Datei nach DES verschlüsselt wird (168-Bit sind in Vorbereitung). Der Session-Key wird anschließend auf der Chipkarte mit dem 1024-Bit-Key des Empfängers RSA-verschlüsselt und an die verschlüsselte Datei angehängt. Der Empfänger entschlüsselt auf seiner Chipkarte mit dem darauf gespeicherten Private-Key den für ihn verschlüsselten Session-Key. Der Private-Key verläßt nicht die Chipkarte.

Die Echtheit der Zertifikate kann beim Trust-Center der DATEV eG überprüft werden. Hier wird eine Datenbank mit allen am Modellversuch teilnehmenden Personen geführt, aus der ihre Public Keys abgerufen werden können.

Das Finanzgericht ist an das FHHinfoNET der hamburgischen Verwaltung (vgl. 3.1) angeschlossen. Auf dem Mail-Server im Landesamt für Informationstechnik bestehen jeweils allgemeine elektronische Postfächer für die Eingangspoststelle und die Geschäftsstellen der einzelnen Senate sowie mehr als 40 persönliche für die Mitarbeiterinnen und Mitarbeiter. Fristwahrend ist nur der Eingang von Schriftsätzen im elektronischen Postfach der Poststelle. Von hier erfolgt die Weiterleitung der Dokumente auf die zuständigen Geschäftsstellen. Für den Rechtsverkehr gelten Datum und Uhrzeit des Eingangs auf dem Mail-Server, nicht der Zeitpunkt, in dem die Nachrichten abgerufen und geöffnet werden.

Die Poststelle und die Geschäftsstellen verfügen über denselben Schlüssel, aber unterschiedliche Signaturen. Die Richter und Sachbearbeiter haben jeweils eigene, individuelle Schlüssel. Die elektronische Kommunikation zwischen dem Finanzgericht und den Finanzämtern in Hamburg erfolgt über die Signatur und Verschlüsselung im FHHinfoNET und nicht über die Hard- und Software der DATEV eG.

Das Finanzgericht hat uns frühzeitig und umfassend über den Modellversuch unterrichtet. Aus datenschutzrechtlicher Sicht bestehen keine Bedenken. Unter der Voraussetzung, daß die PC bei allen Prozeßbeteiligten dem Stand der Technik entsprechend gegen den Zugriff Unbefugter abgeschottet werden, halten wir das Verfahren für hinreichend sicher.

Die elektronische Übermittlung von Klagen und Schriftsätzen führt zur Zeit aber noch zu rechtlichen Schwierigkeiten. Bislang ist gesetzlich immer noch eine handschriftliche Unterzeichnung erforderlich. Sie ist Bedingung für die Zulässigkeit der Klage. Für die Einreichung per Fax haben Bundesverwaltungsgericht, Bundessozialgericht und Bundesfinanzhof bereits Ausnahmen zugelassen. Der Bundesgerichtshof besteht aber für die Klageerhebung per PC noch auf einer verbindlichen Korrektur durch den Gesetzgeber. Bis zur einer endgültigen Klarstellung muß deshalb zur Zeit noch zusätzlich zur elektronischen Übermittlung eines Schriftsatzes ein handschriftlich unterzeichneter Ausdruck eingereicht werden.

8.2 Projekt ELSTER (Elektronische Steuererklärung)

Auch in Hamburg können Steuerzahler ihre Steuererklärung jetzt auf elektronischem Wege einreichen. Der Schutz des Steuergeheimnisses wird dabei ausreichend gewahrt. Die getroffenen Sicherheitsmaßnahmen entsprechen dem Stand der Technik.

Seit Anfang 1999 ist es in Deutschland möglich, Steuererklärungen elektronisch abzugeben. Jeder Steuerzahler, der über einen Internetanschluß verfügt, kann seine Steuerdaten online an das Finanzamt schicken. Einzige Voraussetzungen sind ein im Handel erhältliches Steuerberatungs- und -berechnungsprogramm, das das „ELSTER“-Verfahren (ELektronische STeuerERklärung) unterstützt, und die Teilnahme des für den Steuerzahler zuständigen Finanzamts am bundesweiten Online-Verfahren. Mit Stand vom 01. Dezember 1999 sind bereits 15 Bundesländer angeschlossen, davon zwei aber noch nicht mit allen Finanzämtern.

ELSTER ist ein eigenes Projekt der deutschen Steuerverwaltung, das die elektronische Übermittlung von Steuererklärungen und Voranmeldungen zum Ziel hat. Neben den Steuerberatern erstellen immer mehr Bürger ihre Steuererklärungen am PC. Bei dieser Gelegenheit werden die Daten für die Steuererklärungsformulare bereits in elektronischer Form erfaßt. Diese können nunmehr ohne Medienbruch auch von der Steuerverwaltung genutzt werden. Zur Wahrung des Steuergeheimnisses werden die Daten verschlüsselt in die Rechenzentren der jeweiligen Bundesländer übertragen. Zum Einsatz kommt eine hybride Verschlüsselung, d. h. es werden insgesamt drei Schlüssel erforderlich (ein 3-DES-Key mit 112 Bit Länge und ein RSA-Schlüsselpaar mit 1024 Bit Länge). Der Public-Key und das Verschlüsselungsverfahren sind Bestandteil eines Programmoduls, das die Steuerverwaltung den Herstellern von Steuersoftware zur Integration in deren Produkte kostenlos zur Verfügung stellt. Der zugehörige Private-Key ist für jedes Rechenzentrum verschieden und nur der Steuerverwaltung selbst bekannt. Die Unversehrtheit der Daten wird darüberhinaus durch einen Hash-Algorithmus gewährleistet. Auch die Herkunft der Daten aus dem ELSTER-Programm kann überprüft werden. Um den Umfang der Übertragung zu reduzieren, werden die Daten vor der Verschlüsselung und Signatur komprimiert, d.h. es werden nach Reihenfolge und Inhalt des amtlichen Vordrucks nur die Zeilen übermittelt, die tatsächlich ausgefüllt wurden.

Die Daten werden an einen im Programmodul fest vorgegebenen Rechner übertragen, der bundesweit als zentrale Annahme- und Verteilstelle fungiert. Auf diesem Rechner erfolgt nur eine Integritäts- und Authentizitätsprüfung der eingegangenen Daten, aber keine Entschlüsselung. Dies geschieht erst nach Übernahme anhand der mit übertragenen Landes- und Finanzamtskennungen in den Rechenzentren der einzelnen Bundesländer. Aus Sicherheitsgründen erfolgt die Verteilung vom zentralen Annahmerechner an die zuständigen Finanzämter über separate PC, die keine physikalischen Verbindungen zu anderen Rechnern der Steuerverwaltung haben dürfen.

Auf die Unterschrift des Steuerzahlers kann nach derzeitiger Rechtslage noch nicht verzichtet werden. Deshalb muß eine komprimierte Steuererklärung unterschrieben und zusammen mit den Belegen und der Lohnsteuerkarte an das Finanzamt geschickt werden. Der Ausdruck der Erklärung erfolgt automatisch nach erfolgreicher Datenübertragung. Enthalten ist darin auch eine eindeutige Telenummer, die bei jeder Übertragung neu gebildet wird. Bei mehrfacher oder irrtümlicher Datenübermittlung ist somit immer feststellbar, welche Steuererklärung gültig sein soll. Ohne die Telenummer kann und darf das Finanzamt gesendete Daten nicht abrufen.

Für die Steuerverwaltung vermindert sich durch die elektronische Datenübermittlung der Aufwand für die Datenerfassung. Der Bürger erhält höhere Sicherheit, daß seine sachlich richtigen Angaben beim Finanzamt auch zutreffend als Eingabewert übernommen werden.

8.3 Bereichsspezifische Regelungen in der Abgabenordnung

Eine gesetzliche Normierung der Auskunfts- und Einsichtsrechte von betroffenen Steuerpflichtigen in der Abgabenordnung wird als unverzichtbar angesehen.

Seit längerem setzen wir uns dafür ein, daß von der Steuerverwaltung die Auskunfts- und Einsichtsrechte der Steuerpflichtigen anerkannt werden. Ein negatives Beispiel war im Jahr 1998, daß das Bundesamt für Finanzen (BfF) den Auftraggebern von Freistellungsaufträgen aufgrund eines Erlasses des Bundesministeriums für Finanzen (BMF) die Auskünfte über ihre dort gespeicherten Daten verweigerte. Der Bundesbeauftragte für den Datenschutz verlangte daraufhin unter Hinweis auf die Verletzung des datenschutzrechtlichen Auskunftsanspruchs, daß das BMF den Erlaß aufhebt.

Das BMF hat zwischenzeitlich in einem neuen Erlaß geregelt, daß das BfF nunmehr den Freistellungsauftraggebern „nach pflichtgemäßen Ermessen“ Auskünfte über deren Daten zu erteilen hat, soweit der Freistellungsauftraggeber hierfür ein berechtigtes Interesse darlegt oder dies ohne weitere Ermittlungen ersichtlich ist und keine Versagungsgründe vorliegen. Die Versagungsgründe (z.B. überwiegende schutzwürdige Interessen Dritter) sind in dem Erlaß aufgeführt.

Mit dieser Regelung wird dem Anliegen der Betroffenen auf Auskunft in der Praxis zwar weitgehend entsprochen. Dem gesetzlichen Auskunftsanspruch gemäß den Datenschutzgesetzen des Bundes und der Länder über die – vor allem in automatisierten Daten – zur eigenen Person gespeicherten Daten wird die Regelung aber nicht gerecht, wenn die Auskunft lediglich in das Ermessen der Finanzbehörden gestellt wird.

Wir haben dies zum Anlaß genommen, die hamburgische Steuerverwaltung auf die fehlende bereichsspezifische Normierung des Auskunfts- und Einsichtsrechts in der Abgabenordnung (AO) hinzuweisen. Die für die AO zuständigen Referatsleiter des Bundes und der Länder gehen jedoch bisher davon aus, daß die AO das Gebiet der Auskunfts- und Einsichtsrechte abschließend regelt und verweisen in diesem Zusammenhang insbesondere auf die Bestimmungen des §30 AO.

Diese Bestimmungen regeln aber nur die Offenbarung der dem Steuergeheimnis unterliegenden Daten gegenüber Dritten, nicht aber gegenüber dem betroffenen Steuerpflichtigen selbst. Eigene Auskunfts- und Einsichtsrechte werden daher durch §30 AO in keiner Weise geregelt. Dies geht auch aus einem Urteil des Finanzgerichts Köln vom 18. Dezember 1997 (2 K 382/96) hervor. Auch die §§91 und 364 AO regeln nicht die Auskunft oder die Akteneinsicht des Betroffenen, sondern verbürgen den Grundsatz des rechtlichen Gehörs im steuerrechtlichen Verwaltungsverfahren.

Zudem sieht auch Art. 12 der EG-Datenschutzrichtlinie ein weitgehend uneingeschränktes Auskunftsrecht der Betroffenen vor. Art. 12 EG-Datenschutzrichtlinie macht auch für den Finanzbereich keine Ausnahme vom Auskunftsrecht. Eine entsprechende Normierung in der AO ist auch vor diesem Hintergrund angezeigt.

Da es folglich keine bereichsspezifischen Normen in der AO über Auskunft und Akteneinsicht gibt, haben wir gegenüber der Steuerverwaltung deutlich gemacht, daß dann die entsprechenden Vorschriften der Datenschutzgesetze des Bundes und der Länder neben der AO anzuwenden sind. Für den Bereich der hamburgischen Finanzämter sind dies insbesondere die Vorschriften der §§18 und 19 des Hamburgischen Datenschutzgesetzes (HmbDSG). Ihnen kommt insoweit eine lückenausfüllende Funktion zu.

Aus Gründen der Rechtssicherheit erscheint es uns unabhängig von der ergänzenden Anwendung der Landesdatenschutzgesetze insbesondere hinsichtlich der eigenen Auskunft- und Einsichtsrechte aber sinnvoll, eine bundesweit abgestimmte Regelung anzustreben.

Wir haben deshalb im Oktober 1999 die Steuerverwaltung schriftlich gebeten, unsere Forderung hinsichtlich einer gesetzlichen Nomierung der Auskunftsrechte bei der im Dezember stattfindenden Sitzung der für die AO zuständigen Referatsleiter des Bundes und der Länder zu berücksichtigen. Die Steuerverwaltung hat unsere Forderungen dem BMF und den obersten Finanzbehörden der Länder zwecks Erörterung bei der nächsten Sitzung der AO-Referenten zugeleitet. Da uns bis Redaktionsschluß noch kein Besprechungsergebnis vorlag, werden wir über den Fortgang weiter berichten.

9. Schule und Berufsbildung

9.1 Projekt Technikunterstützung im Verwaltungsbereich der allgemeinbildenden Schulen (TUVAS)

Bei der Einführung moderner IuK-Technik in der Schulverwaltung sind die gesetzlichen Vorgaben zum Schuldatenschutz zu beachten.

Im Berichtszeitraum sind wir von der Behörde für Schule, Jugend und Berufsbildung an der Entwicklung des Projektes TUVAS beteiligt worden. Mit diesem IuK-Vorhaben sollen die Schulbüros der rund 380 allgemeinbildenden Schulen mit einheitlicher Hard- und Software ausgestattet werden, um die Leistungsfähigkeit dieser Schulen bei den vielfältigen Planungs- und Steuerungsaufgaben in der Schulverwaltung zu unterstützen und zu fördern. Mit TUVAS werden insbesondere folgende Ziele verfolgt:

• Optimierung der Verwaltungsabläufe in Schulen mit Arbeitsentlastungen für Schulbüros und Pädagogen,

• Verbesserung der Kostentransparenz und der Wahrnehmung der Budgetverantwortung in Schulen – beispielsweise im Zusammenhang mit der Übernahme der äußeren Schulverwaltung,

• Effizientere Planung und Steuerung des Schulwesens durch die Fachbehörde aufgrund verbesserter Datengrundlagen,

• Reduzierung der Personalausgaben in einer zentralen Verwaltungseinheit durch Vereinfachung der Rechnungsbearbeitung,

• Verbesserte Auskunftsfähigkeit in Schulen durch einen modernen Standard der Bürokommunikation und Einbindung in das hamburgweite TK-Netz.

Die IuK-Unterstützung im Bereich der Schulverwaltung umfasst das Schulsekretariat, die Schulleitung sowie die mit Planungsaufgaben beauftragten Lehrerinnen und Lehrer wie beispielsweise Koordinatorinnen und Koordinatoren oder Sammlungsleiterinnen und Sammlungsleiter. Die Erfassung und Pflege von Schüler- und Lehrerdaten erfolgt im Schulsekretariat. Dort werden Formulare wie Schulbescheinigungen, Zeugnisse oder Rentenbescheinigungen und Listen wie beispielsweise Klassen-, Kurs- oder Gremienlisten erstellt, die an Lehrerinnen und Lehrer, Schülerinnen und Schüler und Eltern verteilt werden. Außerdem wird die Korrespondenz mit Schülerinnen und Schülern, Lehrerinnen und Lehrern, der Behörde oder Lieferanten erledigt.

Die Schulleitung und die Koordinatorinnen und Koordinatoren benötigen Schüler- und Lehrerdaten beispielsweise für die Stundenplanung, die Klassen- und Kurszusammensetzungen oder die Lehrerbedarfsermittlungen.

Im Rahmen unserer Beteiligung an dem Projekt haben wir deutlich gemacht, daß sich Art und Umfang der Verarbeitung personenbezogener Daten von Schülerinnen und Schülern und deren Erziehungsberechtigten nach §1 der Verordnung über die Verarbeitung personenbezogener Daten in den Schulen (Schul-Datenschutzverordnung) vom 1. Juli 1997 zu richten hat. Sofern weitergehende Daten verarbeitet werden sollen, darf dies nur mit Einwilligung der Betroffenen erfolgen. Auch die ansonsten in der Schul-Datenschutzverordnung getroffenen Regelungen über das Recht auf Auskunft und Einsicht in die Unterlagen, über die Sicherung personenbezogener Daten und über die Aufbewahrungsfristen sind zu beachten.

TUVAS soll technisch als Client/Server-Anwendung unter dem Netzwerkbetriebssystem Windows NT realisiert werden. Auf der Grundlage unserer Analyse der Sicherheitsfunktionalitäten dieses Systems aus dem Jahre 1996 (vgl. 16. TB, 3.1) haben wir der Projektleitung die entsprechenden Hinweise gegeben, damit Schwachstellen beachtet und ggf. kompensiert werden können. Auch hinsichtlich des vorgesehenen Softwareproduktes – einer Entwicklung aus dem hessischen Schulbereich – sind wir zum Ende des Berichtszeitraumes von der Behörde für Schule, Jugend und Berufsbildung beteiligt worden. Die Gespräche über das Produkt unter datenschutzrechtlichen Gesichtspunkten dauern noch an.

Der Zeitplan für die weitere Entwicklung des Projektes sieht vor, Anfang des Jahres 2000 in die Pilotphase einzusteigen. Die Aufnahme des Echtbetriebes ist für den Herbst des Jahres 2000 vorgesehen.

9.2 Chipkarte für Studierende an der Universität Hamburg (UniHamburgCard)

Noch fehlt eine Rechtsgrundlage für die Karte.

Die Universität Hamburg hat sich im Laufe des Jahres 1999 entschieden, in Zusammenarbeit mit der Hamburger Sparkasse (Haspa) ab dem Wintersemester 1999/2000 als erste Hamburger Hochschule einen chipkartenbasierten Studierendenausweis einzuführen. Wir hatten von Anfang an Gelegenheit, die erforderlichen datenschutzrechtlichen Hinweise zu geben.

Bei der Chipkarte handelt es sich um eine kontoungebundene GeldKarte. Sie wird mit dem Bild und dem Namen des Studierenden versehen.

Die UniHamburgCard ist:

- Studierendenausweis
- Semesterticket für den Hamburger Verkehrsverbund
- Bibliotheksausweis für alle Bibliotheken der Universität Hamburg
- Kontoungebundene elektronische Geldbörse (es muß kein Konto bei der Haspa geführt werden)

Mit der UniHamburgCard kann bereits folgendes erledigt werden:

- Semesterrückmeldung mit sofortigem Ausdruck der Bescheinigungen (Studienbescheinigungen, BAföG-Bescheinigungen und Überweisungs-/Einzahlungsvordrucke), sofern die Semestergebühr bezahlt ist
- in den Bibliotheken Bücher entleihen und Gebühren bezahlen
- den Hamburger Verkehrsverbund im Gesamtnetz nutzen
- an den SB-Stationen die im Chip und im Studentenverwaltungsverfahren gespeicherten personenbezogenen Daten ansehen
- mit der GeldKarte innerhalb und außerhalb der Universität Zahlungsvorgänge abwickeln

Mit der UniHamburgCard kann in Kürze folgendes erledigt werden:

- einen Internetzugang beim Rechenzentrum der Universität beantragen
- an den SB-Stationen die Semestergebühren bezahlen
- in den Mensen des Studentenwerks Hamburg das Essen bezahlen

Das einzige personenbezogene Datum auf dem Chip ist die Matrikelnummer des Studierenden. Neben einigen allgemeinen Daten, wie z.B. Chipkartennummer und Hochschulnummer, und Daten zur technischen Kartenverwaltung werden im Chip die erforderlichen technischen Bedingungen gesetzt, um die elektronische Geldbörse zu nutzen. Ob sich der Studierende über Ladeterminals seiner oder einer anderen Bank – oder überhaupt – Geld in die elektronische Geldbörse lädt, steht ihm völlig frei.

Beim erstmaligen Benutzen einer Kartenfunktion an der SB-Station muß der Studierende eine 4-stellige PIN-Nummer eingeben. Bei falscher PIN-Eingabe wird die Karte gesperrt und kann anschließend vom Studierenden nur im Studentensekretariat entsperrt werden. Um bei Verlust einen Mißbrauch zu verhindern, kann die Karte im Studentensekretariat gesperrt werden.

Die Ausgabe der UniHamburgCard erfolgt nur an solche Studentinnen und Studenten, die damit auch einverstanden sind. Grundlage hierfür ist ein Informationsblatt mit einer separaten Einwilligungserklärung. Beide Formulare sind mit uns abgestimmt worden.

Mit der Ausgabe der Karte zum Wintersemester 1999/2000 auf freiwilliger Basis soll zunächst erprobt werden, wie die Karte akzeptiert wird und wie sie sich im Universitätsbetrieb bewährt. Die Universität rechnet damit, daß sich etwa 4000 Studierende für die Chipkarte entscheiden werden. Für die Dauer der Erprobungsphase haben wir uns damit einverstanden erklärt, daß auf die Schaffung einer – in Hamburg bislang nicht vorhandenen – universitären Rechtsgrundlage mit den datenschutzrechtlichen Festlegungen verzichtet werden kann, weil die Studierenden in die Ausgabe der Chipkarte wirksam eingewilligt haben und eine Wahlmöglichkeit zwischen dem alten und dem neuen Verfahren besteht. Wer lieber auf die UniHamburgCard verzichten möchte, muß mit keinerlei Benachteiligungen im Universitätsbetrieb rechnen.

Die Universität hat akzeptiert, daß eine universitäre Rechtsgrundlage für die UniHamburgCard spätestens dann erforderlich wird, wenn die Kartenausgabe nicht mehr auf freiwilliger Basis geschieht. Das zu entwickelnde Regelungswerk soll zu gegebener Zeit mit uns erörtert werden.

9.3 Mitteilung von Prüfungsergebnissen an die Ausbildungsbetriebe

Ausbildungsbetriebe müssen ausdrücklich verlangen, daß sie über Prüfungsergebnisse ihrer Auszubildenden unterrichtet werden wollen.

Bis vor zwei Jahren wurden Prüfungsergebnisse der Auszubildenden durch die Handelskammer Hamburg den Ausbildungsbetrieben mitgeteilt, sofern zuvor eine Einwilligung der Auszubildenden dafür eingeholt worden war. Dieses Verfahren basierte auf einer Verabredung mit uns aus dem Jahre 1995, nachdem wir festgestellt hatten, daß eine Einwilligung bisher nicht eingeholt wurde (vgl. 14. TB, 7.1). Im wesentlichen mußte diese Regelung seinerzeit getroffen werden, weil für eine solche Mitteilung eine Rechtsgrundlage fehlte. Dieses ist zwischenzeitlich durch eine Änderung des Berufsbildungsgesetzes nachgeholt worden, die mit Wirkung vom 25. März 1998 in Kraft getreten ist.

§41 Satz 3 Berufsbildungsgesetz (BBiG)

„Dem Ausbildenden werden auf dessen Verlangen die Ergebnisse der Zwischen- und Abschlussprüfung des Auszubildenden mitgeteilt."

Das Berufsbildungsgesetz enthält somit eine ausdrückliche Ermächtigung zur Weitergabe sämtlicher Prüfungsergebnisse aus Ausbildungsverhältnissen. Damit ist allerdings noch nicht eine regelmäßige Weitergabe von Prüfungsergebnissen an die Ausbildungsbetriebe zulässig. Vielmehr enthält die neu eingefügte Regelung ausdrücklich den Vorbehalt, daß der Ausbildungsbetrieb die Mitteilung verlangt haben muß. Es darf somit nicht einfach unterstellt werden – wie die Handelskammer zunächst annahm –, daß bei der überwiegenden Mehrheit der Ausbildungsbetriebe der Wunsch nach Übermittlung der Daten besteht.

Der Gesetzgeber hat durch die gewählte Regelung sprachlich deutlich gemacht, daß die Übermittlung der Daten gerade abhängig gemacht werden soll vom Verlauf der Ausbildung. In den Fällen, in denen steuernd in die Ausbildung eingegriffen und der Auszubildende an das Prüfungsziel herangeführt werden soll, soll der Ausbildungsstand anhand der Prüfungsergebnisse nachvollzogen werden können. Dies ist jedoch keine Rechtfertigung dafür, auch in den weit überwiegenden Fällen, in denen kein Bedarf für einen steuernden Eingriff in die Ausbildung besteht, ebenfalls die Prüfungsergebnisse an die Ausbildungsbetriebe weiterzuleiten. Vielmehr entsteht dadurch die Gefahr, daß bei den Ausbildungsbetrieben Daten auf Vorrat gespeichert werden, von denen völlig unklar ist, ob sie jemals im Einzelfall benötigt werden. Dies widerspricht den datenschutzrechtlichen Grundsätzen, wonach sich die Übermittlung von Daten streng an der Erforderlichkeit zu orientieren hat.

Die Handelskammer teilt inzwischen diese Auffassung und hat deshalb auf dem Formblatt, mit dem die Ausbildungsbetriebe den Antrag auf Eintragung des Ausbildungsvertrages in das Verzeichnis der Berufsausbildungsverträge stellen, einen auf §41 Satz 3 BBiG bezogenen Passus aufgenommen. Die Ausbildungsbetriebe können damit zum Ausdruck bringen, ob sie an der Übermittlung der Ergebnisse der Zwischen- und Abschlussprüfung des Auszubildenden ein Interesse haben oder nicht.

10. Bauen, Wohnen und Stadtentwicklung

10.1 Planfeststellungsverfahren für die Magnetschnellbahn Berlin – Hamburg

Zum Planfeststellungsverfahren für den Bau der Magnetschnellbahn (Transrapid), die zwischen Berlin und Hamburg verkehren soll, waren auch datenschutzrechtliche Fragen zu klären. Es konnte eine datenschutzgerechte Ausgestaltung des Verfahrens erreicht werden.

Die Durchführung des Planfeststellungsverfahrens ist wie folgt geregelt:

Planfeststellungsbehörde für das gesamte Verfahren ist nach §5 des Magnetschwebebahnplanungsgesetzes das Eisenbahn-Bundesamt. Die Durchführung der einzelnen Planfeststellungsverfahren obliegt den jeweiligen Landesbehörden. Die gesamte Strecke wurde in einzelne Planfeststellungsabschnitte unterteilt, wobei der Streckenverlauf durch verschiedene Bundesländer führt. Davon lagen drei Abschnitte auf Hamburger Gebiet. In Hamburg ist für die Durchführung des Planfeststellungsverfahrens für diese drei Streckenabschnitte die Baubehörde verantwortlich. Sie nimmt als Anhörungsbehörde nach Auslegung der Pläne Einwendungen gegen diese Pläne von privater Seite entgegen und führt den Erörterungstermin durch. Danach ergeht vom Eisenbahn-Bundesamt der Planfeststellungsbeschluß.

Datenschutzrechtliche Fragen ergaben sich zu folgender Besonderheit bei der Durchführung des Planfeststellungsverfahrens: Die Einwendungen von privater Seite sollten von der Baubehörde als Anhörungsbehörde gescannt und über E-Mail an die Vorhabensträgerin, die Magnetschnellbahn-Planungsgesellschaft (MSP) mit Sitz in Schwerin und Berlin übermittelt werden, damit diese zur Vorbereitung des Erörterungstermins eine Stellungnahme abgeben konnte.

Dieselben Verfahrensabläufe sollten zur Durchführung des Planfeststellungsverfahrens für den Bau des Transrapids auch in den Bundesländern Schleswig-Holstein, Mecklenburg-Vorpommern, Brandenburg und Berlin durchgeführt werden. Um ein einheitliches Datenschutzniveau in allen am Planfeststellungsverfahren beteiligten Bundesländern zu gewährleisten, wurden zwischen den Datenschutzbeauftragten der beteiligten Bundesländer sowie dem Datenschutzbeauftragten des Eisenbahn-Bundesamtes als Planfeststellungsbehörde gemeinsam die datenschutzrechtlichen Aspekte des Planfeststellungsverfahrens erörtert.

Datenschutzrechtlich wurde das Verfahren wie folgt bewertet:

Die vorgesehene Übermittlung der Einwendungen an die Vorhabensträgerin MSP ist zulässig, soweit sie zur fachgerechten Vorbereitung ihrer Stellungnahme auch die konkret betroffenen individuellen Belange der Einwenderinnen und Einwender kennen muß. Eine Übermittlung personenbezogener Daten von Einwenderinnen und Einwendern an die Vorhabensträgerin ist dagegen unzulässig, wenn sie die personenbezogenen Daten der Einwenderinnen und Einwender nicht kennen muß, z.B. weil diese nur aufgrund allgemeiner Erwägungen Einwendungen gegen das Projekt erheben. Aus Transparenzgründen ist es zudem erforderlich, daß die Anhörungsbehörde bereits bei Auslegung der Pläne darauf hinweist, daß die Einwendungen an die Vorhabensträgerin weitergeleitet werden.

Ferner wurde von den Datenschutzbeauftragten gefordert, daß die Datenübermittlung zwischen der Anhörungsbehörde und der Vorhabensträgerin sicher erfolgen müsse. Dies bedeutet, daß eine Verschlüsselung der Daten mit einem ausreichenden Verschlüsselungsalgorhythmus erfolgen muß.

Die Baubehörde sagte die Erfüllung sämtlicher Punkte zu. Die Ankündigung zur Durchführung des Planfeststellungsverfahrens im Amtlichen Anzeiger enthielt einen Hinweis darauf, daß Einwendungen von privater Seite an die Vorhabensträgerin übermittelt werden würden. Personenbezogene Angaben in Eingaben, deren Kenntnis für die Vorhabensträgerin nicht erforderlich war, wurden vor der Übermittlung an diese geschwärzt. Bei der Durchführung des Planfeststellungsverfahrens zeigte sich dann jedoch, daß die ganz überwiegende Zahl der Einwenderinnen und Einwender Belange geltend machte, deren Kenntnis für die Vorhabensträgerin zur Fertigung ihrer Stellungnahme erforderlich war. So waren unter insgesamt 609 Einwendungen nur zwei sogenannte „Pauschal-Einwendungen“, bei denen die Kenntnis der personenbezogenen Daten der Einwenderinnen und Einwender durch die Vorhabensträgerin nicht erforderlich war.

Von der Vorhabensträgerin MSP wurde aufgrund der Forderungen der Datenschutzbeauftragten der Länder eine ausreichende Verschlüsselung der per E-Mail übermittelten Daten von den Anhörungsbehörden an die Vorhabensträgerin realisiert.

Als Resultat ist festzustellen, daß eine datenschutzgerechte Ausgestaltung des Planfeststellungsverfahrens für den Bau der Magnetschnellbahn zwischen Hamburg und Berlin erreicht werden konnte.

11. Ausländerangelegenheiten

11.1 Öffentlichkeitsarbeit der Ausländerbehörde

Die Ausländerbehörde reagierte auf Zeitungsberichte mit persönlichen Ausländerdaten, indem sie in einer Pressemitteilung zusätzliche personenbezogene Daten veröffentlichte. Dies gab Anlaß zur Klärung des Verhältnisses zwischen dem Datenschutz und dem Interesse der Behörde, sich mit personenbezogenen Ausländerdaten gegen unwahre Berichterstattungen zu wehren.

11.1.1 Der Ausgangsfall

Im September 1999 veröffentlichten die taz und die Hamburger Morgenpost einen Artikel über eine ghanaische Frau und ihre Tochter. Die seit 13 Jahren in Hamburg lebende Ausländerin hatte über eine Flüchtlingsberatungsstelle eine Petition eingereicht, um in einer Einzelfallprüfung als sog. Altfall eine drohende Abschiebung zu vermeiden. Die taz zitierte die Beratungsstelle mit der Feststellung, die Voraussetzungen einer geplanten Altfallregelung seien erfüllt, sowie mit der Kritik, die SachbearbeiterInnen der Ausländerbehörde hätten die Koalititionsvereinbarung nicht im Blick, so daß man in jedem einzelnen Fall darauf pochen müsse.

Die Hamburger Morgenpost hatte die Namen und das Alter der Ausländerinnen genannt und mitgeteilt, daß die Ghanaerin mit ihrem Ehemann eingereist sei, von dem sie inzwischen geschieden wurde. Die Ausländerin habe einen Teilzeitjob und bewohne mit ihrer in Hamburg geborenen Tochter eine kleine Wohnung. Weitere persönliche Angaben machte auch die taz nicht. Die Ausländerbehörde veröffentlichte daraufhin ihrerseits eine Presseerklärung unter dem Titel „Nicht jeder Fall ist ein Altfall“. Darin stellt sie fest, daß die Ghanaerin illegal eingereist sei, erst 3 Jahre später einen Deutschen geheiratet habe und 1993 durch wahrheitswidrige Angaben eine Verlängerung der Aufenthaltserlaubnis erschlichen hätte. Durch das Scheidungsverfahren sei offenbar geworden, daß es sich zumindest seit 1993 um eine Scheinehe gehandelt habe und die Tochter nicht vom deutschen Ehemann abstamme. Das Verwaltungsgericht habe 1999 nach einer detaillierten Einzelfallprüfung die weitere Verlängerung der Aufenthaltserlaubnis versagt. Ferner nennt die Presseerklärung einzelne Voraussetzungen für „die zu erwartende Altfallregelung“, die im vorliegenden Fall nicht erfüllt seien. Sie schließt mit dem Hinweis: „Daß die Mitarbeiter der Ausländerbehörde sich angeblich weder an geltendes Recht noch an Absprachen zwischen den Koalitionspartnern halten würden, ist eine immer wiederkehrende falsche Behauptung, die damit nicht richtiger wird.“

11.1.2 Datenschutz und behördliches Selbstverteidigungsrecht

In einem Schreiben an die Ausländerbehörde wandten wir uns gegen die Veröffentlichung zusätzlicher personenbezogener Daten aus der Ausländerakte. Wir schlugen vor, unwahre Pressedarstellungen ggf. zwar als unrichtig zu kritisieren, aber auf eine Offenbarung der richtigen personenbezogenen Daten grundsätzlich zu verzichten. Dies führte Anfang November 1999 zu einem Gespräch mit der Behörde für Inneres, die sich in ihren Möglichkeiten zur öffentlichen Verteidigung ihrer Position zu stark eingeschränkt sah.

Wir machten deutlich, daß es bislang an einer normenklaren Erlaubnis für eine aktive, also „ungefragte“ Öffentlichkeitsarbeit mit personenbezogenen Daten fehlt. Für das Auskunftsrecht der Presse sowie in besonderen Rechtsverhältnissen (Sozialdatenschutz, Abgabenrecht und parlamentarische Anfragen) fordert das Gesetz jeweils eine Abwägung zwischen dem Persönlichkeitsrecht des Betroffenen und dem Richtigstellungsinteresse der Behörde. Dies würde auch gelten für eine Ergänzung des Presserechts um eine Regelung für eine aktive Öffentlichkeitsarbeit von Behörden.

Als inhaltliche Kriterien für diese Abwägung trugen wir die folgenden Fragestellungen vor, die wir den spezialgesetzlichen Regelungen und ihren Kommentierungen in der Literatur entnahmen: Handelte es sich um eine unwahre Tatsachenbehauptung und nicht nur um eine Meinungsäußerung? Ist sie in wesentlichen Punkten unwahr? Ist die Falschmeldung geeignet, den Ruf der kritisierten Behörde erheblich zu beeinträchtigen, ist der Vorwurf also von Gewicht? Ist die Richtigstellung durch die Offenbarung personenbezogener Daten Betroffener geeignet und notwendig, um der Rufschädigung entgegenzuwirken?

Wir vereinbarten mit der Behörde für Inneres, an einer Leitlinie für die Öffentlichkeitsarbeit der Behörde mit personenbezogenen Daten mitzuwirken. Sie soll das Grundrecht auf informationelle Selbstbestimmung und das rechtsstaatliche Interesse am Ruf der Behörde als rechtmäßig handelnder Verwaltung zu einer „praktischen Konkordanz“ führen. Dabei ist auch zu berücksichtigen, inwieweit bereits die Pseudonymisierung von Betroffenen-Namen in der behördlichen Veröffentlichung den Anforderungen des Datenschutzes gerecht wird.

Die Anwendung der genannten Abwägungskriterien auf den Ausgangsfall hätte nach unserer Auffassung die Veröffentlichung der personenbezogenen Daten auch dann nicht rechtferigen können, wenn sie auf eine Anfrage nach §4 Abs. 2 Pressegesetz erfolgt wäre. Die einzige unwahre Tatsachenbehauptung lag in der Mitteilung, die Ausländerin sei zusammen mit ihrem Ehemann eingereist. Da die Zeitungsberichte erkennbar nur die Dauer des Aufenthalts und die Geburt der Tochter in Hamburg für eine humanitäre Einzelfalllösung als Altfall heranzogen, ist diese unwahre Tatsachenbehauptung nicht entscheidend. Die von der Presse zitierte Kritik der Beratungsstelle ist als Meinungsäußerung zu werten und unterstellt der Ausländerbehörde kein rechtswidriges Verhalten. Sie kann den Ruf der Behörde nicht erheblich beeinträchtigen. Die Darstellung der Ausländerbehörde zu den Voraussetzungen für eine Altfallregelung erforderte keine Offenbarung von personenbezogenen Daten.

Bei Beachtung dieser Abwägungskriterien ist die Behörde für Inneres schon nach geltendem Recht handlungsfähig, wenn die Presse Auskunft gemäß dem Pressegesetz verlangt. Außerdem kann sich die Behörde mit einer presserechtlichen Gegendarstellung äußern. Beides sind Anwendungsfälle von §13 Abs. 2 Satz 1 Nr. 7 HmbDSG, wonach die Behörde bei einem Veröffentlichungsrecht personenbezogene Daten wiedergeben darf, wenn nicht schutzwürdige Interessen der Betroffenen offensichtlich entgegenstehen. Im übrigen gilt das Datenschutzrecht ohnehin nicht für personenbezogene Daten, solange sie in allgemein zugänglichen Quellen – wie in Zeitungsartikeln – gespeichert oder soweit sie von Betroffenen zur Veröffentlichung bestimmt sind. Schließlich dürfen personenbezogene Daten auch bei Einwilligung der Betroffenen veröffentlicht werden.

11.2 Sonstiges

– Die (Teil-)Dezentralisierung der Ausländerbehörde ist weitgehend abgeschlossen. Umstritten war die Regelung der gemeinsamen Ausländerdatenbank, auf die auch alle bezirklichen Dienststellen – ohne eine technische Beschränkung auf ihre jeweilige örtliche Zuständigkeit – zugreifen können. An der notwendigen datenschutzrechtlichen Rechtsverordnung haben wir ebenso mitgewirkt wie an der komplexen Zuständigkeitsanordnung, die die Aufgabenverteilung zwischen der zentralen Ausländerbehörde und den bezirklichen Dienststellen regelt.

– Mehrere Eingaben gaben Anlaß zu Nachfragen, z.T. zu Kritik an der zentralen Ausländerbehörde. In einem Falle übermittelte die Behörde dem Gesundheitsamt, das die Reisefähigkeit eines ausreisepflichtigen Ausländers begutachten sollte, detaillierte Informationen über das Asylverfahren, über illegale Einreisen und Straftaten des Betroffenen sowie über die Art des Lebensunterhaltes.

– In einem politisch heiklen Fall mußte die Ausländerbehörde einräumen, daß sie dem Rechtsanwalt eines Landsmanns des betroffenen Ausländers Einsicht in dessen Ausländerakte mit asylrechtlichen Vorgängen gewährt hatte. Damit wurde sie möglicherweise verantwortlich für erhebliche finanzielle und politische Nachteile zulasten des Ausländers.

12. Verkehr

12.1 Identitätskarte für Taxifahrerinnen und Taxifahrer?

Überlegungen der Baubehörde, für Taxifahrerinnen und Taxifahrer eine bußgeldbewehrte Pflicht einzuführen, bei der Fahrt ständig eine Identitätskarte offen sichtbar mitzuführen, auf der Name und Lichtbild der Fahrerin oder des Fahrers zu sehen sind, werden von uns kritisch und bisher ablehnend bewertet.

Die Baubehörde überlegt, für Taxifahrerinnen und Taxifahrer die Pflicht einzuführen, eine Identitätskarte mit Name und Lichtbild während der Fahrt ständig bei sich zu führen. Ein Verstoß gegen diese Pflicht soll mit einem Bußgeld belegt werden können. Nach Auffassung der Baubehörde könnte die Einführung einer solchen Pflicht dazu beitragen, unerwünschtes, doch leider oft vorkommendes Verhalten der Taxifahrerinnen und Taxifahrer wie unhöfliche Äußerungen oder Fahrtablehnungen einzudämmen. Neben diesen verkehrspolitischen Erwägungen sprächen auch arbeitsmarktpolitische Gründe für die Einführung einer solchen Identitätskarte für Taxifahrerinnen und Taxifahrer. Im Taxengewerbe sei illegale Beschäftigung häufig, eine Pflicht zur Namensoffenbarung der Fahrerinnen und Fahrer könnte dies einschränken.

Wir haben von diesen Überlegungen nur zufällig erfahren und haben gegen die Einführung einer obligatorischen Identitätskarte für Taxifahrerinnen und Taxifahrer folgende datenschutzrechtlichen Bedenken gelten gemacht: Eine bußgeldbewehrte Pflicht, ständig einen „Ausweis“ mit Namen und Lichtbild offen sichtbar bei sich zu tragen, stellt einen Eingriff in das allgemeine Persönlichkeitsrecht der Taxifahrerinnen und Taxifahrer dar, der nach den bisherigen Überlegungen der Baubehörde nicht gerechtfertigt erscheint.

Zunächst einmal fehlt für die Einführung einer obligatorischen Identitätskarte, deren Nicht-Mitführen bußgeldbewehrt sein soll, eine ausreichenden Ermächtigungsgrundlage. §47 Abs. 3 Satz 3 Nr. 3 Personenbeförderungsgesetz (PBefG) wäre nach unserer Auffassung nicht geeignet, um auf dieser Grundlage eine Pflicht zum Mitführen einer Identitätskarte für Taxifahrerinnen und Taxifahrer einzuführen.

§47 Abs. 3 Satz 1 und 3 Nr. 3 Personenbeförderungsgesetz:

Die Landesregierung wird ermächtigt, durch Rechtsverordnung den Umfang der Betriebspflicht, die Ordnung auf Taxenständen sowie Einzelheiten des Dienstbetriebs zu regeln. ... In der Rechtsverordnung können insbesondere Regelungen getroffen werden über:

...

3. den Fahr- und Funkbetrieb

...

Diese Ermächtigungsgrundlage wäre vor allem deshalb nicht ausreichend, weil bereits Regelungen darüber existieren, welche Fahrzeugpapiere bei der Taxifahrt mitzuführen und wem gegenüber diese auszuhändigen sind. Beispielsweise ist die für Taxen erforderliche personenbeförderungsrechtliche Genehmigung nur zuständigen Personen auszuhändigen (§17 Abs. 4 PBefG). In der BOKraft wird auf der Grundlage von §57 PBefG vom Bundesverordnungsgeber geregelt, daß Name und Betriebssitz des Unternehmens im Taxi sichtbar zu machen sind.

Es leuchtet nicht ein, daß daneben ein Landesverordnungsgeber befugt sein soll, eine weitere Identifizierungspflicht für Fahrerinnen und Fahrer einzuführen. Die in §47 Abs. 3 PBefG genannten Regelungszwecke für die Landesverordnung geben jedenfalls für diese Annahme nichts her, insbesondere wäre die Verhinderung illegaler Beschäftigung im Taxengewerbe kein zulässiger Regelungszweck nach §47 Abs. 3 Satz 3 Nr. 3 PBefG („Fahr- und Funkbetrieb“). Dieser Regelungszweck berechtigt nach unserer Auffassung nicht, beliebig weitere Pflichten zum Mitführen von – insbesondere offen zu tragenden – Identitätspapieren einzuführen.

Datenschutzrechtliche Aspekte müßten ferner durch eine differenzierte Würdigung bei angestellten und selbständigen Fahrerinnen und Fahrern berücksichtigt werden. Die geplante Identifizierungspflicht würde unselbständige wie selbständige Taxifahrerinnen und Taxifahrer gleichermaßen treffen, obwohl bei selbständigen Fahrerinnen und Fahrern wegen der Pflicht zur Sichtbarmachung des Namens und Betriebssitzes des Unternehmens gemäß §27 Abs. 2 BOKraft keinerlei Notwendigkeiten für zusätzliche Identifizierungen erkennbar sind.

Ferner ist das infragestehende Vorhaben auch unter Gleichheitsgesichtspunkten fragwürdig, da nicht erkennbar ist, warum das Taxengewerbe anders zu behandeln sein soll als alle andere Gewerbebereiche. Zur Verhinderung illegaler Beschäftigung gibt es Vorschriften im Sozialgesetzbuch (SGB IV). Die Verhinderung illegaler Beschäftigung ist Zweck der Vorschriften über den Sozialversicherungsausweis nach §§95 ff. SGB IV. Dieser ist gemäß §99 Abs.1 SGB IV nur dem Arbeitgeber und gemäß §99 Abs. 2 SGB IV bestimmten Behörden vorzulegen, nicht dagegen sonstigen Privatpersonen. Diese für alle Arbeitnehmerinnen und Arbeitnehmer – also auch für nicht-selbständige Taxifahrerinnen und Taxifahrer – geltenden Vorlagepflichten mit vergleichbarem Datenumfang (auch der Sozialversicherungsausweis enthält – jedenfalls außerhalb der Sozialversicherungsnummer – kein Geburtsdatum und keine Wohnanschrift) sind gesetzlich angeordnet. In anderen Wirtschaftsbereichen, die voraussichtlich für illegale Beschäftigung nicht weniger anfällig sind (z.B. im Gaststätten- und Baugewerbe oder im Einzelhandel), gibt es jedenfalls keine Identifikationspflicht gegenüber Gästen, Kunden oder der weiteren Öffentlichkeit. Es ist nicht ersichtlich, daß der Bereich des Taxengewerbes im Hinblick auf illegale Beschäftigung durch derart schwerwiegende Besonderheiten gekennzeichnet ist, die eine Erweiterung des für alle Arbeitnehmerinnen und Arbeitnehmer geltenden Pflichtenkreises rechtfertigen könnten.

Eine Regelung zur Einführung einer obligatorischen Identitätskarte für Taxifahrerinnen und Taxifahrer wäre darüber hinaus auch unverhältnismäßig. Denn es ist nicht erkennbar, daß die Maßnahme das geeignete Mittel zur Verfolgung des angestrebten Zwecks ist. Auch nach bisherigen Regelungen können sich Fahrgäste über unzulängliches Verhalten von Taxifahrerinnen und Taxifahrern beschweren. Die Beschwerdemöglichkeiten von Fahrgästen werden bisher durch die nach §27 BOKraft vorgeschriebene Angabe zur Ordnungsnummer des Taxis und zum Namen und Betriebssitz des Unternehmens sichergestellt. Mit diesen Angaben und der Kenntnis des Unternehmens, wer zum konkreten Zeitpunkt gefahren ist, sind auch die Fahrerinnen und Fahrer im Beschwerdefall identifizierbar. Fahrgäste von Taxis haben damit die gleichen Beschwerdemöglichkeiten wie Fahrgäste von Bussen im öffentlichen Personennahverkehr.

Es ist bisher nicht ersichtlich, warum diese Beschwerdemöglichkeit nicht ausreicht, zumal auch die Pflicht zur Mitführung einer Identitätskarte deren mißbräuchliche Verwendung nicht ausschließt.

Zur Verhinderung der illegalen Beschäftigung ist festzustellen, daß auch illegal beschäftige Taxifahrerinnen und Taxifahrer ohne weiteres die Möglichkeit hätten, ein Schild mit Foto und Namen auszulegen. Dies besagt nichts über die nach anderen Rechtsvorschriften erforderlichen Erlaubnisse. Anderseits besagt ein fehlendes „Taxifahrerschild“ nicht, daß auch die anderen erforderlichen Erlaubnisse fehlen. Die überprüfungsberechtigen Behörden müßten sich somit in allen Fällen die anderen Erlaubnisse (Führerschein, Erlaubnisse nach §48 Fahrerlaubnisverordnung und nach dem Personenbeförderungsgesetz, Sozialversicherungsausweis) vorlegen lassen, das „Taxifahrerschild“ vermittelt keine zusätzlichen Erkenntnisse. Danach bliebe als einziger Zweck übrig, daß Fahrgäste in Fällen, in denen das Schild fehlt, oder das Lichtbild offenbar nicht mit dem Fahrer bzw. der Fahrerin übereinstimmt, die Fahrt verweigern und/oder gegenüber Behörden Anzeige erstatten. Ohne nachvollziehbare Begründung, daß die vorgesehene Pflicht auch zu dem angestrebten Ziel führen könnte, wäre sie insbesondere in Verbindung mit einer vorgesehenen Bußgeldbewehrung unverhältnismäßig.

Die Baubehörde hat unsere Einwendungen zu den geplanten Vorhaben bereits zur Kenntnis genommen, jedoch hinsichtlich des geplanten Zieles ihre Auffassungen zunächst beibehalten. Hinsichtlich der Begründung sagte sie zu, sich näher mit unseren Einwendungen auseinanderzusetzen. Wir werden die Angelegenheit weiter verfolgen und kritisch beobachten.

12.2 Feststellung von Parksündern durch Privatpolizisten?

Sofern der Einsatz von Hilfspolizisten zur Feststellung von Ordnungswidrigkeiten im Straßenverkehr überhaupt in Betracht kommt, muß jedenfalls sichergestellt sein, daß die erhobenen Daten ausschließlich zur Verfolgung der Ordnungswidrigkeiten durch die Bußgeldstelle verwendet werden und die Tätigkeit der Hilfspolizisten uneingeschränkt datenschutzrechtlich kontrolliert werden kann.

In der Umgebung des Flughafens Hamburg wird häufig verbotswidrig geparkt. Die Ordnungskräfte der Flughafen GmbH bringen Parkverstöße zur Anzeige, indem sie formularmäßige Bußgeldanzeigen mit den festgestellten Fahrzeugkennzeichen an die zur Verfolgung der Ordnungswidrigkeiten im Straßenverkehr zuständige Bußgeldstelle übermitteln. Dort werden die Angaben aus den Formularen in das automatisierte Verfahren zur Bearbeitung der Bußgeldvorgänge übertragen.

Zur Vereinfachung dieses Ablaufs gibt es Überlegungen, den Mitarbeitern des Ordnungsdienstes die mobilen Datenerfassungsgeräte zur Verfügung zu stellen, die auch von den polizeilichen Mitarbeitern zur Aufnahme von Parkverstößen benutzt werden. Die erneute Datenerfassung in der Bußgeldstelle würde wegfallen; vielmehr würden die Daten aus den mobilen Datenerfassungsgeräten elektronisch in das automatisierte Verfahren der Bußgeldstelle übertragen. Damit würden allerdings die Mitarbeiter des privaten Ordnungsdienstes entscheiden, ob, an welchen Stellen und bei welchen Fahrzeugen Parkverstöße als Ordnungswidrigkeiten geahndet werden sollen. Wegen des automatisierten weiteren Ablaufs (Einspielen der Daten in das Verfahren der Bußgeldstelle, Feststellung der Fahrzeughalter aufgrund des Kennzeichens, Anschriftenermittlung im Melderegister und anschließende Erstellung und Versendung des Anhörungsschreibens im Bußgeldverfahren) wäre eine eigenverantwortliche Prüfung der Bußgeldstelle nicht mehr dazwischen geschaltet.

Eine vergleichbare Datenerhebung durch private Stellen in anderen Städten ist durch die zuständigen Gerichte als unzulässig bezeichnet worden, weil die Verfolgung von Ordnungswidrigkeiten als hoheitliche Aufgabe nicht vollständig privaten Stellen überlassen werden darf. Vielmehr muß die Verwaltung ihre Entscheidungs- und Eingriffsmöglichkeit während des gesamten Verfahrensablaufs behalten (Kammergericht Berlin, NJW 1997, 2894 ff.).

Statt der unzulässigen Privatisierung der hoheitlichen Aufgabe sah die Behörde für Inneres eine Möglichkeit zur Lösung des Problems darin, die privaten Mitarbeiter des Ordnungsdienstes in den Bereich der öffentlichen Verwaltung einzubeziehen. Sie schlug vor, die Mitarbeiter des Ordnungsdienstes zu Hilfspolizisten nach §29 des Gesetzes zum Schutz der öffentlichen Sicherheit und Ordnung (SOG) zu ernennen. Nach dieser Vorschrift kann die Behörde Personen mit deren Einwilligung u.a. zur Überwachung der Regelungen des Straßenverkehrs zu Hilfspolizisten ernennen, die dann im Rahmen ihres Auftrages die den Beamten des Polizeivollzugsdienstes zustehenden Befugnisse haben.

In unserer Stellungnahme zu diesen Überlegungen haben wir darauf hingewiesen, daß diese Lösung nicht bedenkenfrei wäre. Das SOG als Landesgesetz zur Regelung von Aufgaben der Gefahrenabwehr kann keine Aussagen zur Verfolgung von Ordnungswidrigkeiten treffen, die bundesgesetzlich geregelt ist. Nach §53 Ordnungswidrigkeitengesetz (OWiG) des Bundes haben nur Behörden und Beamte des Polizeidienstes die eigenständige Befugnis zur Erforschung von Ordnungswidrigkeiten. Somit ist schon vom Wortlaut her zweifelhaft, ob Personen, die weder Polizeivollzugsbeamte noch Angestellte der Polizeibehörde sind, sondern nur als Hilfspolizisten fungieren, zum Kreis der nach §53 OWiG Ermächtigten gehören können. Wir haben allerdings auch deutlich gemacht, daß diese Frage fachlich und erforderlichenfalls durch die Gerichte, nicht jedoch datenschutzrechtlich zu entscheiden ist.

Wenn die rechtliche Prüfung zu dem Ergebnis führt, daß auch die Erhebung und weitere Verarbeitung von Daten durch die Mitarbeiter des Ordnungsdienstes als Hilfspolizisten gemäß §29 SOG grundsätzlich zulässig ist, müßten aus datenschutzrechtlicher Sicht bei der Auftragserteilung nach §29 SOG an die Hilfspolizisten folgende Maßgaben sichergestellt sein:

• Die von den Mitarbeitern des Ordnungsdienstes erhobenen und in mobilen Datenerfassungsgeräten gespeicherten Daten dürfen ausschließlich zur Verfolgung der jeweiligen Ordnungswidrigkeiten verwendet werden. Hierzu müssen die Daten restlos an die Bußgeldstelle abgeliefert werden.

• Die Tätigkeit der Mitarbeiter des Ordnungsdienstes in ihrer Eigenschaft als Hilfspolizisten muß uneingeschränkt der behördlichen Kontrolle und auch unserer Kontrolle unterliegen.

Bei Redaktionsschluß dieses Berichts stand noch nicht fest, ob es zu einer Beauftragung von Hilfspolizisten kommt.

13. Polizei

13.1 Neue Infrastruktur zur polizeilichen Datenverarbeitung

Mit den neu eingeführten Verfahren POLAS und COMVOR und dem geplanten INPOL-Verfahren verfügt die Polizei über eine völlig neue Infrastruktur zur Datenverarbeitung, die mehr Mitarbeitern mehr Informationen über mehr Personen leichter und schneller zur Verfügung stellt. Für eine Reihe von damit zusammenhängenden Fragen konnten datenschutzrechtlich befriedigende Lösungen erreicht werden. Es gibt aber auch ungelöste Probleme.

Im Berichtsjahr hat sich die Infrastruktur zur polizeilichen Datenverarbeitung grundlegend verändert. Bisher war das zentrale Auskunftssystem POLAS mit Verbindung zum bundesweiten INPOL-System das prägende Verfahren zur automatisierten Datenverarbeitung der Polizei. Daneben gab es verschiedene teilweise automatisierte, teilweise aber auch noch manuell geführte dezentrale Anwendungen, mit denen Dateien über kriminalpolizeiliche Erkenntnisse aber auch Register und Indizes zur Aktenverwaltung geführt wurden. Völlig getrennt davon verlief die Bearbeitung einzelner polizeilicher Vorgänge mit Hilfe der automatisierten Textverarbeitung oder auch der Schreibmaschine.

Inzwischen finden die Mitarbeiter der Polizei auf ihrem Arbeitsplatz einen PC vor, bei dem sie mit Mausklick entscheiden können, ob sie polizeiliche Erkenntnisse über eine Person aus POLAS, INPOL, dem Schengener Informationssystem oder einer dezentralen Datei abrufen, Daten aus dem Melde-, dem Fahrzeug- oder aus dem Ausländerzentralregister erfragen, eigene Vorgänge bearbeiten und sie an andere Polizeidienststellen übersenden, sich nach dem Verbleib einer Akte erkundigen, oder feststellen wollen, wann und wo ein bestimmter polizeilicher Einsatz stattgefunden hat. Die technischen Möglichkeiten vernetzter Arbeitsplatzrechner führen dazu, daß Informationssammlungen, die bisher nur für begrenzte Aufgaben bestimmter Dienststellen angelegt wurden, nunmehr von ganzen Abteilungen im Landeskriminalamt genutzt werden. Damit erweitern sich die Zugriffsrechte und auch die Informationssammlungen insgesamt.

Der Ausbau dieser Infrastruktur mit den neuen Verfahren POLAS und COMVOR ist nach langjährigen Vorarbeiten und zahlreichen Problemen und Verzögerungen erfolgt und noch nicht abgeschlossen. Die Projektmitarbeiter haben ungeachtet des erheblichen Zeitdrucks in allen anstehenden datenschutzrechtlichen Fragen stets mit umfassender Information und der Bereitschaft, einvernehmliche Lösungen zu finden, die Zusammenarbeit mit uns gesucht.

Für die neuen polizeilichen Verfahren gelten gemeinsam folgende Vorgaben zur Benutzerverwaltung und Protokollierung:

• Benutzerverwaltung

Die Vergabe sämtlicher innerhalb der Polizei relevanten Benutzerrechte für automatisierte Anwendungen an alle Mitarbeiter und die Organisation dieser Benutzerrechte stellt bei der großen Zahl berechtigter Personen und deren häufigem Wechsel zwischen verschiedenen Dienststellen hohe Anforderungen. Die Polizei hat hierfür eine aus unserer Sicht überzeugende Konzeption entwickelt. Alle Mitarbeiter verfügen jeweils über eine eigene zentral vergebene Chipkarte mit ihren Personendaten, die den Zugriff auf die Arbeitsplatzrechner steuert. Für die einzelnen Organisationseinheiten der Polizei (z.B. Polizeirevier oder Abteilung im LKA) gelten jeweils unterschiedliche Zugriffsrechte. Diese unterscheiden sich auch je nach der Funktion der Mitarbeiter. Das jeweils erforderliche Berechtigungsprofil wird mit Hilfe einer besonderen Datei zur Benutzerverwaltung vergeben. Beim Wechsel der Mitarbeiter zwischen verschiedenen Organisationseinheiten wird sichergestellt, daß mit der Vergabe der neuen Rechte alle bisherigen Rechte entfallen. So wird vermieden, daß frühere u.U. weitere Zugriffsrechte auch nach einem Aufgabenwechsel bestehen bleiben und somit die organisations- und funktionsbezogenen Zugriffsgrenzen unterlaufen werden.

• Protokollierung

Abfragen aus dem polizeilichen Auskunftssystem POLAS wurden früher nicht regelmäßig, sondern nur dann automatisch protokolliert, wenn im Einzelfall ein Mißbrauchsverdacht bestand. Für die Abfragen aus dem Schengener Informationssystem und die neuen Verfahren POLAS und COMVOR ist nunmehr eine Vollprotokollierung sämtlicher lesender und ändernder Zugriffe eingeführt worden.

Die Protokollierung ermöglicht zwar einerseits eine verbesserte Kontrolle beim Mißbrauch und beugt ihm vor. Andererseits entstehen große zusätzliche Datenbestände über die von den Abfragen betroffenen Personen und die polizeilichen Mitarbeiter. Wir haben vorgeschlagen, zur Begrenzung dieser Risiken Festlegungen zu folgenden Fragen zu treffen: Wo werden die Protokolldateien gespeichert? Wer nimmt die Auswertung vor? Nach welchen Kriterien und bei welchen Anlässen ist eine Protokollauswertung möglich? Die Ausarbeitung eines entsprechenden Konzeptes dauerte bei Redaktionschluss dieses Berichts noch an.

13.1.1 POLAS-neu

Die Neuentwicklung des seit Jahrzehnten bestehenden polizeilichen Auskunftssystems POLAS war erforderlich, weil das bisherige Betriebssystem vom LIT nicht weiter zur Verfügung gestellt wird und das verwendete Datenbanksystem nicht Jahr-2000-fähig ist. Es handelt sich daher im wesentlichen um eine technisch neue Version, inhaltliche Änderungen des Datenbestandes sind nicht erfolgt. Allerdings sind die Zugriffsrechte erweitert worden. Insbesondere sind die bisherigen Begrenzungen der Zugriffs auf Speicherungen über Kinder (vgl. 11.TB, 17.4) und bei der sogenannten Gesamtauskunft entfallen. Im früheren Verfahren waren nur Bedienstete, die sachbearbeitende Funktionen ausüben, also überwiegend Angehörige der Kriminalpolizei umfassend zugriffsberechtigt. Für die Mehrzahl der Angehörigen der Schutzpolizei galten Einschränkungen.

Mit unseren Bedenken gegen den Wegfall der bisherigen Differenzierungen konnten wir uns nicht durchsetzen. Die Polizei hat dem entgegengehalten, daß die erweiterten Zugriffsrechte zur Aufgabenerfüllung erforderlich sind. Im Unterschied zu früher sei immer weniger die Zugehörigkeit zu einem bestimmten polizeilichen Organisationszweig (also Schutzpolizei oder Kriminalpolizei) für die Aufgabenerfüllung entscheidend. Vielmehr werde das Aufgabenprofil insbesondere durch die Bildung von Polizeikommissariaten zunehmend vereinheitlicht, so daß auch Beamte der Schutzpolizei sachbearbeitende Funktionen wahrnehmen.

13.1.2 COMVOR

Das Verfahren zur „computergestützten Vorgangsbearbeitung“ (COMVOR) ist in zwei wesentlichen Schritten vorangekommen. Im Frühjahr 1999 wurde die Möglichkeit geschaffen, an 2100 Arbeitsplatzrechnern polizeiliche Vorgänge (Anzeigen, Vernehmungen, Berichte über Einsätze und eine große Fülle weiterer Vorgangsarten) mit Hilfe von elektronischen Formularen automatisiert zu erfassen. Im Sommer wurde dann eine Indexdatei als einheitliches „Tagebuch“ zur Verwaltung der jeweiligen Vorgänge eingeführt.

Diese Funktionalitäten sind nicht völlig neu. Bereits 1994 (13. TB, 17.3) und 1997 (16.TB, 15.1) war die Einführung der ersten Teilleistung zur Formularfertigung vorgesehen, ist allerdings immer wieder gescheitert. Die Lösung der Probleme war dadurch möglich, daß man die frühere technisch sehr aufwendige Konzeption eines integrierten Verfahrens zum Ausfüllen der Formulare und zur Datenhaltung aufgegeben hat. Die neue Konzeption trennt nunmehr den Formularteil von der Indexdatenbank.

• Vorgangsbearbeitung mit Formularen

Zum Ausfüllen der Formulare werden Standardprodukte zur Textverarbeitung benutzt. Grundsätzlich sind die Mitarbeiter nur für die von ihnen selbst ausgefüllten Vorgänge zugriffsberechtigt. Mitarbeiter, die den Vorgang angelegt haben, können diese an andere zuständige Dienststellen (z.B. vom Polizeirevier an das Kriminalkommissariat oder das Landeskriminalamt) weiterleiten. Sie können weitere Mitarbeiter berechtigen. Daten, die in bestimmten Formularfeldern gespeichert sind, können automatisiert in neue Formulare für denselben Vorgang übernommen werden.

Wenn einzelne Vorgänge nicht weitergeleitet oder gelöscht werden, besteht die Möglichkeit zur Archivierung der elektronisch gespeicherten Inhalte für eine Frist von maximal einem Jahr. Anhand des Aktenzeichens kann der jeweilige Eigentümer oder der für die Verteilung der Vorgänge an einzelne Sachbearbeiter zuständige Vorgesetzte die Vorgänge wieder aus dem Archiv holen. Alle in COMVOR erstellten Vorgänge werden ausgedruckt und zum Bestandteil der Ermittlungsakte.

• **Indexdatei**

Aus datenschutzrechtlicher Sicht ruft die neue Indexdatei größere Probleme hervor. Aus bestimmten Feldern in den Vorgangsformularen werden die Daten automatisch in eine gesonderte Indexdatenbank übertragen. Hierbei handelt es sich insbesondere um die Personalien der von einem Vorgang betroffenen Personen mit der jeweiligen Rolle (also z.B. Beschuldigte, Anzeigenerstatter, Geschädigte oder Beteiligte an einem sonstigen Vorgang), Angaben zur Art des Ereignisses (z.B. Straftat, Verkehrsunfall oder polizeiliche Maßnahme zur Gefahrenabwehr), zum Ort und Zeitpunkt, zum Tatobjekt (z.B. Stehlgut), zu Kraftfahrzeugen usw. Mit diesen Angaben sollen vorhandene Vorgänge wiedergefunden werden und Auskünfte über ihren Verbleib erteilt werden, z.B. bei der Nachfrage eines Bürgers, was aus seiner Strafanzeige geworden ist. Auch zur Zuordnung eingehender Schreiben (z.B. Listen von Geschädigten über gestohlene Sachen) zu bestimmten Vorgängen ist die Indexdatei erforderlich. Sie dient ferner dazu, bestimmten Mitarbeitern oder Dienststellen neue Vorgänge zuzuweisen, wenn sie bereits mit vergleichbaren Sachverhalten befaßt waren.

Bisher wurden für diese Zwecke automatisierte Dateien in den Polizeidirektionen oder auch manuelle Verzeichnisse in den jeweiligen Dienststellen des Landeskriminalamtes benutzt. Die faktischen Zugriffsmöglichkeiten auf die genannten Personendaten waren dadurch regional oder funktional begrenzt. Mit der neuen Indexdatei stehen dagegen alle polizeilichen Daten allen Mitarbeitern unmittelbar zur Verfügung. Im Unterschied zu Speicherungen in POLAS hängen die Personendaten im Index nicht davon ab, daß ihre Erforderlichkeit zur vorbeugenden Bekämpfung von Straftaten besonders geprüft und bewertet wurde. Während POLAS nur Aufschluß über Personen gibt, gegen die die Polizei wegen eines Straftatverdachts ermittelt hat und der Verdacht im weiteren Ermittlungsverfahren bestätigt wurde, würde es die Technik und Struktur von COMVOR ermöglichen, Auskunft über jede Person zu erhalten, die irgendeinen Kontakt mit der Polizei hatte.

Um diese Auswirkungen zu begrenzen, sind verschiedene Einschränkungen für Abfragen vorgesehen. Personenabfragen erfordern stets die Eingabe einer Rolle, bei Daten über Vermißte, Geschädigte und Anzeigende muß zusätzlich ein auf drei Monate begrenzter Ereigniszeitraum angegeben werden. Die bei den früheren Planungen zu COMVOR vorgesehene weitere Einschränkung anhand des Ereignisortes war nach der neuen Konzeption nicht realisierbar. Im neuen Verfahren findet keine Überprüfung von Plausibiliäten statt, so daß unrichtige Schreibweisen von Straßennamen ohne Korrektur in der Datenbank erfaßt werden. Eine Benutzung von Anschriften der Ereignisorte als zusätzlichem Kriterium zur Eingrenzung würde daher bei abweichenden Schreibweisen den gesuchten Vorgang nicht anzeigen. Daten von Personen, die bei sonstigen polizeilichen Vorgängen zur Gefahrenabwehr oder bei Ordnungswidrigkeiten beteiligt sind, sind nur im Rahmen der örtlichen Zuständigkeit abrufbar. Das LKA, für das keine örtlichen Zuständigkeitsgrenzen gelten, hat keinen Zugriff auf diese Daten. In Einzelfällen können Daten von besonderer Sensibilität (z.B. Geschädigte bei Sexualstraftaten, Fälle organisierter Kriminalität) mit einem Satzschutz versehen werden, der den Zugriff auf die ermittlungsführende Polizeidienststelle begrenzt.

Mit diesen Vorkehrungen wird immerhin ein gewisser Bezug zum Dateizweck der Vorgangsverwaltung erreicht, so daß der COMVOR-Index nicht als allumfassende Personenauskunftsdatei benutzt wird. Allerdings bleiben Probleme bestehen, die auch bei den intensiven Beratungen nicht einvernehmlich gelöst werden konnten. Sie lassen sich beispielhaft an Daten über Kinder (unter 14 Jahren) aufzeigen. Für Speicherungen über Kinder in POLAS ist eine besondere Begründung erforderlich, die Speicherungsfrist ist durch §15 Satz 5 des Gesetzes über die Datenverarbeitung der Polizei auf zwei Jahre begrenzt (vgl. 11.TB, 17.4). Wenn dagegen in einem Strafermittlungsvorgang ein Kind als Verursacher der Straftat erfaßt wird, führt dies ohne weiteres zur Speicherung im COMVOR-Index. Hierfür ist eine Frist von fünf Jahren vorgesehen, die erst beginnt, wenn der Vorgang bei der Polizei abgeschlossen ist. Die Polizei hat zur Begründung darauf hingewiesen, daß die Speicherungen im COMVOR-Index nicht zur vorbeugenden Bekämpfung von Straftaten, sondern allein zur Verwaltung polizeilicher Strafermittlungsvorgänge erfolgt, die Vorschriften des PolDVG somit nicht gelten. Dies trifft zwar rechtlich zu, ändert jedoch nichts an dem Ergebnis, daß die für POLAS geltenden gesetzlichen Beschränkungen wirkungslos werden, wenn ein polizeilicher Mitarbeiter die Abfrage zu der betroffenen Person nicht in POLAS sondern im COMVOR-Index durchführt.

Wir haben zur Abmilderung dieses Widerspruchs vorgeschlagen, entweder die Speicherungen über Kinder im COMVOR-Index auf zwei Jahre zu begrenzen oder aber – vorzugsweise – für sämtliche Speicherungen zur Vorgangsverwaltung, also auch für die zugrunde liegenden Aktenvorgänge die Fristen zu verkürzen. Die Polizei lehnt dies mit der Begründung ab, daß sie auch nach Abgabe ihrer Ermittlungsvorgänge noch längere Zeit damit rechnen müsse, daß von der Staatsanwaltschaft Rückfragen oder Aufträge zur Nachermittlung eingehen. Für überzeugend halten wir diesen Einwand nicht, denn selbst wenn bei der Polizei die Ermittlungsvorgänge nach zwei Jahren gelöscht würden, gingen keine Informationen verloren, da sie vollständig und rechtlich verbindlich in der staatsanwaltschaftlichen Ermittlungsakte vorliegen.

13.1.3 INPOL-neu

Wenn die Pläne zum Aufbau des Verfahrens INPOL-neu realisiert werden, wird die für Hamburg beschriebene Infrastruktur zur polizeilichen Datenverarbeitung durch ein bundesweites Verfahren ergänzt und erweitert. Die Konzeption für INPOL-neu sieht vor, daß unter einer einheitlichen Benutzeroberfläche Abfragen der einzelnen Mitarbeiter aus den jeweiligen Vorgangsbearbeitungsdateien bis hin zu INPOL möglich sind. Andererseits sollen auch die in INPOL zu speichernden Daten ausgehend von der Vorgangsbearbeitung über das Landesinformationssystem bis zu einzelnen INPOL-Anwendungen übertragen werden. Die fachlichen und technischen Konzepte für das neue Verfahren sind weitgehend abgeschlossen, nach dem bisherige Zeitplan soll im Mai 2000 der Bereich der Fahndungsabfragen aus dem bundesweiten System als erster Schritt realisiert werden.

Die Datenschutzbeauftragten des Bundes und der Länder haben zur Klärung der datenschutzrechtlichen Fragen im Zusammenhang mit INPOL eine Arbeitsgruppe gebildet, die in engem Kontakt zu dem beim Bundeskriminalamt angesiedelten Projekt steht.

Von zahlreichen behandelten Einzelproblemen können beispielhaft die folgenden genannt werden:

• Kriminalaktennachweis

Der bisherige INPOL-Kriminalaktennachweis (KAN) ist auf Daten über Beschuldigte bei Straftaten von länderübergreifender oder sonst erheblicher Bedeutung begrenzt. Die INPOL-Neukonzeption sieht vor, neben diesen bundesweit bedeutsamen Tatvorwürfen die sogenannte „kriminelle Historie“ eines Betroffenen auch dann zu erfassen, wenn diese weiteren Vorwürfe für sich betrachtet keine INPOL-Relevanz besitzen. Dies soll ein „abgerundetes Beschuldigtenbild“ vermitteln. Es sollen alle weiteren Tatvorwürfe über einen Beschuldigten gespeichert werden, wenn in einem Fall die bundesweite Relevanz bejaht wird.

Nach eingehenden Beratungen mit allen Datenschutzbeauftragten hat die INPOL-Arbeitsgruppe diese Pläne abgelehnt, da sie nicht mit §2 Abs. 1 des Bundeskriminalamtsgesetzes (BKAG) in Einklang zu bringen sind. Nach dieser Vorschrift ist die Funktion des BKA als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen, wozu auch die Führung des INPOL-Verfahrens gehört, auf die Unterstützung der Länderpolizeien bei der Verfolgung und Verhütung von Straftaten von länderübergreifender und sonst erheblicher Bedeutung begrenzt. Beurteilungskriterium für die INPOL-Relevanz ist danach „die Tat“, nicht „der Täter“. Bei Redaktionsschluss dieses Berichts lag noch keine Antwort zu dieser Stellungnahme der Datenschutzbeauftragten vor.

• Polizeiführungsinformationen

Grundsätzlich positiv zu bewerten sind dagegen die Überlegungen für sogenannte „Polizeiführungsinformationen“. Hierbei sollen aus der Fülle der einzelnen in den dezentralen polizeilichen Vorgangsverwaltungssystemen erfaßten Falldaten Informationen an einen zentralen Server geliefert werden, der getrennt vom personenbezogenen INPOL-Bestand geführt wird. Mit dem Verfahren sollen auch personenbezogene Meldedienste, die z.B. bisher betrieben werden, um die Gesamtmenge des sichergestellten Rauschgifts zu ermitteln, teilweise ersetzt werden.

Durch eine geeignete Verschlüsselungsfunktion wird erreicht, daß zusammenhängende Einzelinformationen zusammengeführt werden, ohne daß ein Personenbezug aus den aggregierten Daten hervorgeht. Die zentral gespeicherten Falldaten können unter allen nützlichen Gesichtspunkten (etwa zur Häufung bestimmter Straftaten in bestimmten Gegenden) ausgewertet werden. Die Auswertungen stehen dann den Polizeien im Bund und der Ländern zur Verfügung. Wenn dieses Verfahren realisiert wird, entsteht ein umfassendes polizeiliches „Data-Warehouse“ ohne Beeinträchtigung der Datenschutzrechte von Einzelpersonen.

13.2 Analysedateien

Bei Analysedateien handelt es sich um einen neuen Typ polizeilicher Datenverarbeitung, der zunehmend Bedeutung erlangt und erhebliche datenschutzrechtliche Probleme aufwirft. Im Unterschied zu herkömmlichen polizeilichen Dateianwendungen erfolgt die Speicherung von Personendaten nicht primär zu dem Zweck, vorhandene Erkenntnisse über einzelne Personen (z.B. über frühere Ermittlungen oder einen vorliegenden Haftbefehl) für Abfragen zur Verfügung zu stellen. Vielmehr sollen mit Hilfe der in Analysedateien gespeicherten Angaben durch Recherchen und automatisierte Auswertungen („Analysen“) neue Erkenntnisse gewonnen werden. Man spricht auch von Instrumenten zur „Verdachtsgewinnung“ oder „Verdachtsverdichtung“ durch automatisierte Datenverarbeitung. Um diese Ziele zu erreichen, sollen Daten über einen möglichst großen Kreis von Personen und Fällen mit möglichst vielen Einzelangaben erfaßt werden. Die Zwecksetzung von Analysedateien kollidiert somit zwangsläufig mit den datenschutzrechtlichen Forderungen nach Datensparsamkeit, nach Begrenzung auf überprüfte (sogenannte „harte“) Daten und dem Verzicht auf Datenspeicherungen für nicht klar definierte Zwecke.

13.2.1 EUROPOL-Analysedateien

Speicherungen in Analysedateien bei EUROPOL müssen sich stärker als bisher vorgesehen auf den spezifischen Zweck von EUROPOL-Analysen konzentrieren. Eine Übermittlung von Daten an EUROPOL setzt eine strikte Relevanzprüfung voraus.

Nachdem alle im EUROPOL-Übereinkommen vorgesehenen Rechtsakte in Kraft getreten sind, hat EUROPOL im Sommer 1999 seine Tätigkeit aufgenommen. Damit waren die Voraussetzungen für eigene Dateien bei EUROPOL erfüllt. Hierzu wurden Entwürfe für Errichtungsanordnungen entwickelt, auf deren Grundlage einzelne Analysedateien geführt werden sollen. Die Hoffnung, daß die Konkretisierung in den Errichtungsanordnungen die Bedenken gegen den im EUROPOL-Übereinkommen und den Durchführungsbestimmungen vorgesehenen Umfang von Speicherungen abmildern würde (vgl. 15. TB, 15.1), hat sich nicht erfüllt. Vielmehr schöpfen die Errichtungsanordnungen den extrem weiten Rahmen der nach den Rechtsvorschriften möglichen Datenspeicherungen weitestgehend aus. Es ist nicht erkennbar, daß man sich mit der Frage auseinandergesetzt hat, für welche Zwecke welche Arten von Daten erforderlich sind. Vielmehr entsteht der Eindruck, die Analysedateien würden in der Hoffnung angelegt, man würde schon irgendetwas herausbekommen, wenn man möglichst viel hineingibt.

In unserer gegenüber der Behörde für Inneres abgegebene Stellungnahme haben wir kritisiert, daß der Gegenstand der Analysen nur sehr undeutlich mit Bezugnahmen auf einzelne Kriminalitätsbereiche umschrieben wird. Aus den Errichtungsanordnungen ist entgegen Art. 10 Abs. 2 Satz 2 des EUROPOL-Übereinkommens nicht erkennbar, ob eine Analysegruppe gebildet wurde und welche Aufgabenstellung sie hat. Es fehlt insbesondere die Eingrenzung auf Personengruppen, die für den spezifischen Zweck von EUROPOL-Analysen tatsächlich bedeutsam sei können. Es reicht nicht aus, daß die Speicherungen irgendeine Unterstützung für polizeiliche Ermittlungen ermöglichen, denn zu diesem Zweck unterhalten die Polizeien der Mitgliedstaaten eigene Informationssammlungen.

Eine bloße Verdoppelung dieser Speicherungen bei EUROPOL kann nicht Sinn von Analysedateien sein. Insbesondere ist nicht nachvollziehbar, warum z.B. Zeugen oder sogar Personen, die möglicherweise Zeuge sein könnten, mit ihren Personalien in Analysedateien erfasst werden. Die ermittlungsführenden Behörden kennen die für den jeweiligen Fall bedeutsamen Zeugen und benötigen daher keine EUROPOL-Speicherung über diese Daten. Wegen der hierdurch entstehenden massiven Gefährdungen für die Betroffenen wäre es insbesondere nicht vertretbar, wenn aufgrund von EUROPOL-Speicherungen die Identitäten von Personen offenbart würden, die unter Zeugenschutz stehen. Derartige Speicherungen sehen die Errichtungsanordnungen jedoch vor.

In den Errichtungsanordnungen sind einerseits Daten über die persönliche Lebensführung von Betroffenen bis hin zu Angaben über den „Lebensstandard (z.B. über seine Verhältnisse leben) und Routinen“ oder Hinweise auf Speicherungen in anderen nicht-polizeilichen Datensammlungen mit höchstem Detaillierungsgrad vorgesehen. Andererseits fehlen Datenfelder mit Angaben zu konkreten Tatvorwürfen mit Tatzeiten, Bezeichnung des Straftatbestandes, zur zuständigen Ermittlungsbehörde und insbesondere zum Verfahrensergebnis. Ohne diese Einzelangaben sind weder Speicherungsfristen einzuhalten, noch ist die datenschutzrechtliche Verantwortlichkeit der Stellen, die die Daten eingegeben haben, zu wahren.

Die Gemeinsame Kontrollinstanz für EUROPOL hat diese und weitere Kritikpunkte gegenüber dem EUROPOL-Verwaltungsrat zur Sprache gebracht. Daraufhin sind einige Änderungen an den Entwürfen der Errichtungsanordnungen erfolgt. So ist nicht mehr vorgesehen, daß EUROPOL auch Analysen im Interesse von Drittstaaten, die nicht zu EUROPOL gehören, mit den Daten von Mitgliedstaaten durchführt. In anderen wesentlichen Punkten sind die Errichtungsanordnungen dagegen unverändert erlassen worden. Auf unsere Nachfrage hat die Behörde für Inneres mitgeteilt, daß bisher von der Polizei Hamburg keine Daten an EUROPOL angeliefert wurden. Wenn dies im Einzelfall künftig geschehen sollte, muß zuvor eine strikte Relevanzprüfung im Hinblick auf eindeutig definierte Analysezwecke stattfinden.

13.2.2ViCLAS

Wegen des bespiellosen Umfangs von Einzelangaben aus dem höchstpersönlichen Lebensbereich sollte die ViCLAS-Datei möglichst ohne unmittelbaren Personenbezug geführt werden. Bei der Speicherung von Daten über Opfer ist der Verzicht auf Personalien unabdingbar.

Mit dieser Abkürzung, die für „Violent Crime Linkage Analysis System“ steht, wird ein in Kanada entwickeltes Analyse-System zur Verknüpfung von Gewaltverbrechen bezeichnet. Es ist geplant, dieses Verfahren als Verbunddatei im Rahmen des bundesweiten polizeilichen Informationssystems INPOL mit Zugriffsrechten aller Landeskriminalämter einzurichten. Einzelne Landeskriminalämter führen schon jetzt eigenständige ViCLAS-Dateien; Hamburg will sich dem bundesweiten Verfahren anschließen.

Zweck der Datei soll es sein, Tatzusammenhänge bei Gewalttaten – insbesondere bei Tötungsdelikten oder Sexualstraftaten – zu erkennen, um Täter zu identifizieren und Tatserien aufzuklären. Die Besonderheit von ViCLAS besteht darin, den Hergang und die Begleitumstände einzelner Fälle aus diesen Bereichen mit größtmöglicher Präzision zu erfassen. Aufgrund dieser Erkenntnisse wird ein Täterprofil erstellt. Durch automatisierten Abgleich mit den bereits früher erfassten anderen Fällen soll festgestellt werden, ob es Gemeinsamkeiten gibt, die auf weitere Verbrechen bereits bekannter Täter oder auf bisher nicht erkannte Serien hindeuten. Diese Verfahrensweise wird als operative Fallanalyse bezeichnet.

Der beschriebene Ansatz leuchtet ein und ist datenschutzrechtlich unproblematisch, wenn es z.B. um bestimmte kriminaltechnisch festgestellte Merkmale einer Tatwaffe geht, die auch in anderen Fällen vorgefunden werden. ViCLAS beschränkt sich jedoch nicht auf derartige unmittelbar tatbezogene Sachdaten. Vielmehr soll mit einem standardisierten Fragebogen eine Fülle von teilweise höchstsensiblen Einzelangaben über Opfer und Täter erhoben und gespeichert werden. Erst dieser Fragebogen macht die bisher beispiellose Dimension der Datei deutlich. Er umfaßt insgesamt 163 Fragen mit weiteren zahlreichen Unterfragen. Zur Illustration können folgende Beispiele dienen, die nur einen kleinen Ausschnitt aus dem vorgesehenen Datenkatalog darstellen:

• Körperliche Beschreibung des Opfers zum Zeitpunkt der Tat mit Angaben zur Körpergröße, Körpergewicht, Gestalt, Haarlänge, Haarfarbe

• Sonstige körperliche Merkmale des Opfers mit Angaben zu Narben, Hautveränderungen, Mißbildungen, Piercing, Tätowierungen

• Übliche Art der Fortbewegung des Opfers (z.B. zu Fuß, Auto, Bus, Flugzeug usw.)

• Zusammenleben des Opfers mit Eltern, Freunden, gleichgeschlechtlichem Partner usw.

• Angaben zum Lebensstil des Opfers (z.B. Durchschnittsbürger, kontaktfreudig, kriminell auffällig, Spielernatur, Prostituierte/Stricher, Einzelgänger usw.)

• Auffälliges Verhalten des Opfers (z.B. abstoßendes Verhalten, auffälliger Tages- oder Wochenablauf).

Der für Beschuldigte vorgesehene Datenkatalog umfasst ebenfalls derart detaillierte und sensible Angaben.

Wenn es um schwerste Straftaten geht und derartige Informationen unter Umständen dazu beitragen können, die Verbrechen aufzuklären und weitere zu verhindern, wird man die mit den Detailangaben bezweckte Abbildung eines umfassenden Persönlichkeitsbildes nicht grundsätzlich ablehnen können. Wir haben uns allerdings dagegen gewandt, daß auch die Personalien der so beschriebenen Opfer in der Datei erfaßt werden. Dies ist bisher vorgesehen, wenn das Opfer seine Einwilligung erteilt. Eine Einwilligung enthebt die Polizei jedoch nicht von der Verpflichtung, die Speicherung personenbezogener Daten auf das erforderliche Maß zu beschränken. Für die Zwecke der Fallanalyse durch automatisierte Auswertung von ViCLAS sind die Personalien der Opfer nicht erforderlich. Wenn sich im Einzelfall aufgrund der Analyseergebnisse die Notwendigkeit herausstellen sollte, mit den Opfern Kontakt aufzunehmen, hat die ermittlungsführende Dienststelle diese Möglichkeit auch ohne Speicherung der Personalien in ViCLAS aufgrund ihrer sonstigen Unterlagen zum Fall. Eine personenbezogene Abfragemöglichkeit für alle angeschlossenen Polizeidienststellen wäre dagegen unvertretbar. Das Landeskriminalamt Hamburg teilt unsere Auffassung, daß die Personalien von Opfern für die Dateizwecke nicht erforderlich sind und setzt sich gegenüber dem Bundeskriminalamt für einen Verzicht auf die vorgesehene Speicherung mit Einwilligung ein.

Auch bei Beschuldigten rechtfertigt das hochrangige Interesse an der Verhinderung und Aufklärung etwaiger weiterer Straftaten nicht jeden Eingriff. Da die Dateiführung auf die Erstellung eines automatisiert auszuwertenden Persönlichkeitsbildes abzielt, müßte eingehend geprüft und begründet werden, ob eine personenbezogene Erfassung in ViCLAS zu den Analysezwecken zwingend ist. Das Landeskriminalamt Hamburg hält die Speicherung von Personalien über Beschuldigte für unverzichtbar, damit andere Dienststellen im Falle eines künftigen Verdachts feststellen können, ob der Betroffene bereits wegen einer ähnlichen Tat in Erscheinung getreten und wie er hierbei vorgegangen ist. Bei Angaben zum Lebensstil soll stets auf den unmittelbaren Bezug zur Anlaßtat geachtet werden. Weitestgehend verzichten will das Landeskriminalamt auf die Speicherung von Personen, gegen die kein konkreter Tatverdacht sondern nur die Annahme vorliegt, sie würden künftig Straftaten begehen. Hier gibt es keine Anlaßtat, die eine Abgrenzung ermöglicht zwischen „harten“ im Ermittlungsverfahren überprüften Daten und „weichen“ Daten, die sonstige Lebensumstände betreffen.

Die Verarbeitungsbedingungen für ViCLAS-Speicherungen müßten stärker konkretisiert werden, als dies bisher vorgesehen ist. Eine Kombination von Einzelangaben über die Lebensverhältnisse kann auf zahlreiche Personen zutreffen und besagt noch nichts über einen Tatverdacht. Wir haben daher gefordert, daß Dateiauswertungen immer die Verwendung „harter“, d.h. bei den Ermittlungen überprüfter tatbezogener Kriterien erfordern. Die „weichen“ Daten zum Lebensstil von Personen können dann diese Angaben ergänzen, dürfen aber nicht allein als Auswertungskriterien benutzt werden. Das Landeskriminalamt teilt diese Auffassung, schon weil die ausschließliche Verwendung „weicher“ Daten nicht zu verwertbaren Rechercheergebnissen führt. Es wird mit dem Bundeskriminalamt erörtern, ob eine entsprechende programmtechnische Eingrenzung möglich ist.

13.3 DNA-Datei

Molekulargenetische Untersuchungen zur Identitätsfeststellung in künftigen Strafverfahren setzen richterliche Anordnungen voraus. Einwilligungen der Betroffenen sind hierfür ungeeignet. Die Begründung der Annahme, gegen die Betroffenen würden auch künftig Strafverfahren zu führen sein und hierfür sei die Speicherung des DNA-Profils erforderlich, muß eingehender als bisher erfolgen.

Nachdem beim Bundeskriminalamt im April 1998 eine bundesweite Datei zur Speicherung der Ergebnisse molekulargenetischer Untersuchungen eingerichtet wurde, sind die rechtlichen Voraussetzungen für diese Datenverarbeitung geschaffen worden. Zweck der Dateispeicherungen ist es, am Tatort aufgefundene Spuren von Körperzellen mit den gespeicherten DNA-Profilen abzugleichen, um festzustellen, ob eine bereits früher in Erscheinung getretene Person als Täter in Betracht kommt. Gespeichert werden sollen auch Spuren von nicht aufgeklärten Fällen, um sie später erfassten DNA-Profilen zuordnen zu können. §81g Strafprozeßordnung (StPO) erlaubt nunmehr, daß zur Identifizierung in künftigen Strafverfahren von Beschuldigten Körperzellen entnommen und zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersucht werden.

Darüber hinaus wird durch §2 DNA-Identitätsfeststellungsgesetz außerhalb der StPO die molekulargenetische Untersuchung und Dateispeicherung auch bei Personen zugelassen, die bereits wegen einer der genannten Straftaten verurteilt sind, oder bei denen die Verurteilung mangels Schuldfähigkeit unterblieben ist. Die Untersuchung ist möglich, solange die entsprechenden Eintragungen im Bundeszentralregister oder Erziehungsregister noch nicht getilgt sind.

Voraussetzung ist jeweils, daß die Person einer Straftat von erheblicher Bedeutung, insbesondere eines Verbrechens oder eines Vergehens gegen die sexuelle Selbstbestimmung, einer gefährlichen Körperverletzung, eines Diebstahls in besonders schwerem Fall oder einer Erpressung verdächtig ist. Während die Entnahme von Körperzellen nach §81a StPO auch aufgrund einer Einwilligung des Betroffenen erfolgen kann und nur im Fall der Verweigerung richterlich angeordnet werden muß, schreibt §81f StPO für die molekulargenetische Untersuchung ausnahmslos eine richterliche Anordnung vor.

Im September 1999 hatte das Landeskriminalamt 57 DNA-Profile von Beschuldigten oder Verurteilten gespeichert und 5 Spuren aus Unbekanntfällen. Wir haben diese Speicherungen überprüft. In Fällen, in denen die Untersuchung vor dem Frühjahr 1999 durchgeführt worden war, gab es regelmäßig keine richterlichen Anordnungen. Vielmehr waren die Untersuchungen aufgrund von Einwilligungen durchgeführt worden. Diese Verfahrensweise war von der Justizbehörde damit begründet worden, daß bei Strafgefangenen, die kurz vor der Entlassung standen, zügig Untersuchungen durchgeführt werden sollten. Man befürchtete, mit richterlichen Anordnungen zu spät zu kommen.

Wir haben starke Bedenken gegen diese Verfahrensweise vorgebracht, diese im Ergebnis jedoch zurückgestellt, weil es sich nur um eine Übergangslösung handelte. Die ursprünglich angedachten ungeeigneten Texte für die Einwilligungserklärungen wurden zur Verdeutlichung des Zwecks der Speicherungen, des Verfahrensablaufs und der Widerrufsmöglichkeit verbessert.

Maßgeblich dafür, daß wir die Untersuchungen ohne richterliche Anordnung nicht gemäß §25 HmbDSG beanstandet haben, war letztlich, daß ab Frühjahr 1999 molekulargenetische Untersuchungen ausschließlich aufgrund richterlicher Anordnung durchgeführt wurden. Die inzwischen erlassene Fachanweisung des Landeskriminalamtes schreibt dies vor. Das Formular zur Einwilligung in die Entnahme der Körperzellen weist ausdrücklich darauf hin, daß die freiwillige Probeentnahme noch nicht bedeutet, daß sie auch untersucht wird, sondern hierüber allein der zuständige Richter entscheidet.

Nachdem diese Frage somit geklärt erschien, trat im Herbst 1999 eine neue Situation ein. Mehrere Abteilungen des Amtsgerichts Hamburg lehnten die Anordnung der Untersuchung ab mit der Begründung, die Betroffenen hätten eingewilligt. Eine Große Strafkammer des Landgerichts bestätigte diese Auffassung. Wir haben gegenüber der Justizbehörde kritisiert, daß trotz der inzwischen vereinbarten Regularien überhaupt erneut Einwilligungserklärungen eingeholt wurden. Hierzu ist es gekommen, nachdem die zuständigen Richter die Betroffenen, die sich in Strafhaft befanden, ordnungsgemäß angehört haben. Obwohl in den richterlichen Anhörungen nicht danach gefragt war, ob die Betroffenen einwilligten, wurde z.B. einem Betroffenen ein vom Strafvollzugsamt vorgefertigtes Antwortschreiben mit der Erklärung präsentiert, „Ich bin mit der Entnahme einer Speichel- hilfsweise einer Blutprobe, sowie deren molekulargenetischen Untersuchung zur Feststellung des DNA-Identifizierungsmuster zum Zweck der Identitätsfeststellung einverstanden“ und von ihm unterschrieben.

Wir haben deutlich gemacht, daß keine Einwände dagegen bestünden, wenn seitens des Strafvollzugsamtes bei gerichtlichen Anhörungen das von der Polizei verwendete Einwilligungsformular zur Probeentnahme ausgehändigt würde, um den Betroffenen den Verfahrensgang mit richterlicher Anordnung der molekulargenetischen Untersuchung der Probe zu verdeutlichen. Eine Verwendung von Erklärungstexten durch das Strafvollzugsamt oder andere beteiligte Behörden aus Anlaß gerichtlicher Anhörungen, die sich auf ein „Einverständnis“ zur molekulargenetischen Untersuchung beziehen, ist dagegen zumindest solange auszuschließen, wie es keine gefestigte Rechtsprechung gibt, die die Einwilligung als Grundlage der Untersuchung bejaht.

Die Staatsanwaltschaft hat angekündigt, durch Beschwerden gegen weitere Entscheidungen des Amtsgerichts, die eine Anordnung wegen erteilter Einwilligung ablehnen, in Erfahrung zu bringen, ob sich die Rechtsprechung in diesem Sinne verfestigt. Wir haben den zuständigen Abteilungen des Amtsgerichts die Entschließung der Konferenz der Datenschutzbeauftragten vom 7./8. Oktober 1999 zur Kenntnis gegeben, worin die mangelnde Eignung von Einwilligungserklärungen zur molekulargenetischen Untersuchung insbesondere bei Strafgefangenen hervorgehoben wird.

Eine wirksame Einwilligung setzt voraus, daß sie frei von psychischem Zwang erfolgt (§5 Abs. 3 HmbDSG; vgl. auch 14. TB, 1.2). 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. Ferner verlangt §5 Abs. 2 HmbDSG, daß über Gegenstand, Inhalt und Umfang der erlaubten Datenverarbeitung klar und verständlich informiert wird. Angesichts der komplexen Verarbeitungsbedingungen der DNA-Datei ist eine derart umfassende Aufklärung kaum möglich. Die oben zitierte im Strafvollzug verwendete Erklärung macht dies anschaulich. Wichtig ist auch der Hinweis auf die Möglichkeit zum Widerruf der Einwilligung.

Nicht zuletzt die gesetzlichen Voraussetzungen für Speicherungen in der DNA-Datei sprechen gegen die Einwilligungslösung. Eine Zustimmung zur molekulargenetischen Untersuchung zur Identitätsfeststellung in künftigen Strafverfahren verlangt von den Betroffenen die Einsicht ab, sie würden erneut straffällig werden und stimmten einer Verwendung ihres DNA-Profils zu ihrer Überführung zu. Es liegt auf der Hand, daß diese Annahme realitätsfern ist. Der Gesetzgeber hat vielmehr die Prüfung und Entscheidung, ob die Negativprognose gegen den Betroffenen die DNA-Untersuchung und Dateispeicherung rechtfertigt, ausdrücklich dem Richter übertragen. In gerichtlichen Entscheidungen außerhalb Hamburgs wird dieser Gesichtspunkt überzeugend hervorgehoben. Demgemäß sind von Gerichten Untersuchungsanordnungen abgelehnt worden, weil die Negativprognose nicht ausreichte. Andererseits sind Anordnungen ergangen, in denen sich das Gericht ausführlich mit der Negativprognose befasst hat und die Einwilligung des Betroffenen nicht als Grundlage ausreichen ließ.

Unsere Prüfung der Dateispeicherungen hat gerade auch in diesem Zusammenhang Defizite deutlich gemacht. Die Fachanweisung des Landeskriminalamtes sieht zwar eine Vielzahl von Kriterien vor für die Begründung, der Betroffene werde erneut straffällig werden und das DNA-Profil sei zu seiner künftigen Überführung erforderlich. Die Polizei dokumentiert ihre diesbezügliche Beurteilung allerdings nur in solchen Fällen, in denen bereits ein DNA-Profil aus dem Ermittlungsverfahren vorliegt, das ohne weitere richterliche Anordnung gespeichert werden soll. In den übrigen Fällen verweist sie darauf, daß primär die Staatsanwaltschaft für die Stellung der Negativprognose zuständig sei. In den Anträgen der Staatsanwaltschaft für die richterliche Anordnung findet sich hierzu allerdings nichts. Es wird vielmehr nur formularmäßig und lapidar erklärt, die gesetzlichen Voraussetzungen lägen vor. Auch in den früheren Fällen, in denen Einwilligungen eingeholt wurden, gab es gegenüber den Betroffenen keine Darlegung, aus welchen Gründen man einen Rückfall befürchtete.

Bei den bisher in der Datei erfaßten Fällen waren diese Mängel im Ergebnis noch hinnehmbar. Es handelte sich um Tötungsdelikte, schwere Sexualstraftaten oder Serieneinbrüche, bei denen bereits nach der Art der bisher begangen Taten die Negativprognose nachvollziehbar war. Die Polizei beabsichtigt, zukünftig auch in anderen Deliktsbereichen, bei denen sich die Negativprognose nicht vergleichbar aufdrängt, DNA-Untersuchungen und Dateispeicherungen durchzuführen. Dann muß die Annahme, daß gegen die Betroffenen künftig erneut Strafverfahren zu führen sind und hierzu die Speicherung des DNA-Profils erforderlich ist, besser als bisher begründet und nachvollziehbar dokumentiert werden.

13.4 Straflosigkeit des Zugriffs auf offenkundige Daten?

Der unbefugte Abruf personenbezogener Daten, für die rechtlich geregelte Zugangsvoraussetzungen gelten, muß weiterhin strafbar bleiben.

Das im folgenden beschriebene Problem betrifft nicht allein die Polizei. Da die Fälle, die zu dem Problem geführt haben, allerdings jeweils Polizeibeamte betrafen, wird es an dieser Stelle behandelt.

In zwei vom Hanseatischen Oberlandesgericht (RDV 1998, 216) und vom Bayerischen Obersten Landesgericht (RDV 1999, 124) entschiedenen Fällen hatten die Beamten im Interesse einer Privatdetektei bzw. eines privaten Sicherheitsdienstes ohne dienstlichen Grund Daten aus dem Fahrzeugregister beim Kraftfahrt-Bundesamt abgerufen, im hamburger Fall auch an die Detektei weitergegeben. Die Daten beim Kraftfahrt-Bundesamt unterliegen den Regelungen des Bundesdatenschutzgesetzes. §43 Abs. 1 Nr. 3 BDSG lautet:

> Wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind, ... abruft oder sich oder einem anderen aus Dateien verschafft, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Die Gerichte haben die Beamten freigesprochen. Sie haben ihre Entscheidungen damit begründet, die Daten im Fahrzeugregister beim Kraftfahrt-Bundesamt seien offenkundig. Diese Offenkundigkeit ergebe sich daraus, daß die Daten nach den Regelungen des Straßenverkehrsgesetzes „bei Vorliegen bestimmter im einzelnen geregelter Voraussetzungen an jedermann übermittelt werden, vor allem wenn sie zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt werden“ (so das Bayerische Oberste Landesgericht). Der Kreis der Personen, die danach möglicherweise Zugang zu den Daten bekommen könnten, sei nicht überschaubar, was die Daten zu offenkundigen Daten mache. In der Folge haben sich das Amts- und das Landgericht Hamburg in anderen Strafverfahren dieser Auffassung angeschlossen.

Wir halten die Auslegungen des Merkmals der Offenkundigkeit durch die Gerichte für unzutreffend. Als offenkundige Daten sind solche Daten anzusehen, für die es keine rechtlich geregelten Zugangsvoraussetzungen gibt: also z.B. Informationen aus den Medien, aus dem Telefonbuch oder auch aus dem Handelsregister. Wenn dagegen der Gesetzgeber – wie für das Fahrzeugregister – ausdrückliche Voraussetzungen normiert, die erfüllt sein müssen, um die Informationen zu erhalten, hat eben nicht „jedermann“ Zugang, sondern nur diejenigen, die die gesetzlichen Bedingungen erfüllen.

Das Hanseatische Oberlandesgericht verkennt in seiner Entscheidung sogar, welche gesetzlichen Voraussetzungen nach dem Straßenverkehrsgesetz gelten. Die Gerichte setzen sich überhaupt nicht mit der Frage auseinander, ob die gesetzlichen Voraussetzungen für Informationen an Privatpersonen in den Einzelfällen vorlagen. Dabei hätte sich diese Frage aufdrängen müssen: die Privatdetekteien sind doch nur deshalb an die Polizeibeamten herangetreten und haben deren dienstliche Möglichkeit zum Datenabruf ausgenutzt, weil sie selbst keine Auskunft aus dem Fahrzeugregister erhalten hätten. Wie man in solchen Fällen von Offenkundigkeit ausgehen kann, ist unerfindlich.

Nach der Auslegung der Gerichte würde es entweder nur strikte Geheimnisse geben, die keiner Privatperson offenbart werden dürfen, oder offenkundige Daten. Denn praktisch alle Vorschriften über die Verarbeitung personenbezogener Daten lassen unter bestimmten, teils engeren, teils weiteren Voraussetzungen Übermittlungen an Privatpersonen zu. Für die Anwendung der Straf- oder Bußgeldvorschriften gegen unbefugte Datenabrufe nach dem Datenschutzrecht gäbe es dann keinen Anwendungsbereich mehr.

Da jedoch nach den bisherigen Erfahrungen damit zu rechnen ist, daß sich auch weitere Gerichte unbesehen dieser Auslegung anschließen, haben wir in den laufenden Gesetzgebungsverfahren zur Änderung des Bundesdatenschutzgesetzes und des Hamburgischen Datenschutzgesetzes eine Klarstellung vorgeschlagen. Statt der bisherigen Formulierung sollte sich die Strafbarkeit auf den unbefugten Abruf solcher Daten beziehen, „die nicht jeder Person ohne rechtlich geregelte Voraussetzung zugänglich sind“. Damit würden die bisherigen nicht strafwürdigen Fälle des Umgangs mit Daten, die ohne weiteres zugänglich sind, weiterhin ausgeschlossen. Die Mißverständnisse, die sich aus dem bisherigen Merkmal der „Offenkundigkeit“ ergeben haben, würden dagegen vermieden.

Eine Beibehaltung der Strafbarkeit des unbefugten Abrufs aus Dateien ist dringend erforderlich. Nach Presseberichten sollen Polizeibeamte in Hamburg Informationen aus dem Fahrzeugregister abgerufen und an organisierte Autoschieberbanden weitergegeben haben. Die zahlreichen Bemühungen zur Bekämpfung der Korruption und organisierten Kriminalität würden unterlaufen, wenn derartige Abrufe künftig nach Auslegung der Gerichte straflos sein sollen.

13.5 Sonstiges

Wir haben im Bereich der Polizei Prüfungen und Beratungen durchgeführt und Stellungnahmen abgegeben zu Fragen der Datenverarbeitung bei

- Sexual- und Wirtschaftsstraftaten
- Korruptionsdelikten und Geldwäsche
- der zentralen Beschwerdestelle
- Forschungsvorhaben zu jugendlichen Intensivtätern.

14. Staatsanwaltschaft

14.1 Automation bei der Staatsanwaltschaft

Zu den datenschutzrechtlichen Forderungen nach Begrenzung der Zugriffsrechte und zur Protokollierung von Zugriffen sind Kompromisslösungen erreicht worden. Beim weiteren Ausbau des automatisierten Verfahrens der Staatsanwaltschaft sind Fragen zum Datenaustausch mit der Polizei und dem zentralen staatsanwaltschaftlichen Verfahrensregister weiter zu klären.

Das gemeinsam mit den Ländern Schleswig-Holstein, Brandenburg und Hessen entwickelte Verfahren „Mehrländer-Staatsanwaltschafts-Automation“ (MESTA) ist 1999 schrittweise weiter ausgebaut worden. Neben den Funktionen der Zentralkartei sind eine Reihe von Geschäftsstellen an MESTA angeschlossen worden. Neu eingehende Vorgänge werden in diesen Geschäftsstellen nunmehr unmittelbar in MESTA mit Angaben zum Aktenzeichen der Staatsanwaltschaft und der Polizei, zu Art, Ort und Zeitpunkt der Straftat erfaßt. Die Personalien der Beschuldigten werden automatisch mit dem vorhandenen Bestand abgeglichen und übernommen, wenn keine Abweichungen bekannt sind.

Zur lange offen gebliebenen Frage der Zugriffsrechte wurde nunmehr folgende Regelung getroffen:

Die Geschäftsstellenmitarbeiter können grundsätzlich nur auf Verfahren mit Aktenzeichen der eigenen bzw. einer Abteilung mit gleicher Aufgabenstellung zugreifen. Eine Auskunft über Verfahren anderer Abteilungen ist für Geschäftsstellenmitarbeiter allerdings dann möglich, wenn zu dem jeweiligen Beschuldigten auch ein Verfahren aus der eigenen Abteilung vorliegt. Der Zugriff der Dezernenten (Staatsanwälte) unterliegt diesen Beschränkungen nicht. Die beschriebenen Vorkehrungen erfüllen zwar nicht unsere ursprünglichen Forderungen zur Begrenzung der Zugriffsrechte (vgl. 16.TB, 16.1), insbesondere wenn es um Daten nicht beschuldigter Personen (z.B. Anzeigenerstatter) geht. Als Mindeststandard gewährleisten sie aber immerhin, daß MESTA nicht wie ein völlig offenes System ohne jede Binnendifferenzierung betrieben wird, und sind somit als Kompromiß akzeptabel.

Bestimmte Systemaktivitäten z.B. die Anmeldung und Datenänderungen (mit Eintragung des Status vor und nach der Änderung) werden protokolliert. Wir haben für den Umgang mit dieser Protokolldatei Regularien über die zugriffsberechtigten Mitarbeiter, die Anlässe und das Verfahren für Protokollauswertungen und die Länge der Aufbewahrung gefordert und hierzu Vorschläge unterbreitet. Bei Redaktionsschluß lag uns jedoch noch keine Reaktion hierauf vor. Zur weitergehenden Forderung der Protokollierung lesender Zugriffe (vgl. 16. TB, 16.1) deutet sich ebenfalls ein Kompromiß an. In einer Bund-Länder-Kommission sollen einheitliche Standards für staatsanwaltschaftliche Automationsverfahren vereinbart werden. Hamburg setzt sich dabei für eine stichprobenartige Protokollierung lesender Zugriffe ein. Ergebnisse der Bund-Länder-Kommission lagen bei Redaktionsschluss allerdings noch nicht vor.

Beim weiteren Ausbau von MESTA sollen insbesondere auch Schnittstellen zu anderen automatisierten Verfahren realisiert werden. Im Vordergrund steht dabei der Datenaustausch mit dem zentralen staatsanwaltschaftlichen Verfahrensregister (ZStV) und mit der Polizei.

Ein Datenaustausch zwischen dem staatsanwaltschaftlichen Verfahren MESTA und dem polizeilichen Verfahren COMVOR ist seit langem geplant und in den Grundzügen mit uns abgestimmt. Weil jedoch auf beiden Seiten bisher die technischen Voraussetzungen fehlten, sind die Pläne noch nicht realisiert worden. Hiermit ist im kommenden Jahr zu rechnen.

Im ZStV werden die Verfahren sämtlicher Staatsanwaltschaften zentral registriert (vgl. 13. TB, 19.1.1). Die Daten müssen also bei der Verfahrenseinleitung nicht nur im örtlichen System MESTA erfasst werden, sondern von dort an das ZStV übertragen werden. Hamburg leitet zur Zeit noch keine Daten an das ZStV weiter; vielmehr wird der Datenverkehr mit dem ZStV in Schleswig-Holstein stellvertretend für die übrigen MESTA-Länder im Pilotbetrieb getestet. Zu klären sind insbesondere die folgenden Fragen:

Nach den für das ZStV geltenden Regelungen sind auch die Verfahrenserledigungen bei der Staatsanwaltschaft und bei Gericht nebst Angabe der gesetzlichen Vorschriften einzutragen. Wenn eine Verurteilung erfolgt, die im Bundeszentralregister einzutragen ist, bewirkt diese Eintragung der Entscheidung die automatische Löschung im ZStV.

Schwieriger ist allerdings der Ablauf bei Verfahrenserledigungen, die nicht im BZR eingetragen werden (Einstellungen bei der Staatsanwaltschaft oder bei Gericht, Freisprüche). Die Eintragung dieser Erledigungen ist wesentlich für die Löschung nach Fristablauf im ZStV. In Schleswig-Holstein erfolgen die Erledigungsmitteilungen automatisiert, sobald sie in MESTA eingetragen werden, ohne daß ein besonderer Bearbeitungsschritt erforderlich wäre. Diese Verfahrensweise dürfte sicher und mit dem geringsten Aufwand verbunden sein. Wir haben der Staatsanwaltschaft Hamburg empfohlen, ebenso zu verfahren.

Hinzu kommt ein weiteres Problem: Gesetzlich ist vorgeschrieben, daß im ZStV die Tatvorwürfe mit Angaben zum verletzten Straftatbestand eingetragen werden. In Hamburg besteht die Praxis, daß die Staatsanwaltschaft bei der Ersteintragung von Verfahren in MESTA die rechtliche Bewertung der Polizei unbesehen übernimmt. Demgemäß würden auch bei der Mitteilung der Verfahrenseinleitung an das ZStV zunächst nur die polizeilichen Bewertungen eingetragen. Nicht selten ändert sich jedoch die rechtliche Bewertung, für die im Ermittlungsverfahren primär die Staatsanwaltschaft zuständig ist, im Zuge der weiteren Ermittlungen (z.B. polizeilicher Verdacht auf Totschlag, Anklageerhebung durch die StA wegen fahrlässiger Tötung). Es muß daher eine Berichtigung der ursprünglichen Eintragung im ZStV erfolgen. In Schleswig-Holstein erfolgt zunächst eine Vorkontrolle beim Eingang der Daten von der Polizei. Im weiteren Verfahren wird die rechtliche Bewertung von den zuständigen Dezernenten überprüft und erforderlichenfalls eine Korrektur veranlaßt. Die Übernahme dieser Verfahrensweise in Hamburg wird insbesondere davon abhängen, wie die Schnittstelle mit der Polizei ausgestaltet wird.

Ein Fortschritt ist bei der Frage der Verschlüsselung des Datenverkehrs zwischen den dezentralen Staatsanwaltschaften und dem ZStV erreicht worden. Die beteiligten Justizverwaltungen haben ihre frühere Ablehnung der Verschlüsselung inzwischen aufgegeben. Nunmehr sollen verschiedene Verschlüsselungsverfahren auf ihre Eignung getestet werden, so daß zu einem späteren Zeitpunkt der Datenaustausch generell verschlüsselt wird.

14.2 Berichtspflichten über Abhörmaßnahmen

Berichte über Abhörmaßnahmen müssen insbesondere auch Aufschluß über Personengruppen geben, deren Gespräche ohne Tatverdacht überwacht wurden.

Mit der Änderung von Art. 13 Grundgesetz (GG) zum Abhören von Wohnungen (sog. Lauschangriff) wurde auch ein Verfahren zur parlamentarischen Kontrolle dieser weitreichenden Grundrechtseingriffe eingeführt. Art 13. Abs. 6 Satz 1 GG sieht vor, daß die Bundesregierung den Deutschen Bundestag jährlich über Abhörmaßnahmen in Wohnungen zur Strafverfolgung und präventiv-polizeiliche Lauschangriffe durch Bundespolizeibehörden unterrichtet. Nach Art. 13 Abs. 6 Satz 3 GG gewährleisten die Länder eine gleichwertige Kontrolle.

Zu begrüßen ist, daß mit der Justiz- und der Innenbehörde in Hamburg rasch Übereinstimmung darüber erzielt werden konnte, daß die Berichte über Abhörmaßnahmen gegenüber der Bürgerschaft die Maßnahmen nach der Strafprozeßordnung und die nach dem Gesetz über die Datenverarbeitung der Polizei gleichermaßen umfassen sollen. Damit wird eine umfassende Berichterstattung und parlamentarische Kontrolle über verdeckte Datenerhebungsmaßnahmen aus Wohnungen in Hamburg sichergestellt. Eine Begrenzung der Berichtspflichten auf die landesgesetzlich geregelten polizeilichen Befugnisse, wie sie in anderen Bundesländern vorgesehen ist, würde dagegen zu einem unvollständigen Bild führen. Die Berichte sollen ohne Personenbezug erfolgen, so daß die Bürgerschaft die Möglichkeit hat, sie öffentlich zu erörtern. Aufgrund dieser parlamentarischen Behandlung besteht die Chance, die Auswirkungen der nunmehr grundgesetzlich zugelassenen Eingriffe auf die Rechte der Betroffen abzuschätzen. Ein entsprechender Gesetzentwurf ist inzwischen in der Bürgerschaft eingebracht worden.

Das von den Justizministerien der Länder vereinbarte Erhebungsraster, das als Grundlage für die Berichterstattung gegenüber dem Deutschen Bundestag dienen soll, ist unzulänglich. Danach ist lediglich vorgesehen, die Gesamtzahl der von einer Abhöranordnung betroffenen Personen (Beschuldigte und Wohnungsinhaber) zu erfassen. Weitere Personen, die in der Anordnung nicht benannt werden, und die sich „lediglich zufällig“ in der überwachten Wohnung aufgehalten haben, sollen nicht zum Kreis der Betroffenen zählen und daher in den Berichten nicht erwähnt werden. Wir haben uns gegen diese Festlegungen gewandt.

Die Regelung über die Berichtspflichten in §100e Abs.1 StPO verlangt Angaben über Anlaß, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen und über die Benachrichtigung der Beteiligten. Der Umfang der Maßnahme kann aber nicht allein aufgrund der gerichtlichen Anordnung sondern erst aufgrund der tatsächlichen Durchführung benannt werden. Daher kann nicht allein auf die Anordnung Bezug genommen werden, wenn es um Erkenntnisse über den Umfang einer Abhörmaßnahme geht.

Es trifft zwar zu, daß in allen Fällen neben den Beschuldigten auch die Wohnungsinhaber betroffen sind. Falsch ist dagegen die Annahme, daß weitere Personen, die sich in der überwachten Wohnung aufhalten, nicht zum Kreis der Betroffenen gehören. Dies gilt nur dann, wenn ihre Gespräche nicht überwacht wurden. Wenn dies aber geschieht, richtet sich die Maßnahme zweifellos gegen sämtliche an den Gesprächen beteiligten Personen. Die Frage, aus welchen Gründen sich jemand in der Wohnung aufhält, ändert nichts an der Betroffenheit im rechtlichen Sinne. Es ist Zweck der Berichtspflichten, Erkenntnisse darüber zu gewinnen, welche Personenkreise tatsächlich in die Abhörmaßnahme einbezogen wurden. Im Hinblick auf die betroffenen Grundrechte macht es einen wesentlichen Unterschied, ob sich die Maßnahme allein auf Gespräche zwischen Beschuldigten bezogen hat, oder ob auch Dritte (z.B. unverdächtige Familienangehörige, Bekannte, Besucher) überwacht wurden. Die gesetzlich geforderten Berichte würden verzerrt, wenn ausgerechnet der Personenkreis der unverdächtigen Gesprächsteilnehmer, in deren Rechte am stärksten eingriffen wird, ausgeblendet würde. Wenn die exakte Zahl der in Abhörmaßnahmen einbezogenen Personen nur mit Schwierigkeiten zu ermitteln ist, reichen für den Zweck der Berichte auch Schätzungen aus.

Die Justizbehörde hat zwar eingeräumt, daß es für die Evaluation der Maßnahmen von großem Interesse wäre, wie viele Personen insgesamt Grundrechtseinbußen durch eine Abhörmaßnahme erlitten. Sie wollte der bundeseinheitlichen Verfahrensweise jedoch nicht entgegentreten, hat allerdings angekündigt, daß die Daten über weitere beteiligte Gesprächspartner erhoben werden sollen, falls die staatsanwaltschaftliche Praxis hierzu Möglichkeiten sieht. Bisher ist die Frage theoretisch geblieben, weil es keine Wohnungsüberwachung aufgrund der Neuregelung durch Art. 13 Abs. 3 GG und §100c Abs. 1 Nr. 2 StPO in Hamburg gegeben hat.

Eine vergleichbare Schwierigkeit gibt es bei der Frage, wie viele Personen von Telefonüberwachungen betroffen sind. Auch hier werden bisher nur die in der Anordnung genannten Beschuldigten und die Inhaber der von ihnen benutzten Anschlüsse gezählt. Auf Anfragen – z.B. von Bürgerschaftsabgeordneten – , wie viele Personen insgesamt in die Überwachung einbezogen wurden, können die Behörden dagegen keine Auskunft geben, weil sie bisher nicht gezählt werden.

Diesem Erfahrungsdefizit soll ein vom Bundesministerium der Justiz in Auftrag gegebenes Forschungsvorhaben über die Praxis und Effizienz der Telefonüberwachung abhelfen. Die Datenschutzbeauftragten des Bundes und der Länder haben das Forschungsvorhaben begrüßt und werden sich an der Lösung der datenschutzrechtlichen Fragen, die sich z.B. bei der Einsichtnahme in Akten zu Telefonüberwachungen stellen, konstruktiv beteiligen. Die über das Forschungsprojekt hinausgehende Forderung einer umfassenden Rechtstatsachensammlung über Eingriffsbefugnisse der Sicherheitsbehörden (vgl. 13. TB, 17.4.1; 14.TB, 15.7), die sich insbesondere auch auf die Auswirkungen der Eingriffe auf Unverdächtige beziehen muß, werden wir gemeinsam mit den übrigen Datenschutzbeauftragten weiterverfolgen.

14.3 Europaweite Telefonüberwachung?

Grenzüberschreitende Maßnahmen zur Überwachung der Telekommunikation im Rahmen der Europäischen Union dürfen nur erfolgen, wenn die grundrechtlichen Sicherungen zum Schutz des Fernmeldegeheimnisses gewahrt bleiben.

Die Mitgliedstaaten der Europäischen Union streben die Verbesserung der Zusammenarbeit bei der Verfolgung von Straftaten an. Insbesondere soll die Gewährung von Rechtshilfe durch die Behörden eines Mitgliedstaates zur Strafverfolgung in einem anderen Mitgliedstaat erleichtert werden. Vorgesehen ist der Abschluß eines neuen Übereinkommens über die Rechtshilfe in Strafsachen, das die bisherigen Regelungen aus dem Jahr 1959 ergänzen soll.

Nach dem bisher bekannt gewordenen Entwurf für das Rechtshilfe-Übereinkommen sind zahlreiche Regelungen vorgesehen, die sich auf die Erhebung und weitere Verarbeitung personenbezogener Daten zur Strafverfolgung auswirken. So ist z.B. ein europaweiter Informationsaustausch ohne Ersuchen über Strafermittlungen vorgesehen, wie er nach deutschem Recht durch das Justizmitteilungsgesetz geregelt ist (15. TB, 17.1). Auch Vernehmungen per Video- oder Telefonkonferenz sollen ermöglicht werden (16. TB, 17.1). Verdeckte Ermittler können grenzüberschreitend eingesetzt werden.

Eingehende Bestimmungen sind ferner für die Überwachung des Telekommunikationsverkehrs geplant. Danach soll es künftig für alle EU-Staaten die Möglichkeit geben, Ersuchen zur Überwachung des Telekommunikationsverkehrs an andere Mitgliedstaaten zu richten. Aufgrund der Überwachung sollen der Telekommunikationsverkehr entweder unmittelbar an den ersuchenden Staat weitergeleitet oder Aufzeichnungen der Überwachung an den ersuchenden Staat übermittelt werden.

Bei der Überwachung von Personen auf Ersuchen anderer EU-Staaten kommt es wesentlich darauf an, ob auch das Recht des ersuchten Staates Anwendung findet, oder ob nur die Bedingungen gelten sollen, die für den ersuchenden Staat maßgeblich sind. Für Deutschland würde die erste Variante bedeuten, daß auch auf Anforderung anderer EU-Mitgliedstaaten der nach §100b StPO zuständige Richter prüft, ob ein hinreichend begründeter Tatverdacht auf eine der in §100a StPO genannten Straften vorliegt. Die zweite Variante würde dagegen dazu führen, daß es keiner Entscheidung des deutschen Richters bedarf und es von der Ausgestaltung des Rechts des jeweiligen anderen EU-Staates abhängt, ob überhaupt eine richterliche Prüfung und eine Begrenzung auf gesetzlich bestimmte Straftaten erfolgt. Die im Entwurf des Rechtshilfeübereinkommens vorgesehenen Bestimmungen sind insofern nicht eindeutig.

Völlig unklar bleibt in dem Entwurf auch, nach welchem Recht sich die weitere Verwendung der Ergebnisse von Überwachungsmaßnahmen richtet, die auf Ersuchen in anderen Mitgliedstaaten erhoben worden sind. Gelten die nach deutschem Recht in §100b StPO vorgesehenen Regelungen zur Zweckbindung und zur Vernichtung und die Benachrichtungspflichten nach §101 StPO, wenn die in Deutschland erhobenen Überwachungsergebnisse an die ersuchenden EU-Staaten unmittelbar weitergeleitet oder ihnen nach Aufzeichnung übermittelt werden? Umgekehrt stellt sich die Frage ebenso, wenn aufgrund einer Telefonüberwachung in einem anderen EU-Mitgliedstaat die Überwachungsergebnisse von deutschen Strafverfolgungsbehörden verwertet werden.

Das Bundesverfassungsgericht hat 1999 im Verfassungsbeschwerdeverfahren gegen die Befugnisse des Bundesnachrichtendienstes zur Überwachung des internationalen Fernmeldeverkehrs grundsätzliche Aussagen zur Geltung des Fernmeldegeheimnisses nach Art. 10 GG bei Auslandsberührung getroffen. Wir haben in diesem Verfahren sowohl schriftlich als auch in der mündlichen Verhandlung Stellung genommen. Das Gericht hat im zweiten Leitsatz der Entscheidung klargestellt, daß der räumliche Schutzumfang des Fernmeldegeheimnisses nicht auf das Inland beschränkt ist. Art. 10 GG kann vielmehr auch dann eingreifen, wenn eine im Ausland stattfindende Telekommunikation durch Erfassung und Auswertung im Inland hinreichend mit staatlichem Handeln verknüpft ist.

Danach kann kein Zweifel daran bestehen, daß bei Ersuchen deutscher Strafverfolgungsbehörden zur Telekommunikationsüberwachung im Ausland die gesetzlichen Voraussetzungen und Bindungen zum Schutz des Fernmeldegeheimnisses uneingeschränkt zu beachten sein werden. Insbesondere setzen von deutschen Strafverfolgungsbehörden veranlasste Abhörmaßnahmen im europäischen Ausland voraus, daß eine Katalogtat nach §100a StPO vorliegt, eine richterliche Anordnung erfolgt und die Zweckbindungsregelungen, Löschungs- und Benachrichtigungspflichten eingehalten werden.

Für den umgekehrten Fall einer von ausländischen Behörden veranlaßten Überwachungsmaßnahme in Deutschland darf das geplante Übereinkommen ebenfalls Grundrechtseingriffe nur unter Wahrung der genannten Schutzvorkehrungen zulassen.

Wir haben die Justizbehörde darauf hingewiesen, daß der bisherige Entwurf zahlreiche Unklarheiten zu diesen Fragen enthält. Der Entwurf soll im Amtsblatt der EU veröffentlicht werden, um den Diskussionstand einer breiteren Öffentlichkeit insbesondere auch zur Beratung im Europäischen Parlament zugänglich zu machen.

15. Justiz

15.1 Prüfung des Amtsgerichts Hamburg

Die Maßnahmen des Amtsgerichts zur Datensicherung entsprechen in mehrfacher Hinsicht nicht den gesetzlichen Anforderungen.

Im Januar und Februar 1999 führten wir eine umfangreiche Kontrolle beim Amtsgericht Hamburg durch. Prüfungsmaßstab war, ob die erforderlichen Maßnahmen zur Datensicherung getroffen und eingehalten werden. In die Kontrolle einbezogen wurden insbesondere das Familiengericht, das Vormundschaftsgericht sowie die Dezernate und Abteilungen für Strafsachen.

Wir stellten fest, daß Akten mit sensiblen personenbezogenen Daten in den Regalen der Geschäftsstellen unverschlossen aufbewahrt werden. Damit hat zumindest das Reinigungspersonal außerhalb der Geschäftszeiten ungehindert Zugang zu den Akten. Die offene Aufbewahrung halten wir jedenfalls im Bereich des Vormundschaftsgerichts für nicht vertretbar, da dort besonders schutzwürdige Daten, z.B. in Adoptions- und Betreuungssachen, verarbeitet werden. Wir konnten erreichen, daß für das Haushaltsjahr 2001 ein Sonderbedarf zur Ausstattung des Vormundschaftsgerichts mit zugriffssicherem Mobiliar angemeldet wurde.

Einen weiteren Schwerpunkt unserer Prüfung bildete die Heimarbeit von Schreibkräften, denen zu diesem Zweck neben den Tonbändern komplette Verfahrensakten nach Hause mitgegeben werden. Diese Praxis rechtfertigt das Amtsgericht mit dem Hinweis, daß beim Diktat häufig auf Blattzahlen der Akten verwiesen werde, z.B. wegen der Schreibweise von Familiennamen und Fachbegriffen oder zur wörtlichen Wiedergabe längerer Textpassagen. Unseren Vorschlag, den Tonbändern Karteikarten mit handschriftlichen Diktathilfen oder Ablichtungen der jeweils benötigten Seiten aus der Akte beizufügen, lehnt das Amtsgericht mit der Begründung ab, dieses Verfahren sei zu aufwendig und könne weder Richtern noch Rechtspflegern verbindlich vorgeschrieben werden.

Demgegenüber sind wir der Auffassung, daß eine datenschutzgerechte Gestaltung der Heimarbeit von Schreibkräften die Richter und Rechtspfleger nicht in ihrer Unabhängigkeit berührt, sondern lediglich die äußere Form der Aufgabenwahrnehmung regelt. Wir legten dem Amtsgericht nahe, zumindest besonders sensible Vorgänge, z.B. Adoptions- und Betreuungsakten sowie Personalsachen, von der häuslichen Bearbeitung auszuschließen. Das Amtsgericht hat uns mitgeteilt, daß generell eine Reduzierung der Heimarbeit angestrebt werde.

Positiv aufgenommen hat das Amtsgericht unseren Vorschlag, telefonische Auskünfte zum Verfahren mit personenbezogenem Inhalt gegenüber Dritten besonders zurückhaltend zu erteilen und die Entsorgung personenbezogener Unterlagen durch Shredder (neben den bereits aufgestellten Containern) zu unterstützen. Die rechtzeitige Abholung und Leerung der Container durch das hiermit beauftragte Unternehmen müssen vom Amtsgericht sichergestellt und überwacht werden. Ferner hat das Amtsgericht als Ergebnis unserer Prüfung veranlaßt, daß die automatisierte Speicherung von Haftbefehlsdaten durch die Strafdezernate einheitlich auf höchstens einen Monat begrenzt wird.

Als besonders gravierendes Problem hat sich erwiesen, daß das Amtsgericht sensible personenbezogene Unterlagen offen ohne Verwendung von Umschlägen durch den Behörden – Transport – Service (BTS) der Finanzbehörde befördern läßt (vgl. hierzu näher unter 18.).

16. Strafvollzug

16.1 Prüfung des Strafvollzugsamtes

Datenpflege und Datensicherheit beim Strafvollzugsamt konnten deutlich verbessert werden.

Im Mai 1999 führten wir eine umfangreiche Kontrolle beim Strafvollzugsamt durch. Gegenstand der Prüfung waren das Programm „Sicherheitsangelegenheiten“, die Aufbewahrung von Einzelvorgängen über Gefangene und Besucher in der Registratur der Justizbehörde sowie die Sicherheitsüberprüfungen von Praktikanten, ehrenamtlichen Vollzugshelfern, Drogenberatern, Handwerkern und Reinigungskräften durch das Strafvollzugsamt.

Hinsichtlich des Programms „Sicherheitsangelegenheiten“ und der darin enthaltenen automatisierten Dateien haben wir detaillierte Anforderungen zur Datensicherung sowie zur Festlegung und Überwachung von Prüffristen für personenbezogene Daten formuliert. Das Strafvollzugsamt hat diesen Anforderungen zwischenzeitlich entsprochen. Die von uns vorgeschlagene Vereinheitlichung und Verkürzung der Aufbewahrungsfristen für Einzelvorgänge hat der Leiter der Registratur zugesagt.

Die Durchführung von Sicherheitsüberprüfungen beim Strafvollzugsamt gab nur in geringem Maße Anlaß zur Kritik. Der Grundsatz der Datensparsamkeit und Datenvermeidung wird bei der Dokumentation von Sicherheitsüberprüfungen weitgehend beachtet. Unsere Empfehlung, bei Anfragen an Staatsanwaltschaften und andere Stellen eigene Erkenntnisse des Strafvollzugsamtes über die Betroffenen künftig nur noch im jeweils erforderlichen Umfang mitzuteilen, wurde aufgegriffen.

17. Gesundheit

17.1 Gesundheitsreform 2000

Die Gesundheitsreform 2000 wird den Patientendatenschutz verändern. Zusammen mit anderen Datenschutzbeauftragten gelang es uns, die Idee einer Pseudonymisierung (Verschlüsselung)) von Patientendaten in die parlamentarischen Beratungen einzubringen.

Ab Juli 1999 befaßten wir uns – in enger Abstimmung mit den anderen Datenschutzbeauftragten – intensiv mit der Gesundheitsreform 2000. In einer ersten Stellungnahme kritisierten wir vor allem die geplante patientenbezogene Datenübermittlung zur Abrechnung ambulanter Leistungen. Bisher übermitteln die Kassenärztlichen Vereinigungen dazu grundsätzlich nur fallbezogene, nicht patientenbezogene Daten an die Krankenkassen. Zusammen mit den Daten aus einer stationären Behandlung, die den Kassen auch bisher schon patientenbezogen übermittelt werden, erhielten die Kassen damit die Möglichkeit, ein umfassendes Krankheitsprofil der Versicherungsnehmer zu erstellen.

Im August 1999 verabschiedeten die Datenschutzbeauftragten von Bund und Ländern eine gemeinsame Entschließung zur Gesundheitsreform 2000. Sie baten den Gesetzgeber dringend, die bisher versäumte Prüfung nachzuholen, ob die geplanten zusätzlichen Einschränkungen des Datenschutzes erforderlich und verhältnismäßig sind. Sie bezeichneten die Begündung des Gesetzentwurfs für eine generell patientenbezogene Datenübermittlung als nicht überzeugend, eine entsprechende Notwendigkeit als nicht ersichtlich. Als weitere Problempunkte nennt die Entschließung:

– die nur vage umgrenzte Erweiterung der Beratungs- und Steuerungsaufgaben der Krankenkassen mit entsprechend umfangreichen Datenerhebungs- und -verarbeitungsbefugnissen,

– die Einrichtung von kassenübergreifenden zentralen Datenannahme- und -verteilstellen mit zusätzlichen Mißbrauchsrisiken und

– Fragen der Patienten-Einwilligung bei dem neuen Hausarztmodell und der integrierten Versorgung in Praxisnetzen.

Bei einem Gespräch im September 1999 im Bundesgesundheitsministerium erläuterten wir unsere technischen Vorstellungen von einer Pseudonymisierung von Patientendaten. Die Einladung erfolgte insbesondere aufgrund unserer Veröffentlichung „Der Patient im Gesundheitsnetz“ im Februar 1999, die ein Kapitel „Der pseudonyme Patient“ enthält (Datenschutz und Datensicherheit 2/99, S. 70). In der nachfolgenden politischen Auseinandersetzung über die Gesundheitsreform 2000 spielte die Verschüsselung (Pseudonymisierung) von Patientendaten eine große Rolle. Die parlamentarischen Beratungen haben weitgehenden Konsens darüber erzielt, daß eine patientenbezogene Datenverarbeitung so weit wie möglich vermieden werden sollte. Wir regten an, eine Verschlüsselung von Patientendaten – jedenfalls mittelfristig – schon bei den Leistungserbringern (Ärzten / Krankenhäusern) und nicht erst bei den nun geplanten zentralen Datenannahme- und Verteilstellen vorzusehen.

Die im Bundestag am 4. November 1999 beschlossene Entwurfsfassung sieht tatsächlich eine grundsätzliche Pseudonymisierung der Patientendaten vor – und zwar für alle Daten, die von den Datenannahme- und Verteilstellen an die Kassen weiterzugeben sind, also auch für Patientendaten der Krankenhäuser und die Rezeptdaten. Für eine Reihe fest umrissener Zwecke und nur für die Zeit der Zweckerfüllung wird den Kassen die Reidentifikation der Patientendaten durch eine besondere Stelle gestattet. Diese Lösung wurde von allen Parteien und den Spitzenverbänden des Gesundheitswesens befürwortet.

Diese datenschutzrechtliche Errungenschaft einer grundsätzlichen Pseudonymisierung von Versichertendaten ist in der Gefahr, bei den Verhandlungen im Bundesrat wieder abgeschafft zu werden. Als zustimmungspflichtiger Teil der Gesundheitsreform könnte Sie der prinzipiellen Kritik der Ländermehrheit zum Opfer fallen. Wir haben deswegen die Behörde für Arbeit, Gesundheit und Soziales gebeten, sich im Bundesrat für den Erhalt dieses allgemein begrüßten Reformteils einzusetzen.

17.2 Charta der Patientenrechte

Durch unsere Mitwirkung an der Formulierung der „Patientencharta“ enthält das von der Gesundheitsministerkonferenz beschlossene Dokument auch eine Reihe spezifischer Datenschutzrechte; die Aufnahme anderer Datenschutzanliegen konnten wir nicht erreichen.

Im November 1997 richtete die Gesundheitsministerkonferenz eine Arbeitsgruppe unter der Federführung Hamburgs und Bremens ein, die eine „Patientencharta“ erarbeiten sollte. Als Ziel wurde ein „Konsenspapier“ aller Stellen und Organisationen im Gesundheitswesen angestrebt. Ein erster Entwurf wurde im Januar 1999 in der Behörde für Arbeit, Gesundheit und Soziales mit Vertretern der Wissenschaft, den Spitzen-Körperschaften des Gesundheitswesens, mit Patientenorganisationen und mit uns diskutiert. Die Datenschutzbeauftragten der anderen Bundesländer hatten uns beauftragt, vor Ort an der Entwicklung der Patientencharta mitzuwirken und die Anliegen des Datenschutzes einzubringen.

In einer ausführlichen Stellungnahme drangen wir darauf, daß der Datenschutz bzw. das Recht auf informationelle Selbstbestimmung nicht nur in wenigen verstreuten Details inhaltlich angesprochen, sondern auch als Begriff und Grundrecht ausdrücklich benannt wird. Wir schlugen einen eigenen Abschnitt „Ärztliche Schweigepflicht und Datenschutz“ vor, der insbesondere den Willen der Betroffenen bei den verschiedenen Übermittlungen von Patientendaten an Dritte betont und die datenschutzrechtlichen Auskunfts-, Berichtigungs- und Löschungsrechte vorstellt. Ferner wollten wir die Patientinnen und Patienten über ihre Rechte bei der Anamnese, also der Erhebung der Krankengeschichte, sowie über das Recht auf Nichtwissen hinweisen, das insbesondere bei der Durchführung von Genomanalysen eine Rolle spielt.

Das von der Gesundheitsministerkonferenz im Juni 1999 verabschiedete Dokument „Patientenrechte in Deutschland heute“ (der Titel „Patientencharta“ wurde nicht von allen Beteiligten mitgetragen) berücksichtigt diese Ergänzungswünsche zum Teil. Der Datenschutz und die spezifisch datenschutzrechtlichen Betroffenenrechte wie das umfassende Auskunftsrecht nach dem Bundesdatenschutzgesetz werden ausdrücklich angesprochen. Einzelne Mitbestimmungsrechte der Patienten, z.B. bei Krankenhausbesuchen Dritter, bei der Versendung von Arztbriefen und bei der Information dritter Personen durch den Arzt, wurden aufgenommen. Nicht gelungen ist uns die Verankerung des Rechts auf Nichtwissen bei der genomanalytischen Diagnostik und des Patientenrechts, sich bei der Anamnese nach Aufklärung durch den Arzt auf jene Angaben zu früheren Erkrankungen zu beschränken, die der Patient für relevant hält hinsichtlich der gegenwärtigen Behandlung.

Die von der Behörde für Arbeit, Gesundheit und Soziales zunächst angekündigte weitere Diskussion des Dokuments in der Fachöffentlichkeit wird – soweit ersichtlich – derzeit nicht weiter verfolgt. Der offensichtlich prekäre Kompromiß zwischen den beteiligten Gesundheitsstellen, Organisationen und Körperschaften soll nicht wieder gefährdet werden. Bei Anfragen interessierter Patientinnen und Patienten sowie anderer Stellen werden wir auf die von der Gesundheitsministerkonferenz beschlossene Fassung hinweisen und bei Bedarf zusätzliche Datenschutzrechte hinzufügen.

17.3 Psychotherapeutengesetz und Umsetzung in Hamburg

Für die vorzulegenden Behandlungsnachweise im Approbationsverfahren nach dem neuen Psychotherapeutengesetz konnten wir den Patientendatenschutz weitgehend durchsetzen. Das datenschutzwidrige Kassenzulassungsverfahren mit externen Gutachtern ist für die Zukunft unterbunden.

Das Psychotherapeutengesetz vom 16. Juni 1998 (PsychthG) schützt erstmals die Berufsbezeichnung „Psychologische Psychotherapeutin“ bzw. „Psychologischer Psychotherapeut“ und bindet die Berufsausübung an eine formelle behördliche Approbation. Die Abrechnung mit den Krankenkassen setzt eine Zulassung bei der Kassenärztlichen Vereinigung voraus. Datenschutzrechtlich problematisch war die Umsetzung der Übergangsbestimmungen für bereits praktizierende Therapeuten.

17.3.1 Die Approbation

Bereits berufstätige Psychologen mußten für die Approbation innerhalb kurzer Frist unter anderem 60 bzw. 30 „dokumentierte und abgeschlossene Behandlungsfälle“ nachweisen. Schon früh haben wir sowohl mit der Behörde für Arbeit, Gesundheit und Soziales als auch mit den Datenschutzbeauftragten der anderen Bundesländer sowie mit Fachverbänden der Psychotherapeuten Kontakt aufgenommen, um beim Nachweis der Behandlungsfälle den Patientendatenschutz sicherzustellen. Da das Gesetz keine ausdrückliche Regelung zur personenbezogenen Datenübermittlung enthält, mußten die Nachweise grundsätzlich anonymisiert erfolgen. Nur bei Anhaltspunkten dafür, daß eine vorgelegte Behandlungsdokumentation gefälscht war, hielten wir eine Beweisführung anhand der personenbezogenen Original-Dokumente für vertretbar. Dies kam besonders bei selbstzahlenden Patienten in Betracht, für die es keine Fremdbestätigung der Leistung durch eine Versicherung gibt.

Das dann vom Amt für Gesundheit herausgegebene Merkblatt für Approbationsanträge sieht für die Einzelnachweise „Angaben unter Berücksichtigung der Schweigepflicht (§203 StGB) und des Datenschutzes“ und als Patientenidentifikationsdaten nur eine Patientenchiffre, Alter und Geschlecht vor. Bei Vorlage von Rechnungen für selbstzahlende Patienten sollten als Chiffre die Initialen des Patienten verwendet werden. Letzteres haben wir kritisiert: Eine laufende Nummer, die der Psychologe bei Bedarf entschlüsseln kann, reicht aus. Soweit Antragsteller mit ausdrücklicher Einwilligung der Patienten personenbezogene Dokumentationen vorlegten, baten wir die Approbationsbehörde, in keinem Falle die Patientenidentifikationsdaten zu erfassen und zu speichern. Beschwerden zum Approbationsverfahren haben wir daraufhin nicht mehr erhalten.

17.3.2 Die Kassenzulassung

Ganz anders war dies beim Kassenzulassungsverfahren. Im Vordergrund der Beschwerden stand hier der Datenschutz der Antragsteller: Kritisiert wurde die Praxis des Zulassungsausschusses, zur Bewertung der Fachkunde des Antragstellers andere Psychotherapeuten als externe Gutachter zu beauftragen, die zum Teil direkte Konkurrenten der Antragsteller sind. Sie erhielten die gesamten personenbezogenen Unterlagen der antragstellenden Psychologen und konnten sich so ein umfassendes Bild von den Wettbewerbern machen. Es bestand die Befürchtung, daß die sog. „Richtlinien-Therapeuten“ sich vor der Konkurrenz durch die „Erstattungs-Therapeuten“ schützen wollten. Die hohe Ablehnungsquote bei den Zulassungsverfahren kann diesen Verdacht kaum entkräften. Besonders schwer wog, daß den Antragstellern die Beauftragung und die Identität des externen Gutachters nicht mitgeteilt, sondern erst durch Akteneinsicht offenbar wurde.

Auf unsere Schreiben vom Juni und Juli 1999 an die Kassenärztliche Vereinigung (KVH), den Zulassungs- und den Berufungsausschuß teilte uns der Zulassungsausschuß im September 1999 schließlich mit, daß er in Zukunft keine externen Gutachter mehr beauftragen werde. Inzwischen waren die Entscheidungen über die Zulassung der praktizierenden Psychotherapeuten allerdings auch abgeschlossen. Der Berufungsausschuß, vor dem nun viele Anfechtungen der Zulassungsablehnungen zu prüfen sind, hat sich bisher nicht selbst geäußert. Die KVH berichtete jedoch, auch der Berufungsausschuß plane den Verzicht auf externe Gutachter. Trifft dies zu, haben wir wenigstens für die Zukunft eine datenschutzgerechte Umsetzung des neuen Psychotherapeutengesetzes erreicht.

17.4 BtmG-Änderung, AUB-Richtlinien, Methadonprogramm

Die Neuregelung der Substitutionsbehandlung Drogenabhängiger wirft auf Bundes- wie auf Landesebene eine Reihe datenschutzrechtlicher Fragen auf. Durch Gespräche mit den zuständigen Stellen des Gesundheitswesens konnten wir in Hamburg erste Anworten finden.

Zwei neue Rechtsvorschriften auf Bundesebene betreffen die Behandlung Drogenabhängiger mit Substitutionsstoffen. Zum einen wird derzeit das Betäubungsmittelgesetz geändert, um „Drogenkonsumräume“ und einen bundesweiten Abgleich von Substitutionsbehandlungen zu ermöglichen. Unsere Stellungnahme dazu wurde von der Behörde für Arbeit, Gesundheit und Soziales (BAGS) weitgehend geteilt. Wir forderten ein Zeugnisverweigerungsrecht für die Mitarbeiterinnen und Mitarbeiter der Drogenkonsumräume. Für die BAGS ist dies unproblematisch: Jeder Drogenkonsumraum sei zugleich eine „Drogenberatungsstelle“ im Sinne der Strafprozeßordnung. Damit hätten deren Mitarbeiterinnen und Mitarbeiter eine Schweigepflicht und ein Zeugnisverweigerungsrecht.

Zum anderen geben die neuen „Richtlinien zur substitutionsgestützten Behandlung Opiatabhängiger“ des Bundesausschusses der Ärzte und Krankenkassen seit April 1999 die Indikationen und das Verfahren für die Substitutionsbehandlung vor. Dabei handelt es sich erstmals um „Anerkannte Untersuchungs- oder Behandlungsmethoden“ (deswegen im folgenden: AUB-Richtlinien). Sie können mit den Kassen abgerechnet werden. BAGS, Kassenärztliche Vereinigung (KVH), Ärztekammer und Kassen hoben daraufhin den Hamburger Methadonvertrag auf und entwickelten zur Umsetzung der AUB-Richtlinien eine neue „Einverständniserklärung“ für den Patienten. Die KVH fragte uns darüber hinaus, ob sie der Krankenkasse die Behandlungsscheine für Substituierte gesondert übermitteln darf.

In einem Schreiben vom August 1999 lehnten wir die Übermittlung der Behandlungsscheine ab. Die Substitutionsbehandlung als nunmehr anerkannte Methode soll bei der Abrechnung gerade keine Sonderstellung mehr einnehmen, sondern wie jede andere Leistung abgerechnet werden. Hierfür schreibt das Sozialgesetzbuch vor, die Angaben seien „fallbezogen, nicht versichertenbezogen“ an die Kassen zu übermitteln. Behandlungsscheine sind dagegen versichertenbezogen. Eine gewünschte Protokollnotiz des Honorarvertrages zwischen KVH und AOK entfiel damit.

Mit der neuen Einverständniserklärung stimmt der Patient zu, daß die Gutachterkommission der KVH alle Unterlagen, die ihr der behandelnde Arzt zur Genehmigung der Substitutionsbehandlung zusendet, auch an die Kassen weiterreichen darf. Dies kritisierten wir als zu weitgehend. In einem Gespräch im September 1999 mit Vertretern von BAGS, KVH, AOK und anderen Kassen erörterten wir die Gesamtproblematik und kamen zu einem Kompromiß. Die AUB-Richtlinien verpflichten die KV zwar, der Kasse des Patienten „bei der Beratung der Einzelfallindikationen“ Gelegenheit zur schriftlichen Stellungnahme zu geben. Übereinstimmend hielten die Kassenvertreter dafür aber die Übersendung des Substitutionsantrags, der Indikation und des Therapievorschlags für ausreichend. Laborberichte, Krankenhausentlassungsberichte und anderes werden danach nicht mehr übermittelt. Die AOK versicherte ferner, daß bei ihr nur 2 Personen mit der Stellungnahme für die Gutachterkommission befaßt sind und andere Personen keinen Zugriff auf diese Akten haben. Auch würden diese Patientendaten nicht in der EDV erfaßt, sondern bis auf das Antragsformular nach der Stellungnahme vernichtet. Die KVH sagte eine Prüfung zu, ob die von den AUB-Richtlinien vorgeschriebene Gutachterkommission ihre Entscheidung nicht auch anhand pseudonymisierter Daten treffen kann und ob der dafür erforderliche Aufwand noch verhältnismäßig ist. Schließlich vereinbarten wir, daß die KVH uns die geänderte Einverständniserklärung sowie die Formblätter für Antrag, Indikation und Therapievorschlag zur Verfügung stellt.

Den Bundesbeauftragten für den Datenschutz baten wir, die AUB-Richtlinie insbesondere daraufhin zu überprüfen, ob nicht eine pseudonyme Verarbeitung der Patientendaten vorgeschrieben werden kann. Wir haben grundsätzliche Bedenken gegen die Einverständnislösung der AUB-Richtlinien: Die patientenbezogene Datenübermittlung an KV und Kassen zur Behandlungsgenehmigung weicht von den üblichen Verfahren ambulanter Behandlung nach dem Sozialgesetzbuch ab. Die fehlende Rechtsgrundlage für die Datenübermittlung durch eine Einwilligung zu ersetzen, erscheint uns angesichts der hochgradigen Zwangssituation für die Betroffenen sehr problematisch.

17.5 Berufsordnung für Hamburger Ärzte

Im Streit um die Regelung des Verkaufs einer Arztpraxis und des Akteneinsichtsrechts der Patienten verwarf die Ärztekammerversammlung einen zuvor mit Kammer und Aufsichtsbehörde vereinbarten Kompromiß.

Bereits im 13. TB (21.1) beschrieben wir die Auseinandersetzung mit der Ärztekammer um ein datenschutzgerechtes Verfahren beim Verkauf einer Arztpraxis. Der Bundesgerichtshof (BGH) hatte 1991 die Übergabe der Patientenunterlagen von der Einwilligung der Patienten abhängig gemacht.

Auch der Neufassung der Hamburger Berufsordnung vom 4. Mai 1998 mußten wir widersprechen. Neben der alten Position, dem BGH-Urteil werde schon eine besondere Verwahrung der Patientenunterlagen beim Praxis-Käufer gerecht, schrieb die Ärztekammer erstmals eine Einschränkung des Akteneinsichtsrechts des Patienten fest: „Subjektive Eindrücke und Wahrnehmungen des Arztes“ sollen die Patienten nicht erfahren. Wir verwiesen demgegenüber auf das Auskunftsrecht nach §34 Bundesdatenschutzgesetz, das sich auf alle zur Person des Betroffenen gespeicherten Daten bezieht.

In einem gemeinsamen Gespräch mit der Ärztekammer und der Aufsichtsbehörde im Februar 1999 einigten wir uns zu beiden Problemen auf eine Kompromißformulierung: Sie ging beim Praxisverkauf vom grundsätzlichen Einwilligungerfordernis aus, ließ aber für Sonderfälle Ausnahmen zu, für die die Kammer vereinheitlichende Richtlinien mit uns abstimmte. Hinsichtlich des Einsichtsrecht sollte wie bei der früheren Fassung der Berufsordnung auf die Einschränkung im Text verzichtet, aber durch die Einfügung des Wortes „grundsätzlich“ auf die Möglichkeit von Ausnahmen im Einzelfall hingewiesen werde. Datenschutzbeauftragte anderer Bundesländer nahmen daraufhin die Diskussion ihrerseits wieder auf.

Am 3. Mai 1999 verwarf die Kammerversammlung in Hamburg den Kompromiß jedoch ohne protokollierte Begründung als „grotesk und nicht realisierbar“ und bestätigte die Fassung der Berufsordung vom Mai 1998. Seitdem drängen wir die Behörde für Arbeit, Gesundheit und Soziales als Aufsichtsbehörde, die beiden erwähnten Regelungen nicht zu genehmigen.

17.6 Prüfung Universitätsfrauenklinik

Die Prüfung in der Universitätsfrauenklinik offenbarte neben einer Reihe kleinerer Defizite vor allem ein unsicheres und unorganisiertes Patientenakten-Archiv. Verbesserungen sind inzwischen eingeleitet oder umgesetzt.

Im September / Oktober 1998 prüften wir die Kernklinik und die Abteilung für Endokrinologie und Reproduktionsmedizin der Universitätsfrauenklinik. Gegenstand der Prüfung war sowohl die konventionelle als auch die elektronische Verarbeitung von Patientinnendaten. Mit dem Prüfbericht vom Januar 1999 faßten wir in 36 Punkten unsere datenschutzrechtlichen, organisatorischen und sicherheitstechnischen Anregungen und Forderungen zusammen. Inzwischen sind die meisten Punkte abgearbeitet und umgesetzt. Zu den behobenen bzw. angegangenen Mängeln zählten unter anderem folgende:

– Die Organisation der krankenhausinternen Datenschutzkontrolle war in einer Abteilung unzureichend.

– Bei der Wiederaufnahme einer Patientin wurden der Aufnahmekraft alle früheren Aufenthalte der Patientin auch in allen anderen UKE-Kliniken angezeigt.

– Der Patientinnenwunsch, Dritten gegenüber den Klinikaufenthalt geheimzuhalten, („Pförtnersperre“) wurde nicht wirksam umgesetzt.

– Das Geburtendokumentationssystem GDS ist nicht auf dem neuesten technischen Sicherheitsstand, nicht Jahr-2000-fähig und genügt zum Teil dem Hamburgischen Krankenhausgesetz nicht.

– Die Sicherheit der Sekretariats-PC und die Aufbewahrung von Briefkopien war unzureichend.

– Die von den Patientinnen erbetene Einverständniserklärung zur Datennutzung für Forschungszwecke ging zu weit.

– Das Archiv der Patientenakten sowie die Hinweiskarten waren kaum gesichert; das Archiv war/ist in Teilen desorganisiert; die Aufbewahrungs- bzw. Löschungsfristen wurden überschritten.

Die Krankenhausmitarbeiterinnen und -mitarbeiter wurden auf unsere Bitte inzwischen schriftlich auf die richtige Paßworthandhabung und das Verbot hingewiesen, auf PC mit Internet-Zugang zugleich Patientendaten zu verarbeiten. Die Einverständniserklärung für Forschungszwecke wurde überarbeitet, die Patientinnen-Karteikarte in der Abteilung für Endokrinologie soll neugefaßt werden. Die Ersetzung bzw. grundsätzliche Überarbeitung der Systeme GDS und QUASIC („Qualitätssicherung in der Chirurgie“ – genutzt als Dokumentationssystem) steht dagegen noch aus. Auch die Aktualisierung der Dienstanweisung zur Führung und Herausgabe von Patientenunterlagen, die für das gesamte UKE gilt, ist angekündigt, aber noch nicht umgesetzt.

17.7 Prüfung einer Drogenambulanz

Die Prüfung offenbarte gravierende Mängel der technischen Datensicherheit und unerwartete datenschutzrechtliche Organisationsprobleme durch die Privatisierung der Drogenambulanz in einer GmbH. Über die Behebung der Mängel wurde Einvernehmen erzielt.

Im November 1998 überprüften wir eine der drei Drogenambulanzen, die nun gemeinschaftlich in privater Rechtsform (GmbH) vom Landesbetrieb Krankenhäuser (LBK) getragen werden. Hauptaufgabe der Drogenambulanzen ist die Substitution von Drogenabhängigen nach den bisherigen NUB-Richtlinien und dem Hamburger Methadon-Rahmenvertrag, die Mitte 1999 durch die AUB-Richtlinien abgelöst wurden (siehe 17.4).

Aufgrund der Privatisierung ist ein betrieblicher Datenschutzbeauftragter zu bestellen, die Kontrolle durch uns dagegen – zur Zeit noch – auf eine Anlaßaufsicht beschränkt. Die ärztliche Schweigepflicht schließt trotz des gemeinsamen GmbH-Vertrages einen Zugriff aller Mitarbeiterinnen und Mitarbeiter auf die Patientendaten aller drei Drogenambulanzen aus.

Ohne die Rechtsfolgen der Privatisierung der drei Drogenambulanzen in einer gemeinsamen GmbH abschließend geklärt zu haben, konnten wir uns in einem Gespräch mit dem Medizinischen und dem Verwaltungs-Geschäftsführer sowie dem LBK im Mai 1999 auf folgendes einigen:

– Der vorgefundene Internetzugang von dem PC aus, auf dem auch Patientendaten verarbeitet werden, wurde unterbrochen. Für die Zukunft ist entweder eine Firewall-Lösung zu installieren oder ein stand allone-PC ohne Patientendaten-Verarbeitungsprogramm allein für den Internetzugang einzurichten. Die geplante Implemetierung einer neuen Praxis-Software wird mit uns abgestimmt.

– Der ärztliche Geschäftsführer der drei Drogenambulanzen wird durch entsprechende Einwilligungserklärungen der Patienten ermächtigt, zu Qualitätssicherungszwecken auch Patientendaten der anderen beiden Drogenambulanzen einzusehen.

– Jede Drogenambulanz benennt einen eigenen betrieblichen Datenschutzbeauftragten. Einer von ihnen ist zugleich übergeordneter zentraler Datenschutzverantwortlicher, der die Datenschutz- und -sicherungsmaßnahmen koordiniert, aber keinen Zugriff auf Patientendaten in den anderen beiden Ambulanzen hat.

– Die Einverständniserklärung bzw. Entbindung von der Schweigepflicht, die die Patienten zur personenbezogenen Datenübermittlung an Krankenkasse, Kassenärztliche Vereinigung, Labore und zu Qualitätssicherungszwecken unterzeichnen, wird geändert. Unsere Zweifel an der Freiwilligkeit des Einverständnisses stellten wir zurück, um eine praktikable Substitutionsbehandlung nicht insgesamt zu gefährden. Durch die Einführung der AUB-Richtlinien Mitte 1999 entstand hier allerdings eine neue Situation (siehe 17.4).

Nach der Prüfung wurden wir auf das Problem aufmerksam, daß die Drogenambulanz Arbeitsunfähigkeitsbescheinigungen für Arbeitgeber der Patienten regelmäßig mit dem Stempel „Drogenambulanz...“ versieht und so indirekt sehr sensible Informationen über den Arbeitnehmer offenbart. Wir haben dies für datenschutzwidrig erklärt und bei Drogenambulanz und Kassenärztlicher Vereinigung auch auf die grundsätzliche Bereitschaft zu einer neutralen Praxis-/Arztbezeichnung getroffen. Dennoch konnte diese bisher anscheinend nicht gefunden werden.

17.8 Prüfung Externe Qualitätssicherung

Bei der Prüfung der Externen Qualitätssicherung ging es darum, die Anonymität der verarbeiteten Patientendaten zu gewährleisten. Die vorgeschlagenen Verbesserungen wurden kurzfristig umgesetzt.

Im April 1999 prüften wir die Projektgeschäftsstelle der Arbeitsgemeinschaft Externe Qualitätssicherung (EQS) bei der Hamburgischen Krankenhausgesellschaft. Die Krankenhäuser erfassen Patientendaten zu verschiedenen medizinischen Fachgebieten nach einheitlichen Vorgaben und übermitteln sie fallbezogen an die EQS. Diese hat die Aufgabe, die Patientendaten zu vergleichen und den medizinischen Fachgesellschaften und betroffenen Krankenhäusern Auffälligkeiten mitzuteilen. Die technische Durchführung der Datenverarbeitung wurde einer von der Krankenhausgesellschaft gegründeten GmbH in den Nachbarräumen der EQS übertragen.

Diese rechtliche Konstruktion hat zur Folge, daß die GmbH als Auftragsdatenverarbeiter meldepflichtig ist und eine/n eigene/n Datenschutzbeauftragte/n bestellen muß. Meldung und Bestellung wurden inzwischen nachgeholt.

Das Hamburgische Krankenhausgesetz läßt eine personenbezogene Datenübermittlung zu Qualitätssicherungszwecken nicht zu. Schwerpunkt der Prüfung war deswegen die Frage, ob alle Verfahren der EQS tatsächlich mit hinreichend anonymisierten Daten arbeiten. In einigen Verfahren, bei denen dies fraglich erschien, konnte der Schutz vor Reidentifizierungen der Falldaten verbessert werden. So wird beim Projekt Anästhesiologie (Narkose) in Zukunft auf minuten- und tagesgenaue Terminangaben verzichtet. Bei der Neonatal(Neugeborenen)erhebung wurden die zuständigen Bundesgremien um die Einführung von Zeitspannen statt Terminen, um eine Beschränkung der Postleitzahl und um eine eigens generierte Patientennummer (statt der vielfach genutzten krankenhausinternen Patientennummer) gebeten.

Die Datensicherheit der eingesetzten Rechner war nicht ausreichend. Inzwischen rüstete die EQS bzw. die GmbH die EDV auf eine sicherere Betriebssoftware um. Die von uns zur Verfügung gestellte Verschlüsselungssoftware PGP wurde getestet und wird bei Vereinbarungen mit Vertragspartnern als Option angeboten.

Insgesamt trafen wir in der EQS auf ein hohes Maß an Datenschutzbewußtsein, technischer Kompetenz und Verbesserungsbereitschaft.

17.9 Prüfung Patientenbeschwerdedatei Verbraucherzentrale

Die Beschwerdedatei der Verbraucherzentrale war vor allem hinsichtlich der Speicherungs- bzw. Löschungsfristen für berechtigte und für ungeklärte Beschwerden zu ändern.

Die Patientenberatungsstelle der Verbraucherzentrale führt seit 1999 eine EDV-Datei für Beschwerden von Patienten gegen einzelne namentlich genannte Ärzte und Gesundheitseinrichtungen. Ziel der Datei ist es auch, mittelfristig über Häufungen von Beschwerden bei bestimmten Medizinern die „schwarzen Schafe“ zu erkennen. Bereits 1993 hatten wir die Planung dieser Datei datenschutzrechtlich begleitet. Aufgrund von aktuellen Anfragen prüften wir Datei und Verfahren im September 1999 vor Ort.

Folgende Fragestellungen waren dabei von besonderem Interesse:

– Benachrichtigt die Verbraucherzentrale die Ärzte, zu denen eine Beschwerde in der Datei erfaßt wird?

– Erfahren die Beschwerdegegner den Namen des beschwerdeführenden Patienten?

– Wann werden die Beschwerden – insbesondere die Namen der kritisierten Ärzte – wieder gelöscht?

Nicht zu beanstanden war die Praxis der Verbraucherzentrale bei der Information der Beschwerdegegner: Bei Erfassung einer Patientenbeschwerde in der Datei unterrichtet die Verbraucherzentrale den betroffenen Arzt davon in allgemeiner Form mit einem Schlagwort für den Beschwerdegegenstand und ohne den Namen des beschwerdeführenden Patienten. Bei Nachfragen erhält der betroffene Arzt zusätzliche Informationen zu dem Verfahren. Eine Bitte des Beschwerdegegners um direkte Auseinandersetzung mit dem Patienten gibt die Verbraucherzentrale an diesen weiter.

Als problematisch erwies sich das Löschungsverfahren: Angesichts der noch kurzen Betriebsdauer wurden bislang keine Beschwerdedaten gelöscht. Geplant war eine Speicherfrist von 5 Jahren für jede einzelne Beschwerde. Dem haben wir widersprochen: Bei vielen Beschwerden erfährt die Verbraucherzentrale angesichts einer anderweitigen Klärung gar nicht, ob die Vorwürfe berechtigt oder unberechtigt waren. Andere Beschwerde bleiben unaufgeklärt oder werden von den Patienten nicht weiter betrieben, wenn die Aufklärung nur mit Nennung ihres Namens möglich ist. Unaufgeklärte Beschwerden eignen sich aber kaum zum Erkennen von „schwarzen Schafen“. Wir haben deswegen eine Löschung von unbestätigten Beschwerden nach spätestens 1 Jahr gefordert. Für berechtigte Beschwerden haben wir eine Speicherdauer von 2 Jahren eingeräumt. Von einer „Beschwerdehäufung“ kann nach unserer Auffassung nicht gesprochen werden, wenn erst nach 2 Jahren eine weitere (berechtigte) Beschwerde gegen denselben Arzt eingeht. Die Reaktion der Verbraucherzentrale auf unsere Auffassung steht noch aus.

17.10 Prüfung UKE-FOKUS

Die Prüfung des Forschungs-Kommunikationssystems (FOKUS) des UKE ergab, daß trotz gegenteiliger Selbstverpflichtung wissenschaftliche Mitarbeiter auf Internet-PCs mit unsicherem Betriebssystem zugleich Patientendaten verarbeiteten.

Im Jahr 1999 haben wir das UKE-Forschungs-Kommunikationssystem (UKE-FOKUS) der Abteilung Informatik in der Medizin geprüft. Über das Forschungs-Kommunikationssystem wird ca. 2000 UKE-Anwendern, die noch nicht an das im Aufbau befindliche UKE-Forschungsnetz angeschlossen sind, der Zugang zum Internet vermittelt. Die IP-Adressen werden dynamisch vergeben.

Aus Sicherheitsgründen muß sich jeder Anwender – hauptsächlich wissenschaftliche Mitarbeiter und Doktoranden – schriftlich dazu verpflichten, auf dem jeweiligen Internet-PC keine personenbezogenen Daten zu speichern. Bei einer stichprobenartigen Überprüfung einzelner Stand-alone-PC mußten wir jedoch feststellen, daß diese Selbstverpflichtung von den Anwendern in der Regel nicht eingehalten wird. Dies ist umso problematischer, als auf den geprüften PC kein sicheres Betriebssystem installiert war. Wir haben daher das UKE aufgefordert, sämtliche EDV-Benutzer nochmals darauf hinzuweisen, daß medizinische Daten im UKE nur auf gesicherten Systemen innerhalb des Krankenhausinformationssystems (KIS) gespeichert werden dürfen. Sofern die Daten außerhalb des KIS gespeichert werden, ist entweder Windows 3.11 bzw. Windows 95 zusammen mit entsprechender Zusatzsoftware oder Windows NT als Betriebssystem in Verbindung mit geeigneten BIOS-Maßnahmen einzusetzen. Zudem haben wir angeregt, sämtliche PC, die nicht in das KIS eingebunden sind, mittelfristig einer stichprobenhaften internen Revision zu unterziehen.

Die Abteilung Informatik in der Medizin betreibt darüber hinaus die Web- und Mail-Server des UKE. Sowohl auf dem Web- als auch auf dem Mail-Server waren internetweit zahlreiche TCP/IP-Dienste verfügbar, die zum Ausgangspunkt von Internetattacken werden können. Da nicht alle Dienste internetweit benötigt werden, haben wir den Einsatz einer Firewall gefordert. Um Hackerangriffe aus dem Internet insgesamt besser erkennen zu können, wurde von uns zusätzlich der Einsatz von Sicherheitssystemen empfohlen, die entsprechende Attacken anhand der Angriffsmuster erkennen und auch blockieren können. Für Statistikzwecke wurden auf dem Web-Server die IP-Adressen sämtlicher Benutzer protokolliert, die auf das Internetangebot des UKE zugreifen. Personenbezogene Daten über die Inanspruchnahme von Telediensten dürfen gemäß §6 Teledienstedatenschutzgesetz (TDDSG) jedoch nur dann erhoben werden, soweit dies für die Abrechnung oder die Inanspruchnahme von Telediensten erforderlich ist. Da die IP-Adresse von Internetnutzern, die auf das UKE-Angebot zugreifen, ein personenbeziehbares und somit auch ein personenbezogenes Nutzungsdatum darstellt, das weder für die Inanspruchnahme noch für die Abrechnung relevant ist, haben wir das UKE aufgefordert, auf die Speicherung von IP-Adressen zu verzichten. Diese Forderung wurde vom UKE kurzfristig umgesetzt.

17.11 Basisdokumentation der Kinder- und Jugendpsychiatrie des UKE

Bei den besonders sensiblen Daten jugendlicher Psychiatriepatienten konnten wir durch organisatorische Änderungen der standardisierten Dokumentation entscheidende Verbesserungen des Datenschutzes erreichen.

Anläßlich der Prüfung eines EDV-Konzeptes für die Abteilung für Psychiatrie und Psychotherapie des Kindes- und Jugendalters im Universitätskrankenhaus Eppendorf erfuhren wir von der ausführlichen standardisierten „Basisdokumentation“ dieser Klinik: Auf einem Erhebungsbogen werden unter den Daten der Krankenversichertenkarte nach dem multiple choice-Verfahren Anamnese-, Befund-, Diagnose-, Therapie- und Sozialdaten jedes Patienten (und z.T. der Eltern) erfaßt. Diese Bögen wurden als „statistische Daten“ (aber personenbezogen) unabhängig von der Patientenakte aber ebenso lange wie sie aufbewahrt. Sie dienen zudem der EDV-Erfassung für Zwecke der Forschung. Dabei werden allerdings die Daten der Krankenversichertenkarte nicht mit gespeichert.

Da es sich bei den erfaßten Daten um äußerst sensible und schutzbedürftige Informationen handelt, haben wir verschiedene Verbesserungen des Datenschutzes angeregt. Diese wurden akzeptiert und mit folgenden Maßnahmen umgesetzt:

– Die Erhebungsbögen werden in Zukunft der individuellen Patientenakte beigeheftet und mit dieser archiviert. Daß sie nicht mehr unabhängig von den Akten sortiert gesammelt werden, schließt einen schnellen Zugriff durch unbefugte Dritte aus.

– Damit ist entgegen der bisherigen Praxis auch zugleich gewährleistet, daß bei einer Akteneinsicht auch der Erhebungsbogen zur Kenntnis genommen werden kann.

– Die Erfassung der Daten in der EDV-Datei erfolgt faktisch anonym. Dazu werden statt der bislang gespeicherten genauen Termine für die Aufnahme und das Behandlungsende nur noch die Behandlungsdauer festgehalten. Es gibt keine Möglichkeit, von den EDV-Falldaten auf die Patientenakte (mit dem Erfassungsbogen) zurückzuschließen.

– Es wird sichergestellt, daß auf allen Rechnern mit Internetzugang keine Patientendaten verarbeitet werden. Für den Austausch elektronischer Post wird ein zentraler Emailhost eingerichtet, der Emails für die berechtigten PC bereithält, ohne einen direkten Internetzugang zu gewähren.

Für die Umsetzung des abgestimmten EDV-Konzepts stehen wir weiter als Berater zur Verfügung.

17.12 Sonstiges

– Im August / September 1999 führten wir eine Prüfung in der allgemein-psychiatrischen Abteilung und im Krankengeschichtenarchiv des Klinikums Nord, Betriebsteil Ochsenzoll, durch. Der Sachbericht über die Prüfung wurde inzwischen mit den Verantwortlichen des Krankenhauses abgestimmt. Unsere rechtliche Würdigung ist derzeit in Arbeit.

– In einem Unternehmen der Arzneimittelherstellung untersuchten wir, wie die Pharmareferenten Arztdaten (Verschreibungen, Verschreibungspotential) erheben und in der zentralen Datenbank speichern. Wir vereinbarten mit dem Unternehmen eine Änderung der Anweisung an die Pharmareferenten. Sie stellt nun sicher, daß arztbezogene Daten nur offen beim Arzt selbst oder mit seiner Zustimmung beim Praxispersonal, aber z.B. nicht verborgen bei den Apotheken, erhoben werden.

– Die Vermittlung von Privatgutachten durch die Zahnärztekammer wurde für die Patienten transparenter: Im Musterschreiben an Patienten, die um die Benennung eines Gutachters bitten, weist die Kammer nun darauf hin, daß sie den behandelnden Zahnarzt verständigt, um Überlassung der Behandlungsunterlagen an den Gutachter bittet und ihm anschließend das Gutachten zur Kenntnis gibt. Mit der im Musterschreiben erbetenen Zahlung des Kostenvorschusses an die Kammer hat der Patient es in der Hand, dies zu akzeptieren oder zu vermeiden.

– Auch in den Jahren 1998/9 nahmen wir zu einer ganzen Reihe von medizinischen Forschungsvorhaben Stellung. Häufig ging es dabei um eine frühzeitigere oder stärkere Anonymisierung von Patientendaten. Bei den nicht seltenen überregionalen Projekten bedarf es zudem einer Abstimmung zwischen den betroffenen Datenschutzbeauftragten, die zum Teil unterschiedliches Landesrecht anzuwenden haben. Verschiedene Anfragen bezogen sich auch auf die Weitergabe von Patientendaten aus dem Hamburger Krebsregister. Hier stellt das Hamburgische Krebsregistergesetz besondere Anforderungen.

18. Behördlicher Aktentransport

Die bisherige Praxis des behördeninternen Versands sensibler personenbezogener Unterlagen muß dringend korrigiert werden.

Im Zeitraum August bis November 1999 führten wir eine umfangreiche Prüfung beim Behörden-Transport-Service (BTS) durch, über den der behördeninterne Post- und Aktenaustausch der Freien und Hansestadt Hamburg abgewickelt wird. An den BTS sind insbesondere die Senatsämter und Fachbehörden, Gerichte, der Rechnungshof, öffentliche Unternehmen in privater Rechtsform (z.B. die HEW) sowie Krankenkassen angeschlossen. Organisatorisch ist der BTS in die Finanzbehörde eingegliedert. Die datenschutzrechtliche Verantwortung liegt jedoch bei den absendenden Stellen.

Bei unserer Kontrolle stellten wir in großer Anzahl gravierende Verstöße gegen Anforderungen des Datenschutzes fest. Akten und einzelne Unterlagen mit sehr sensiblen personenbezogenen Daten wurden offen ohne Verwendung von Umschlägen in die Behördenpost gegeben und waren deshalb während des Transports nicht besonders gegen eine inhaltliche Kenntnisnahme geschützt. Diese Praxis kann auch unter Berücksichtigung der Verschwiegenheitspflicht, der das Personal beim Transport unterliegt, nicht akzeptiert werden.

Die Verletzungen des Datenschutzes gingen in erheblichem Umfang von Gerichten aus. Offen vorgefunden haben wir Betreuungs-, Vormundschafts-, Ermittlungs- und Bußgeldakten. Auch Auskünfte aus dem Schuldnerverzeichnis, Räumungsklagen, Scheidungsurteile, Mitteilungen zum Versorgungsausgleich und Kindergeld, Testamente, Erbscheine, Haftbefehle in Straf- und Zwangsvollstreckungssachen, Besuchsregelungen für die Untersuchungshaft, Berichte von Justizvollzugsanstalten, Beschlüsse über die vorläufige Entziehung der Fahrerlaubnis, Strafurteile und Bewährungsbeschlüsse waren offen in die Behördenpost gelangt.

Selbst Vorgänge über Adoptionen und Namensänderungen, Beweisbeschlüsse zur Einholung von Abstammungsgutachten, Urkunden über die Anerkennung der Vaterschaft, Verfahren zur Übertragung oder Entziehung der elterlichen Sorge, gerichtspsychologische und nervenärztliche Gutachten sowie Beschlüsse über die Betreuung, geschlossene Unterbringung und Fesselung psychisch Kranker wurden ohne Umschlag befördert.

Die verantwortlichen Stellen haben wir, sobald Verletzungen des Datenschutzes festgestellt wurden, nachdrücklich über das Problem informiert. Als die Verstöße sich Anfang Oktober 1999 nach Anzahl und Gewicht häuften, haben wir uns umgehend an die Justizbehörde gewandt und dringend um Abhilfe gebeten. Bei weiteren Kontrollen Anfang November 1999 fanden wir wiederum eine hohe Anzahl sensibler Unterlagen offen vor. Deshalb sahen wir uns veranlaßt, die Öffentlichkeit mit einer Presseerklärung über die Ergebnisse unserer Kontrolle zu unterrichten. Gleichzeitig legten wir der Justizbehörde nahe, gemeinsam mit uns und den Gerichten ein tragfähiges Gesamtkonzept zur Gewährleistung des Datenschutzes zu entwickeln. Mit den Gerichten haben wir bereits Gespräche über eine praxisgerechte verschlossene Übersendung von Akten und Schriftstücken aufgenommen. Die Finanzbehörde hat zugesagt, die an den BTS angeschlossenen Stellen in einem Rundschreiben erneut auf die Anforderungen des Datenschutzes besonders hinzuweisen.

Auch bei Prüfungen, die wir nach unserer Presseerklärung durchführten, ergaben sich zahlreiche Datenschutzverstöße. Offen übersandt wurden z.B. Scheidungsurteile, Sitzungsprotokolle und anwaltliche Schriftsätze in Verfahren zum elterlichen Sorge- und Umgangsrecht, ein Blutgruppengutachten, eine für die Steuerfahndung bestimmte Bankauskunft, die Anordnung der Unterbringung in einem psychiatrischen Krankenhaus und ein verwaltungsgerichtlicher Beschluß zur Entlassung eines Beamten auf Probe. Zuletzt konnten wir beim Versand durch das Amtsgericht Hamburg – Vormundschaftsgericht – die Beachtung des Datenschutzes feststellen, während bei den Familien- und Strafsachen sowie bei den vom Landgericht Hamburg als Beschwerdeinstanz bearbeiteten Betreuungs- und Freiheitsentziehungssachen noch eine deutliche Besserung zugunsten des Datenschutzes erreicht werden muß.

Erfreulich ist, daß die Staatsanwaltschaft aufgrund einer Anfang November 1999 erlassenen Verfügung Mitteilungen in Strafsachen und sonstige personenbezogene Schriftstücke nunmehr durchgehend verschlossen übersendet.

Eine Tendenz zur verstärkten Umsetzung des Datenschutzes zeichnet sich auch im Bereich der Jugend- und Sozialämter ab. Allerdings haben wir auch bei aktuellen Prüfungen noch offene Sendungen, z.B. Rechnungen von Krankenhäusern und Pflegeheimen sowie Unterlagen zur Vaterschaftsfeststellung und -anfechtung, vorgefunden.

Unseren Dialog mit den verantwortlichen Stellen und die Kontrollen beim BTS werden wir intensiv fortsetzen.

Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

19. Versicherungswirtschaft

19.1 Registrierung von Versicherungsvermittlern

Erst der tatsächliche Umgang mit dem noch nicht in Kraft getretenen Vermittlerregister wird zeigen, ob datenschutzrechtliche Bedenken gerechtfertigt sind.

Auch 1998 und 1999 konnte nicht mit letzter Sicherheit geklärt werden, ob es noch zu einer Umsetzung der EG-Empfehlung vom 18. Dezember 1991 (vgl. 15. TB, 22.1; 16. TB, 19.1) kommen wird. Darüber hinaus stellte sich in dem Berichtszeitraum jedoch auch heraus, daß das Register – anders als zunächst angekündigt – die Registrierung ohne gesetzliche Regelung vorläufig nicht aufnehmen soll. Dennoch hat die Versicherungswirtschaft die Aufsichtsbehörde um eine abschließende datenschutzrechtliche Beurteilung gebeten, um jedenfalls die Möglichkeit zu haben, unabhängig von diesen rechtlichen Bedenken die Registrierung erforderlichenfalls aufnehmen zu können.

Im Laufe der Gespräche stellte sich heraus, daß die bereits 1997 dargestellten datenschutzrechtlichen Bedenken trotz einiger Veränderungen im Wortlaut des Richtlinienentwurfs nicht endgültig ausgeräumt werden konnten. Wesentlich dafür war, daß bei der Registrierung von Versicherungsvermittlern bestimmte Vorgehensweisen, wie z.B. die Nichtbeschäftigung nicht registrierter Vermittler, nicht ausgeschlossen werden konnten. Da die Versicherungswirtschaft nicht bereit war, den Wortlaut deutlicher zu gestalten, blieben einige Punkte offen, deren Zulässigkeit sich erst im konkreten Umgang mit dem Verfahren selbst ergeben werden. Es wurde daher vereinbart, zunächst keine weitere Klärung herbeizuführen und erst anläßlich von Zweifeln nach Aufnahme der Registrierung den datenschutzgerechten Umgang zu überprüfen.

19.2 Sonstiges

– Die Gespräche mit dem Gesamtverband der Deutschen Versicherungswirtschaft über die datenschutzrechtlichen Aspekte der Tätigkeit von Versicherungen im Internet wurden fortgeführt.

– Der Dissens über die Reichweite des Fragerechts von Versicherungen gegenüber behandelnden Ärzten angesichts eingeschränkter Schweigepflicht-Entbindungsklauseln (vgl. 16. TB, 19.2) konnte leider nicht zufriedenstellend ausgeräumt werden. Die Obersten Aufsichtsbehörden für den Datenschutz, die Arbeitsgemeinschaft der Verbraucherverbände e.V. und das Bundesaufsichtsamtes für das Versicherungswesen sind übereinstimmend der Auffassung, daß die Fragen sich teilweise nicht im Rahmen der von den Patienten unterzeichneten Klauseln halten. Dennoch ist die Versicherungswirtschaft nicht zu einer generellen Änderung bereit und kann hierzu rechtlich auch nicht gezwungen werden. Die Folge kann allerdings sein, daß sich der Auskunft gebende Arzt strafbar macht.

– Die Versicherungswirtschaft hatte angekündigt, noch 1999 einen Leitfaden zur Imageverarbeitung herauszugeben. Darin sollte auch der Einsatz opto-elektronischer Speichermedien, wie mit den Obersten Aufsichtsbehörden für den Datenschutz vereinbart, dargestellt werden. Da der Leitfaden nicht rechtzeitig vorlag, kann aus Sicht der Obersten Aufsichtsbehörden noch keine abschließende Stellungnahme abgegeben werden.

20. Schufa und Auskunfteien

20.1 Scoring-Verfahren

Erläuterungen zum Scoring-Verfahren wurden in das Schufa-Merkblatt aufgenommen.

Die Erörterung zwischen den Obersten Aufsichtsbehörden und der Schufa über das Scoring-Verfahren wurde im Berichtszeitraum fortgesetzt (vgl. 16. TB, 20.1). Von den Aufsichtsbehörden wurde zustimmend zur Kenntnis genommen, daß die Schufa bei der beabsichtigten Überarbeitung ihrer Klausel eine Information über das Scoring-Verfahren aufnehmen wird. Das Merkblatt zum Schufa-Verfahren in der Fassung von Januar 1999, das Bankkunden auf Wunsch von ihrer Bank oder der Schufa ausgehändigt wird, enthält nun allgemeine Erläuterungen zum Scoring-Verfahren.

In Bezug auf die Beauskunftung des Scorewertes gegenüber den Betroffenen nach §34 BDSG besteht dagegen noch keine Einigkeit zwischen der Schufa und den Aufsichtsbehörden. Die Schufa ist der Auffassung, daß sie nach der Vorschrift des §34 BDSG nicht verpflichtet sei, Auskunft über Bildung und Zusammensetzung des Scorewertes zu geben, da dieser im Einzelfall errechnet und übermittelt, nicht jedoch gespeichert werde. Eine nachträgliche Berechnung des Scorewertes sei häufig nicht möglich, da sich die Datenbasis und die statistischen Bezugsgrößen täglich ändern könnten. Die Schufa hält es für sachgerecht, wenn der Empfänger der Schufa-Auskunft, in der Regel eine Bank, den Betroffenen den Scorewert mitteilt und erläutert.

Aus Sicht der Aufsichtsbehörden haben die Betroffenen nach §34 BDSG gegenüber der Schufa und den Vertragspartnern der Schufa einen Anspruch auf Beauskunftung des Scorewertes (vgl. 16. TB, 20.1). Die Kreditwirtschaft zeigte in Gesprächen mit den Aufsichtsbehörden allerdings keine Bereitschaft, ihren Kunden Auskunft über den Scorewert zu geben. Insbesondere die Erläuterung setzt erhebliches Wissen über die Bildung des Scorewertes voraus, das bei den Vertragspartnern in der Regel kaum vorhanden sein wird.

20.2 Neukonzeption der Schufa-Merkmale

Die Schufa führt neue Auskunftsmerkmale bei nicht vertragsgemäßem Verhalten ein.

Die Schufa hat die Obersten Aufsichtsbehörden 1998 über die beabsichtigte Neukonzeption der Auskunftsmerkmale bei nicht vertragsgemäßem Verhalten informiert. Betroffen sind 16 Auskunftsmerkmale, die in 7 Merkmalen zusammengefaßt werden sollen. Die Schufa verspricht sich dadurch eine Vereinfachung des Verfahrens und eine Entlastung ihrer Vertragspartner durch Reduzierung der Einmeldungen. Seit Januar 1999 speichert und beauskunftet die Schufa außerdem Insolvenzmerkmale.

Es ist geplant, mit dem neuen Meldeverfahren im dritten Quartal des Jahres 2000 zu beginnen. Die völlige Umstellung bei allen Vertragspartnern wird einige Zeit in Anspruch nehmen. Die derzeitigen Auskunftsmerkmale sollen daher auch nach Umgestaltung des Verfahrens noch 3 Jahre erhalten bleiben.

Von Seiten der Aufsichtsbehörden bestehen keine Einwendungen gegen die Änderungen der Schufa-Auskunftsmerkmale.

20.3 Neufassung der Schufa-Klausel

Die Schufa-Klausel wird überarbeitet.

Die Schufa beabsichtigt, ihre derzeit geltende Klausel in inhaltlicher Hinsicht wegen neuerer Entwicklungen, z.B. Scoring und Neukonzeption der Meldemerkmale, zu überarbeiten. Zur Erhöhung der Transparenz der Klausel ist auch eine Modernisierung in redaktioneller Hinsicht beabsichtigt.

Auf Vorschlag der Schufa wurde eine „Formulierungsgruppe“ gebildet, der Vertreter der Datenschutzaufsichtsbehörden, des Zentralen Kreditausschusses und der Schufa-Organisation angehören. Die Gruppe hat ihre Tätigkeit aufgenommen. Arbeitsergebnisse sollen jedoch erst vorgelegt werden, wenn feststeht, ob und welche Auswirkungen die anstehende BDSG-Novellierung für die Formulierung der Klausel hat.

20.4 Schufa-Verfahren für die Wohnungswirtschaft

Im Rahmen eines zeitlich begrenzten Testverfahrens erhält die gewerbliche Wohnungswirtschaft von der Schufa Auskünfte über potentielle Mieter.

Viele Beschwerden in den letzten Jahren betrafen die Praxis gewerblicher Vermieter, von Mietinteressenten regelmäßig die Vorlage von Schufa-Selbstauskünften zu verlangen (vgl. 13. TB, 22.1, 15. TB, 23.1). Wir haben darüber Gespräche mit Verbänden der Wohnungswirtschaft, der Schufa Hamburg und den übrigen Obersten Aufsichtsbehörden geführt. Die Verhandlungen haben zu dem Ergebnis geführt, im Rahmen eines zeitlich auf 6 Monate begrenzten Testverfahrens der gewerblichen Wohnungswirtschaft in Hamburg die Gelegenheit zu geben, am Schufa-B-Auskunftsverfahren teilzunehmen. Dieses Auskunftsverfahren beschränkt sich auf die Übermittlung von Daten über die nicht vertragsgemäße Abwicklung von Vertragsverhältnissen und gerichtliche Vollstreckungsmaßnahmen.

Ziel des Testverfahrens ist es, die hohe Zahl der Selbstauskünfte, die für Wohnungsanmietungen eingeholt werden, zu reduzieren. Die Aufnahme der Wohnungsunternehmen als Vertragspartner der Schufa bedeutet zwar eine Abweichung vom Prinzip der Schufa, nur Firmen anzuschließen, die Geld- oder Warenkredite vergeben. Dies war aber im Interesse einer verfassungsnäheren Alternative zu den problematischen Schufa-Selbstauskünften notwendig, durch die die Wohnungswirtschaft eine Fülle von Daten erhält, die für den Abschluß von Mietverträgen gar nicht erforderlich sind.

Bei Vereinbarung des Auskunftsverfahrens erhalten Vermieter von der Schufa künftig nur negative Daten über die Mietinteressenten. Die Vermieter verpflichten sich im Gegenzug, Forderungen ab Mahnbescheid aus dem Mietverhältnis an die Schufa zu melden. Nachmeldungen der Schufa an die Vermieter bei bestehenden Mietverhältnissen gibt es in der Testphase nicht. Die Aufsichtsbehörden sind der Auffassung, daß die Vermieter nach Abschluß eines Mietvertrages diese Angaben nicht mehr benötigen und insoweit kein berechtigtes Interesse nach §29 Abs. 2 BDSG haben.

Vor Einholung einer Schufa-Auskunft durch den gewerblichen Vermieter ist eine entsprechende schriftliche Einwilligung des Bewerbers erforderlich. Eine Einwilligungsklausel haben wir mit der Schufa abgestimmt.

Die zunächst von uns angestrebte Reduzierung der Negativmerkmale für das Auskunftsverfahren war der Schufa aus technischen und organisatorischen Gründen nicht möglich. Nach Ablauf des Testverfahrens soll erneut darüber nachgedacht werden, zumal die Schufa die Merkmale über nicht vertragsgemäßes Verhalten ab 2000 völlig neu konzipiert hat (siehe 20.2).

Das Testverfahren hat im Juli 1999 begonnen. Eine erste Auswertung läßt erkennen, daß die gewerbliche Wohnungswirtschaft immer mehr Auskünfte einholt. Nach anfänglich 133 Auskünften im Juli, lag die Zahl der Auskünfte im September bei 2514. Die Schufa teilte mit, daß ein deutlicher Rückgang bei der Erteilung von Eigenauskünften für Mietinteressenten festzustellen ist. Über die weitere Entwicklung werden wir im nächsten Bericht informieren.

20.5 Datenerhebung durch Auskunfteien

Die Aufsichtsbehörde fordert die lückenlose Dokumentation der Herkunft und Beschaffungsart von personenbezogenen Daten im Rahmen von Ermittlungen durch Detekteien und Auskunfteien.

Die Aufsichtsbehörde hatte Kenntnis erhalten, daß die Berichte einer Detektei in Einzelfällen personenbezogene Daten über Sozialleistungen enthielten, deren unbefugte Offenbarung nach dem Sozialgesetzbuch strafbar ist. U.a. enthielten Berichte genaue Angaben über den Bezug von Arbeitslosenunterstützung, Arbeitslosengeld, Krankengeld und Sozialhilfe. Auskunft über die Herkunft der Daten erteilte die Detektei nicht. Ermittlungsunterlagen wurden nicht aufbewahrt.

Eine Landesversicherungsanstalt informierte uns darüber, daß von einem Telefonapparat in einem allgemein zugänglichen Raum der Detektei ein Versuch unternommen worden war, Sozialdaten zu erfragen. Deshalb haben wir die Detektei aufgefordert, die innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird. Insbesondere haben wir innerbetriebliche Maßnahmen gefordert, die die lückenlose Dokumentation der Herkunft und Beschaffungsart von personenbezogenen Daten im Rahmen von Ermittlungen in oder aus Dateien durch einen konkret benannten Mitarbeiter gewährleisten.

Nachdem die Detektei auf entsprechende Schreiben nicht reagiert hatte, haben wir zur Gewährleistung des Datenschutzes nach §38 Abs. 5 BDSG zur Beseitigung von organisatorischen Mängeln angeordnet. Die Detektei hat gegen die Anordnung Widerspruch eingelegt. Gegen unseren Bescheid und den Widerspruchsbescheid ist eine Klage vor dem Verwaltungsgericht anhängig.

21. Kreditwirtschaft

Es zeigt sich von Jahr zu Jahr wieder, daß das Verhalten der Kreditwirtschaft zwar nicht wegen erheblicher datenschutzrechtlicher Verstöße kritisiert werden kann. Daran ist auch das große Eigeninteresse an der Einhaltung insbesondere des Bankgeheimnisses erkennbar. An der datenschutzfreundlicheren Gestaltung ihres Angebots haben die Unternehmen jedoch äußerst wenig Interesse. Dies wird beispielhaft sowohl an der geringen Aktivität deutlich, mit der die kontoungebundene Geldkarte verbreitet wird (vgl. 1.3.2), als auch an der Weigerung, den bankinternen Zugriff auf Kontoinformationen technisch unterstützt zu beschränken.

21.1 Beschränkung des Zugriffs auf Kontoinformationen

Auch künftig werden Kunden nicht selbst entscheiden dürfen, ob eine oder einzelne Filialen eines Kreditinstituts ausschließlichen Zugriff auf ihre Daten haben sollen.

Nachdem die Vertreter der Kreditwirtschaft im Mai 1997 zunächst zugesagt hatten, die Möglichkeiten der Beschränkung des bankinternen Zugriffs auf Kontoinformationen einzelner Kunden zu prüfen (vgl. 16. TB, 21.3), änderten sie diese Aussage schon im Dezember 1997. Da die Nachfrage nach dieser „Sonderregelung“ minimal sei, sei der mit der Einführung technischer Beschränkungen verbundene hohe Aufwand nicht vertretbar. Gleichwohl wurde ein nochmaliges Überdenken der Angelegenheit zugesagt.

Ein häufig vorgebrachtes Argument der Kreditwirtschaft in dieser Angelegenheit ist es, daß der unberechtigte Zugriff auf Kundendaten durch nichtbefugte Mitarbeiter strafbar sei und auch arbeitsrechtlich streng verfolgt würde. Angesichts der Tatsache, daß tagtäglich tausende von – weit überwiegend berechtigten – Zugriffen erfolgen, fällt jedoch ein derart strafbares Verhalten so gut wie nie auf. Um die sensiblen personenbezogenen Bankdaten der Kunden nicht nur rechtlich, sondern auch tatsächlich vor unberechtigten Zugriffen zu schützen, wäre die technische Unterstützung der Beschränkung des Zugriffs auf Kontoinformationen unerläßlich. Nicht verkannt wird dabei seitens der Obersten Aufsichtsbehörden der Länder, daß filialübergreifende Abteilungen eines Unternehmens, wie z.B. die Revision oder auch in bestimmten Fällen die Rechtsabteilung, weiterhin umfassende Zugriffsrechte haben müssen. Ebenso sollte der Kunde, der mehrere Filialen aufsuchen möchte, die Wahl haben, seine Daten jeder Filiale oder einzelnen Filialen zugänglich zu machen.

Im Februar 1998 haben sich die Vertreter des Zentralen Kreditausschusses zunächst abschließend zu diesem Thema geäußert. Sie gaben bekannt, daß eine Beschränkung des bankinternen Zugriffs auf Kontoinformationen auf bestimmte Zweigstellen aus kostenmäßigen Gesichtspunkten und wegen des damit verbundenen erheblichen Aufwands auch personeller Art derzeit allgemein nicht zu verwirklichen ist. Diese Aussage ist angesichts der Tatsache, daß mandantenfähige Informationssysteme (vgl.1.2.2) ohne Verursachung unangemessener Kosten einsetzbar sind, sehr zu bedauern. Unter Berücksichtigung der deutlichen Verbesserung des Rechts auf informationelle Selbstbestimmung des Einzelnen erscheint dieser Aufwand durchaus vertretbar.

21.2 Elektronische Geldkarte

Die Kreditwirtschaft unterstützt nicht aktiv die Verwendung von Geldkarten, die nicht an ein bestimmtes Konto gebunden sind.

Bereits 1997 (16. TB, 21.2) wurde der unbefriedigende Zustand hinsichtlich der Verbreitung der kontoungebundenen Geldkarte bemängelt. Der zusätzliche Service, der mit der elektronischen Geldkarte verbunden ist, muß durchaus nicht gleichzeitig zu weniger Datenschutz führen (vgl. zu diesem allgemeinen Thema 1.). Auf unseren Vorschlag hat die Bürgerschaft den Senat ersucht, gegenüber den Hamburger Kreditinstituten darauf hinzuwirken, bei den Geldkarten als Wahlmöglichkeit auch die datenschutzfreundliche anonyme White Card anzubieten. In diesem Zusammenhang hatte die Wirtschaftsbehörde die Unternehmen angeschrieben. Die Antworten zeigten – wie auch schon die bundesweiten Gespräche mit der Kreditwirtschaft – daß die Frage, ob bei den Evidenzzentralen personenbezogene Daten anfallen (vgl. hierzu 14. TB, 25.1), immer noch nicht einheitlich beurteilt wird. Darüber hinaus wurde deutlich, daß die fehlende Nachfrage nach kontoungebundenen Karten nicht durch Werbung erhöht werden soll. Bundesweit sind nach den Informationen des Zentralen Kreditausschusses lediglich 1,5% aller ausgegebenen Geldkarten kontoungebunden.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer 55. Sitzung vom 19./20. März 1998 die Kartenherausgeber und die Kreditwirtschaft erneut dazu aufgefordert, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezogene Daten – sog. White Cards – anzubieten. Darüber hinaus hat die Arbeitsgruppe Kreditwirtschaft der Obersten Datenschutzaufsichtsbehörden der Länder zwischenzeitlich in ihren Sitzungen gegenüber der Kreditwirtschaft mehrfach darauf hingewiesen, daß es aus datenschutzrechtlicher Sicht erstrebenswert ist, den einzelnen Kunden die Möglichkeit zu geben, sich frei für eine kontogebundene oder kontoungebundene Geldkarte zu entscheiden.

Abzuwarten bleibt, ob sich die Erwartungen des Zentralen Kreditausschusses erfüllen, wonach eine höhere Inanspruchnahme der White Card erfolgt, wenn die freien Speicherplätze durch weitere Zusatzanwendungen (z.B. den elektronischen Fahrschein) genutzt werden. Im Rahmen eines Pilotprojektes der Bremer Kreditinstitute und der Bremer Straßenbahn wird derzeit schon die kontoungebundene Geldkarte als gleichwertige Alternative zur kontogebundenen Geldkarte vermarktet (zum HVV siehe nachstehend 22.1).

22. Handel und Verkehr

22.1 Bargeldloses Zahlungsverfahren beim Hamburger Verkehrsverbund (HVV)

Das bargeldlose Zahlungsverfahren beim HVV, über das wir im 13.TB (26.2.2) und im 16.TB (24.1) berichtet haben, ist inzwischen auf die Zahlungsmöglichkeit mit der EC-Geldkarte ausgeweitet worden. Aus datenschutzrechtlicher Sicht beinhaltet dieses Verfahren wegen der Abrechnung auf sogenannten „Schattenkonten" nach wie vor Risiken.

Fast alle Verkaufsgeräte des HVV in Bussen und Bahnen sind mittlerweile mit Lesegeräten sowohl für die Paycard und EC-Geldkarte ausgerüstet und in Betrieb genommen worden.

Das Zahlungsverfahren mit der Paycard stellt die datenschutzfreundlichere Variante dar, da es sich hierbei um eine sogenannte „White Card" handelt (siehe 16. TB, 24.1). Die Karte kann wie eine Telefonkarte mit einem Geldbetrag aufgeladen werden. Beim Bezahlen werden in den Verkaufsgeräten keine personenbezogenen Daten gespeichert.

Anders stellt sich die Situation bei der Zahlung mit der EC-Geldkarte dar. Auf der EC-Karte wird ein Chip mit einer bestimmten Summe aufgeladen, die dann beim Fahrscheinkauf jeweils „verbraucht" wird. Zu Abrechnungszwecken werden personenbezogene Daten erhoben und auf sogenannten „Schattenkonten" gespeichert. Bei der Zahlungsabwicklung mit der EC-Geldkarte werden zwei Zahlungsdatensätze erzeugt.

Dies ist zum einen der sogenannte „Transaktionsdatensatz", der den Evidenzzentralen der Kreditwirtschaft übermittelt wird. Dieser Datensatz enthält folgende Informationen:

- Datum und Uhrzeit des Fahrscheinkaufes
- Information, daß der Fahrschein mit dem Zahlungsmittel „Geldkarte" gekauft wurde
- Preisstufe
- Kennung des Automaten, der den Fahrschein ausgedruckt hat
- Nummer der EC-Karte und Bankleitzahl als personenbezogene Abrechnungsdaten.

Der HVV hat auf den Umfang dieser Datensätze keinen Einfluß, da sie in dieser Form von der Kreditwirtschaft zu deren Abrechnungszwecken gefordert werden. Appelle an die Kreditwirtschaft, auf diese Schattenkonten zu verzichten, haben bisher zu keinem befriedigenden Ergebnis geführt (siehe auch allgemein zur Thematik unter 21.2. und im 14. TB, 25.1.).

Beim Zahlen mit der EC-Geldkarte fällt daneben ein weiterer Datensatz an, der sogenannte „Händlerdatensatz". Dieser wird vom Automaten über eine definierte Schnittstelle zum Abrechnungssystem des Verkehrsunternehmens übertragen.

Es werden hier folgende Daten übermittelt:

- Datum und Uhrzeit des Fahrscheinkaufes
- Information, daß der Fahrschein mit dem Zahlungsmittel „Geldkarte" gekauft wurde
- Preisstufe
- Kennung des Automaten, der den Fahrschein ausgedruckt hat.

Dieser Datensatz enthält im Gegensatz zum Transaktionsdatensatz keine personenbezogenen Daten.

Nach Darstellung des HVV ist die Einführung des flächendeckenden bargeldlosen Zahlungsverfahrens erst ein Schritt auf dem Weg zur Entwicklung und Realisierung neuerer Möglichkeiten des bargeldlosen Fahrscheinverkaufes, die in den nächsten Jahren untersucht werden sollen. Zu nennen sind hier insbesondere der elektronische Fahrschein sowie damit verbundene Bonus- und Rabattsysteme. Zur Zeit finden zum „electronic ticketing“ und zum „Check-In-Check-Out-Verfahren“ Modellversuche in anderen Städten im In- und Ausland statt. Der HVV plant derzeit keine solchen Pilotprojekte. Wir werden die Entwicklung in Hamburg beobachten und aus datenschutzrechtlicher Sicht dazu ggf. Stellung nehmen und Anregungen geben.

Bei dem gegenwärtigen bargeldlosen Zahlungsverfahren ist es aus datenschutzrechtlicher Sicht zu begrüßen, daß für die Fahrgäste des HVV die Wahlmöglichkeit besteht, auf die datenschutzfreundliche Variante der PayCard zurückzugreifen, da hier im Gegensatz zur EC-Geldkarte keine personenbezogenen Daten erhoben und gespeichert werden.

22.2 E-Commerce

Der Datenschutz beim Teleshopping ist verbesserungsbedürftig.

Wir haben uns im Berichtszeitraum mit den Internetangeboten des Einzelhandels beschäftigt. Neben reinen Informationsdiensten bietet der Einzelhandel zunehmend Bestellmöglichkeiten über das Internet an. Die Kunden können in einem elektronischen Warenkatalog blättern, sich die verschiedenen Angebote ansehen und dann Waren bestellen, die ihnen per Post oder Zustelldienst geliefert werden.

Für die Erhebung und Verarbeitung von personenbezogenen Daten im Zusammenhang mit der Nutzung des Teleshopping sind die Vorschriften des TDDSG und ergänzend des BDSG zu beachten. Nicht alle Anbieter von Teleshopping halten sich an diese gesetzlichen Vorgaben.

Häufig werden für die Ausführung von Bestellungen mehr personenbezogene Daten erhoben als erforderlich. Ein Unternehmen bot zum Beispiel eine kostenlose Katalogbestellung über das Internet an und erhob dafür zwingend Daten über Alter der Besteller, Telefonnummer, Anzahl der Kinder und E-mail-Adresse. Die Erhebung dieser Daten war weder zur Durchführung des Teledienstes noch zur Zusendung des Katalogs notwendig. Dem Unternehmen ging es um den Aufbau einer Kundendatenbank zu Werbezwecken. Nachdem wir unsere Zweifel an der datenschutzrechtlichen Zulässigkeit der Erhebung wegen §3 Abs. 3 TDDSG und §28 Abs. 1 BDSG geäußert hatten, erklärte sich das Unternehmen bereit, künftig das Katalogangebot auf der Website zu ändern.

§3 Abs. 3 TDDSG: „Der Diensteanbieter darf die Erbringung von Telediensten nicht von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig machen, wenn dem Nutzer ein anderer Zugang zu diesen Telediensten nicht oder in nicht zumutbarer Weise möglich ist.“

Einige Unternehmen verwenden Cookies, ohne die Betroffenen darüber zu unterrichten. Unproblematisch ist das Setzen von Cookies, die nach der Beendigung der Sitzung wieder gelöscht werden. Werden permanente Cookies gesetzt, ist eine Information der Betroffenen nach §3 Abs. 5 TDDSG erforderlich.

§3 Abs. 5 TDDSG: „Der Nutzer ist vor der Erhebung über Art, Umfang, Ort und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten. Bei automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, ist der Nutzer vor Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muß für den Nutzer jederzeit abrufbar sein. Der Nutzer kann auf die Unterrichtung verzichten. Die Unterrichtung und der Verzicht sind zu protokollieren. Der Verzicht gilt nicht als Einwilligung im Sinne der Absätze 1 und 2."

Häufig verstoßen Unternehmen gegen die in §6 TDG vorgeschriebene Anbieterkennzeichnung. Danach haben Diensteanbieter für ihre geschäftsmäßigen Angebote Name und Anschrift sowie bei Personenvereinigungen und -gruppen auch Namen und Anschrift des Vertretungsberechtigten anzugeben. Bei mehreren von uns geprüften Angeboten war für die Nutzer nicht erkennbar, wer Diensteanbieter ist, d.h. insbesondere, wo sich Sitz und Verwaltung eines Unternehmens befinden, das die Daten erhebt.

§6 TDG: „Diensteanbieter haben für ihre geschäftsmäßigen Angebote anzugeben

1. Namen und Anschrift sowie

2. bei Personenvereinigungen und -gruppen auch Namen und Anschrift des Vertretungsberechtigten."

Bei der Nutzung des World Wide Web oder von E-Mail zur Übermittlung personenbezogener Daten an den Anbieter (z.B. im Rahmen einer Bestellung) kann eine Kenntnisnahme Dritter regelmäßig nicht ausgeschlossen werden, sofern keine geeigneten Maßnahmen getroffen wurden. Nach §4 Abs. 2 Nr. 3 TDDSG obliegt dies dem Anbieter. Zumindest in solchen Fällen, in denen sensible Daten übermittelt werden (z.B. zur Angebotserstellung für eine Krankenversicherung), ist daher für eine ausreichende Verschlüsselung auf dem Übertragungsweg zu sorgen, z.B. durch den Betrieb eines SSL-fähigen Web-Servers.

§4 Abs. 2 TDDSG: „Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, daß ...

3. der Nutzer Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann"

Wir werden unsere Prüfungen fortsetzen und intensivieren.

22.3 Kundenkarten

Der Einzelhandel erhält detaillierte Informationen über das Kaufverhalten einzelner Kunden durch Kundenkarten.

Große Einzelhandelsunternehmen und Kaufhäuser bieten ihren Kunden zunehmend eigene Kundenkarten an, die in allen Filialen bundesweit eingesetzt werden können. Je nach Ausgestaltung handelt es sich dabei um reine Bonuskarten mit Rabattfunktion oder um Kundenkarten mit Zahlungsfunktion. Beispielsweise werden beim Einkauf mit Bonuskarte dem Kundenkonto Bonuspunkte gutgeschrieben, über deren Stand er vierteljährlich unterrichtet wird. Beim kartengestützten Zahlungsverfahren erfolgt zusätzlich eine Abrechnung und ein Einzug der Forderung im Lastschriftverfahren.

Bei jedem Einkauf mit Karte werden personenbezogene Daten über Kaufdatum, Kartennummer, Betrag, Kassennummer, Abteilung und Warengruppe gespeichert. Anders als bei Barzahlungen, bei denen der Käufer anonym bleibt, erhält das Unternehmen so detaillierte Informationen über das Kaufverhalten des einzelnen Kunden. Diese Daten werden zu Kundenprofilen verdichtet und zu unternehmenseigenen Werbezwecken genutzt. Die Nutzung erfolgt im Rahmen des Vertragsverhältnisses zwischen dem Unternehmen und dem Kunden und ist nach §28 BDSG zulässig.

Kundenprofile sind für die werbende Wirtschaft insgesamt von großem Interesse. Bisher liegen uns noch keine Anhaltspunkte dafür vor, daß Kundenprofile, die bei kartengestützten Zahlungsverfahren gewonnen werden, an andere Unternehmen veräußert wurden. Ein Verkauf dieser personenbezogenen Daten wäre nach §28 BDSG unzulässig, wenn keine entsprechende Einwilligung vorliegt.

22.4 Gebäudedatenbank des Tele-Info Verlages

Das Fotografieren von Häusern und die Verwendung dieser Daten bringt die betroffenen Hauseigentümer und Bewohner aus dem Häuschen.

Das Vorhaben des Tele-Info Verlages in Garbsen bei Hannover, den Gebäudebestand aller Städte mit mehr als 20.000 Einwohnern komplett fotografisch in einer elektronischen Gebäudedatenbank zu erfassen und die so gewonnenen Daten kommerziell zu verwerten, hat sowohl bei den betroffenen Hauseigentümern als auch bei den Haus- und Grundeigentümerverbänden und den Medien bundesweit Aufsehen erregt.

Zahlreiche hamburgische Hauseigentümer und Bewohner haben sich bei uns beschwert, weil sie der Ansicht sind, daß durch die automatisierte Verarbeitung dieser Daten und die Verknüpfung der Bilddaten mit den dazugehörigen Adreßdaten (z.B. Postleitzahl, Orts- und Straßennamen, Hausnummer) ein Personenbezug zu bestimmten Personen (z.B. zu Hauseigentümern) hergeleitet werden kann und somit gegen datenschutzrechtliche Bestimmungen verstoßen wird. Außerdem haben sie erhebliche Sicherheitsbedenken, weil sie durch die kommerzielle Verwertung und unkontrollierte Verwendung dieser Daten eine Gefährdung ihres Eigentums und ihrer Persönlichkeitssphäre (z.B. durch kriminelle Aktivitäten) befürchten.

Der für den Tele-Info Verlag zuständige niedersächsische Landesbeauftragte für den Datenschutz ist bei seiner datenschutzrechtlichen Prüfung in Übereinstimmung mit dem niedersächsischen Innenministerium als der Obersten Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich zu dem Ergebnis gekommen, daß das Bundesdatenschutzgesetz in der derzeit geltenden Fassung auf die bisher bekannten Anwendungs- und Auswertungsmöglichkeiten der elektronischen Gebäudedatei nicht anwendbar ist, weil es sich nicht um eine Datei im Sinne von §3 Abs. 2 BDSG handelt.

Allerdings ist damit zu rechnen, daß der Dateibegriff im Rahmen der Anpassung des Bundesdatenschutzgesetzes an die EG-Datenschutzrichtlinie geändert wird, so daß es auf die Auswertungsmöglichkeit nicht mehr ankommt. Dies bedeutet allerdings noch nicht, daß die Datenverarbeitung dann unzulässig ist, sondern nur, daß die §§28 ff. BDSG zu beachten sind. Dieselbe Folge tritt ein, wenn die Funktionalität der Gebäudedatei so geändert wird, daß eine automatisierte Auswertung nach zwei Merkmalen möglich ist.

Für die Gebäudedatei gilt in diesen Fällen §29 BDSG (geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung). Bei der Speicherung und Übermittlung der Daten hat eine Abwägung der Interessen des Tele-Info Verlages und der Empfänger der Daten mit den Interessen der Betroffenen (z.B. Hauseigentümer) zu erfolgen. Im Rahmen der Interessenabwägung ist unter anderem zu berücksichtigen, daß nach bisheriger Rechtsprechung durch das Fotografieren eines Gebäudes Eigentumsrechte nicht berührt werden, da eine Einwirkung auf das Eigentum fehlt; denn beim Fotografieren eines Hauses von allgemein zugänglichen Stellen (z.B. öffentlich zugänglichen Straßen oder Wegen) wird weder die Sachsubstanz verletzt noch wird der Eigentümer hierdurch in der Nutzung der Sache und seinem Recht, mit dieser nach seinem Belieben zu verfahren, in tatsächlicher oder rechtlicher Hinsicht irgendwie beeinträchtigt (BGH NJW 1989, 2251, 2252).

Anders zu werten ist die Rechtslage aber hinsichtlich der Persönlichkeitsrechte der Betroffenen, insbesondere deren Recht auf informationelle Selbstbestimmung. Dieses könnte durch die Aufnahme der Gebäudefotos in eine Gebäudedatenbank verletzt sein, zumal es nach geltendem Recht keine Widerspruchsmöglichkeit dagegen gibt. Nach dem Bundesdatenschutzgesetz kann nur gegen die Nutzung der Daten zu Zwecken der Werbung und der Markt- und Meinungsforschung widersprochen werden, nicht dagegen gegen die Nutzung von Daten in digitalen Verzeichnissen. Widerspruchsmöglichkeiten, wie im Telekommunikationsbereich gegen die Aufnahme personenbezogener Daten in Telefonverzeichnisse, sind für das Vorhaben nicht einschlägig. Die dortige Widerspruchsmöglichkeit gegen die Aufnahme in ein solches Verzeichnis könnte ein Indiz dafür sein, daß das schutzwürdige Interesse des Betroffenen am Ausschluß der Veröffentlichung offensichtlich überwiegt. Die Aufnahme eines allgemeinen Widerspruchrechts aus überwiegendem schutzwürdigen Interesse gemäß der EG-Datenschutzrichtlinie in das novellierte Bundesdatenschutzgesetz bleibt abzuwarten.

Der niedersächsische Landesbeauftragte für den Datenschutz sieht jedenfalls zur Zeit keine Möglichkeit, auf der Grundlage des Datenschutzrechts gegen diese Aufnahmen vorzugehen und eine Löschung der Daten zu verlangen.

Der Verlag hat ohne Anerkennung einer Rechtspflicht angeboten, Widersprüche gegen die Speicherung einer Gebäudeaufnahme zu beachten. Bei vielen, die diese Möglichkeit nutzen, hat aber die Aufforderung des Verlages, ein Foto ihres Hauses vorzulegen, zu Verärgerung geführt. Da der Tele-Info Verlag keine Hausnummern und Straßennamen speichert und die Hausnummern in der Regel nicht zu erkennen sind, kann das betreffende Haus nur durch optischen Vergleich bestimmt werden. Der Einwand von Betroffenen, daß der Verlag mit der Vorlage des Fotos sein Ziel erreicht habe, ist nach Auffassung des niedersächsischen Landesbeauftragten für den Datenschutz unbegründet, weil ein solches Foto nicht für ein elektronisches Verfahren wie die elektronische Gebäudedatei verwendet werden kann.

Bei der gegenwärtigen Überarbeitung des BDSG (siehe 2.1) wird der Gesetzgeber zu entscheiden haben, inwieweit für neue Formen der kommerziellen Nutzung von digitalem Bildmateral über das private Umfeld bereichsspezifische rechtliche Schranken geschaffen werden. Die Datenschutzbeauftragten des Bundes und der Länder haben ihre Unterstützung angeboten, entsprechende Änderungsvorschläge mit vorzubereiten. Über das Vorhaben des Tele-Info Verlages und etwaige Änderungen des BDSG werden wir weiter berichten. Eine ausführlichere Darstellung dieses Themas ist bei uns auf Anfrage erhältlich.

23. Videoüberwachung

Die Videoüberwachung in Geschäften, Kaufhäusern und im öffentlichen Personennahverkehr nimmt, vor allem auch durch die Entwicklung neuartiger und preiswerterer Technik, zu. Damit verbunden sind auch rechtliche Probleme.

23.1 Rechtliche Grundlagen

Durch eine Videoüberwachung wird stets in das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) des davon betroffenen Personenkreises eingegriffen. Dieses ist gegen das Interesse desjenigen, der die Videoüberwachung vornehmen will, abzuwägen. Wir haben bereits im Jahre 1994 über Videoüberwachung in der Wirtschaft berichtet und dargelegt, unter welchen Voraussetzungen eine Videoüberwachung aus datenschutzrechtlicher Sicht zulässig ist. (vgl. 13.TB, 28.1)

Nunmehr ist auch im Entwurf des neuen Bundesdatenschutzgesetzes (Stand: Juli 1999) eine Vorschrift (§6 b BDSG neu) vorgesehen, die die Zulässigkeit der Videoüberwachung öffentlich zugänglicher Räume ausdrücklich regelt.

§6 b n.F.

Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit dies zur Aufgabenerfüllung, zur Wahrnehmung des Hausrechts oder zur Erfüllung eigener Geschäftszwecke erforderlich ist und keine Anhaltspunkte bestehen, daß schutzwürdige Interessen der betroffenen Personen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Speicherung von nach Absatz 1 erhobenen Daten ist zulässig, wenn dies zum Erreichen des verfolgten Zweckes erforderlich ist.

(4) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

In diesem Entwurf wird das Persönlichkeitsrecht der von der Videoüberwachung betroffenen Personen zwar berücksichtigt, jedoch nicht auf ganz zufriedenstellende Weise. Wir sind der Auffassung, daß die vorgesehene Zulässigkeit der Videoüberwachung „für jede Art der Aufgabenerfüllung“ zu weit geht. Statt dessen ist eine solche Maßnahme nur zum Schutz eigener wichtiger Interessen vertretbar.

23.2 Videoüberwachung in Wohnanlagen in Bergedorf und Wilhelmsburg

Bei zwei Neubauprojekten haben die verantwortlichen Wohnungsbaugesellschaften jeweils eine Videoüberwachung (der Wohnanlage bzw. von Teilbereichen der Wohnanlage) und die Einspeisung von Aufnahmen in das lokale TV- Kabelnetz der Haushalte in den jeweiligen Wohnanlagen vorgesehen.

Nach den Planungen der für das Bergedorfer Bauvorhaben zuständigen Wohnungsbaugesellschaft sollten eine Videokamera für Panorama-Aufnahmen der Wohnanlage und zwei Kameras für die Überwachung des zur Wohnanlage gehörenden Kinderspielplatzes eingesetzt werden. Wir haben deutlich gemacht, daß wir gegen die Panorama-Aufnahmen und deren Einspeisung in den lokalen TV-Kabelkanal keine datenschutzrechtlichen Bedenken haben, soweit durch die Aufnahmen aufgrund des hohen Standortes und des geringen Auflösungsgrades keine Identifizierung von Personen oder von Kfz-Kennzeichen möglich ist. Ob ein Personenbezug tatsächlich auszuschließen ist, werden wir vor Inbetriebnahme der Anlage prüfen.

Zur datenschutzrechtlichen Bewertung der geplanten Videoüberwachung des öffentlich zugänglichen Kinderspielplatzes wird auf die Ausführungen zu 1.2.1 verwiesen.

Mit der Videoüberwachung in Wilhelmsburg sollen die Hauseingänge, die Tiefgarageneinfahrt und die Tiefgarage kontrolliert werden. Damit sollen Störungen, die von Personen ausgehen, festgestellt und abgewehrt (z.B. Belästigungen von Mietern, Vandalismusschäden) bzw. begangene Straftaten in der Tiefgarage dokumentiert werden (z.B. Kfz-Aufbrüche), um so dem dortigen Risiko wirksam begegnen zu können.

Sämtliche Mieter der Wohn- und Garagenanlage sind über die Videoüberwachung schriftlich informiert worden, Neumieter werden bei Vertragsabschluß entsprechend informiert. Auf die Videoüberwachung in der Tiefgarage wird außerdem durch Hinweisschilder an den Eingängen aufmerksam gemacht. Die Kameras an den Hauseingängen sind für jeden deutlich sichtbar angebracht, so daß Fremde dadurch informiert sind, wenn sie sich in den Aufnahmebereich der jeweiligen Kamera begeben.

Die Aufnahmen aus der Tiefgarage werden nicht in den TV-Kabelkanal eingespeist, sondern zentral mit einem digitalen Aufzeichnungs-Recorder aufgezeichnet und im 5-Tage-Rhythmus automatisch überspielt und damit gelöscht. Die Auswertung erfolgt nur gezielt in begründeten Einzelfällen (z.B. bei gemeldeten betrieblichen Störungen oder vermeintlich strafrechtlichen Vorgängen). Eine Weitergabe der Aufzeichnungen soll im Bedarfsfall nur an die Polizei zur Verfolgung von Straftaten erfolgen.

Diese Videoüberwachung erfolgt mit Einwilligung der Mieter und soll insbesondere der Gefahrenabwehr dienen. Sie ist auf die eng begrenzten Hauseingänge und die Tiefgarage der Wohnanlage und somit auf den privaten Grund beschränkt. Bei der für die Videoüberwachung erforderlichen Güter- und Interessenabwägung sind wir zu der Auffassung gelangt, daß die Eigentumsrechte des Hauseigentümers und der Mieter höher zu bewerten sind als der damit verbundene Eingriff in das Persönlichkeitsrecht der potentiellen Straftäter und auch unverdächtiger Personen. Daher haben wir diese Videoüberwachung für zulässig erachtet.

Allerdings halten wir es für unverzichtbar, daß der Umgang mit dem Videosystem in einer Dienstanweisung geregelt wird, um die Persönlichkeitsrechte der Personen zu schützen, die nicht als Straftäter in Betracht kommen. Ein Entwurf der Dienstanweisung befindet sich zur Zeit in der endgültigen Abstimmung. Nach redaktioneller Überarbeitung durch die verantwortliche Wohnungsbaugenossenschaft soll uns die endgültige Fassung demnächst zugeleitet werden, so daß der Inbetriebnahme dieser Videoüberwachung keine Bedenken mehr entgegenstehen.

23.3 Weitere Einzelfälle

Viel beachtet wurde in jüngster Zeit, daß die Hamburger Hochbahn AG (HHA) einen Testversuch zur Videoüberwachung in U-Bahnen und Bussen durchführt. Zwei U-Bahn-Wagen und zwei Busse sind für eine Testphase von ca. einem Jahr mit Videokameras ausgestattet worden. Auch hier war das Persönlichkeitsrecht der betroffenen Fahrgäste mit dem Interesse der HHA an der besseren Aufdeckung von Straftaten abzuwägen. Aufgrund unserer Forderungen sind die betroffenen Fahrzeuge mit einem Hinweis auf die Videoüberwachung gekennzeichnet worden. Auch wird eine Betriebsvereinbarung zu den regelungsbedürftigen Einzelheiten des Umgangs mit der Videotechnik im Testversuch erstellt. Wir haben bisher aus datenschutzrechtlicher Sicht gegen eine Durchführung des Testversuches unter den oben dargestellten Bedingungen keine Bedenken geäußert.

Diese Bewertung ist aber nicht abschließend, da die Ergebnisse des Testversuchs ausgewertet werden sollen, bevor eine Entscheidung für oder gegen eine dauerhafte Einführung des Systems getroffen wird. Insbesondere haben wir uns für den Fall einer flächendeckenden Einführung einer Videoüberwachung in U-Bahn-Wagen und Bussen eine Stellungnahme aus datenschutzrechtlicher Sicht vorbehalten.

Eine weitere Problematik ergibt sich bei der Videoüberwachung des Hamburger Hauptbahnhofes. Hier stellt sich das Problem, daß dort mittlerweile sogenannte „DomeKameras“ eingesetzt werden, die für Laien nicht als Kameras erkennbar sind. Hinweise auf die Videoüberwachung finden sich im Bereich des Hauptbahnhofes nur vereinzelt und nicht an exponierter Stelle. Es bestehen daher Zweifel, ob die getroffenen Maßnahmen ausreichend sind, um auf den Umstand der Videoüberwachung hinzuweisen. Verhandlungen mit den Betreibern der Videoanlage und den für die Betreuung des Hauptbahnhofes zuständigen Stellen, wie der Kennzeichnungspflicht wirksamer nachgekommen werden kann, sind noch nicht abgeschlossen.

Fragen der Videoüberwachung von Mitarbeitern sind als Teilthema der Mitarbeiterkontrolle dargestellt (siehe 7.3.1).

24. Register nach §32 BDSG und Prüftätigkeit

24.1 Register und Meldepflicht

Die Aufsichtsbehörde führt nach §38 Abs. 2 BDSG ein Register der Stellen, die personenbezogene Daten zum Zwecke der personenbezogenen oder anonymisierten Übermittlung speichern oder im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen. Diese Stellen unterliegen nach §32 BDSG der Meldepflicht. Derzeit sind zu diesem Register 220 Unternehmen gemeldet. Unterteilt nach der Art der meldepflichtigen Tätigkeit ergibt sich folgendes Bild:

Speicherung zum Zwecke der Übermittlung	
Auskunfteien/Warndienste	11
Direktmarketing/Adreßhändler	31
Speicherung zum Zwecke der anonymisierten Übermittlung	
Markt- und Meinungsforschung	14
Auftragsdatenverarbeitung	
Servicerechenzentren	21
Akten- und Datenträgervernichter	11
Mikroverfilmer	5
Datenerfasser	20
sonstige Auftragsdatenverarbeitung	107

24.2 Prüfungen

Der folgenden Übersicht sind die Zahlen der Überprüfungen im Berichtszeitraum zu entnehmen, die gemäß §38 Abs. 2 BDSG regelmäßig vor Ort stattfinden:

Auskunfteien/Warndienste	5
Direktmarketing/Adreßhändler	13
Markt- und Meinungsforschung	8
Servicerechenzentren	10
Akten- und Datenträgervernichter	6
Mikroverfilmer	2

Datenerfasser	2
sonstige Auftragsdatenverarbeitung	13
Gesamt	**59**

Bürgerservice und die Dienststelle

25. Unterstützung der Bürgerinnen und Bürger

Die Zahl der Eingaben steigt weiter. Die Veranstaltungen und die Öffentlichkeitsarbeit finden gute Akzeptanz.

Weiterhin wenden sich täglich Bürgerinnen und Bürger mit ihren Datenschutzproblemen an uns. Dabei ergab sich mit 457 schriftlichen Eingaben im Jahr 1999 ein neuer Höchststand. Vielfach sorgten wir außerdem für telefonische und persönliche Beratungen. Wir haben Mitte 1999 begonnen, auch diese Unterstützung der Bürgerinnen und Bürger zahlenmäßig zu erfassen, und werden die Ergebnisse in den folgenden Berichten jeweils angeben.

25.1 Eingaben

Von Anfang Dezember 1997 bis Ende November 1999 gingen 850 schriftliche Eingaben ein. Sie betrafen – getrennt für die Jahre 1998 und 1999 – folgende Datenschutzbereiche, wobei eine Reihe von Eingaben mehrere Themen enthielten:

	1998	1999
Versicherungswirtschaft	22	30
Kreditwirtschaft	16	21
priv. Wohnungswirtschaft	10	9
Versandhandel	4	7
sonst. Handel	5	12
Werbung, Direktmarketing	31	50
SCHUFA, Auskunfteien	39	50
Markt- und Meinungsforschung	4	6
Vereine	10	11
freie Berufe	6	2
Soziales und Gesundheitswesen, nicht-öff.	14	17
Personaldatenschutz, nicht-öff.	8	16
Verkehrswesen, nicht-öff.	3	8
Sonstiges, nicht-öff.	12	13
Justiz	13	11
Strafvollzug	6	6
Sicherheitsüberprüfung	1	-
Verfassungsschutz	10	12
Polizei	43	33

Staatsanwaltschaft	7	10
Meldewesen	32	16
MDK, Kranken- und Pflegedienste	8	10
andere Sozialbereiche	12	23
Gesundheitswesen, öff.	17	18
Personaldatenschutz, öff.	11	19
Verkehrswesen, öff.	10	8
Ausländerwesen	8	8
Finanz-, Steuerwesen	1	2
Bildungswesen	4	6
Wirtschaftsverwaltung	4	3
Telekommunikation	9	13
Teledienste	1	27
Medien	8	5
Personenstandswesen	3	3
Statistik	1	2
Bau-, Vermessungswesen	6	4
Hochschulen	-	7
Scientology	2	-
Sonstiges, öff.	9	7

25.2 Veranstaltungen

Die Veranstaltungen der von mir mitgegründeten Hamburger Datenschutzgesellschaft waren jeweils gut besucht. Besonders zu danken ist dem 1. Vorsitzenden Rechtsanwalt Dr. Ivo Geis und dem Vorstandsmitglied Klaus Scharlibbe für ihren Einsatz.

Gemeinsam mit der Handelskammer Hamburg führten wir am 6. Mai 1998 eine ganztägige Tagung zum Thema „Kann moderne Technik unsere Daten schützen? Datenschutz für Online, Internet/Intranet, electronic commerce“ durch. Unter Beteiligung internationaler Vertreter, von Praktikern aus Unternehmen und von Landesdatenschutzbeauftragten wurde die neueste Datenschutztechnik vorgetragen und diskutiert.

Im Auditorium von Gruner + Jahr fand am 23. November 1998 eine Veranstaltung statt über „Die Zukunft der Informationsgesellschaft – Neue Chancen für die Bürger?“. Prof. Opaschowski vom BAT Freizeit-Forschungsinstitut sprach zunächst über „Der gläserne Konsument: ein Meinungsbild des Bürgers“ aufgrund einer repräsentativen Meinungsumfrage über die Einstellung zum Datenschutz. Anschließend erläuterte Dr. Binder als früherer Datenschutzbeauftragter des NDR das Spannungsverhältnis „Neue Dienste: Medienfreiheit und Privatsphäre“. Schließlich sprach Dr. Saxe als Leiter des Landesamtes für Informationstechnik über neue Chancen und Probleme im Verhältnis „Staat und Bürger: eine vernetzte Beziehung“.

Wiederum zusammen mit der Handelskammer führten wir am 21. Juni 1999 die Halbtagesveranstaltung „Datenschutz bei Chipkarten – Gesetzliche Anforderungen und praktische Umsetzung“ durch. Vertreter von Landesdatenschutzbeauftragten behandelten zunächst die datenschutzrechtlichen Anforderungen und die datenschutztechnischen Ausgestaltungen bei Chipkarten. Anschließend wurden praktische Anwendungen für multifunktionelle Chipkarten zum einen bei der UniHamburgCard vorgestellt und danach beim sog. Cartemonnaie, das von Herrn Dethloff als Miterfinder der Chipkarte entwickelt wurde.

Im Warburg-Haus hielt Prof. Bull am 22. September 1999 einen Vortrag zum Thema „Probleme und Scheinprobleme des Datenschutzrechts“. Dabei ging er auf die Kritik an den Rechtsinstituten des Datenschutzes ein und beschrieb die Chancen für das Datenschutzrecht. Seine Ausführungen wurden – unter Beteiligung mehrerer norddeutscher Datenschutzbeauftragter – intensiv diskutiert.

25.3 Öffentlichkeitsarbeit

Im Rahmen unserer Medienarbeit hatten wir Mitte 1998 die Ergebnisse der erwähnten bundesweiten Meinungsumfrage zum Datenschutz vorgestellt. Bei einer Repräsentativbefragung von 3.000 Personen hatten sich die Bürgerinnen und Bürger ganz überwiegend dafür ausgesprochen, daß der Datenschutz noch mehr Bedeutung bekommen sollte. Sie gaben auch an, daß sie überwiegend bereit seien, gegen Datenschutzverstöße aktiv vorzugehen. Viele wußten sich allerdings nicht zu helfen und kannten insbesondere nicht ihre Datenschutzrechte.

Wir haben deshalb bei dieser Gelegenheit erneut auf unser Datencheckheft „Kennen Sie Ihre Datenschutzrechte?“ hingewiesen. Das Heft war im Mai 1999 in 4. aktualisierter und erweiterter Auflage erschienen und wurde bei rund 70 öffentlichen Einrichtungen in Hamburg verteilt. Die Auflage beträgt mit der 5. Auflage von Anfang Dezember 1999 insgesamt 23.000 Exemplare.

Im Datencheckheft haben wir seit der 1. Auflage hervorgehoben, wie sich die Bürgerinnen und Bürger gegen adressierte Wahlwerbung der Parteien wenden können, indem sie Widerspruch gegen die Weitergabe ihrer Meldedaten an die Parteien einlegen (16. TB, 11.2). Durch unsere Aktivitäten und die wiederholten Berichte in den Medien hat sich die Zahl der Widersprüche von ursprünglich nur rund 900 bis Ende November 1999 auf ca. 12.500 erhöht.

Im Februar 1999 wurde unser „Bericht 1998“ mit einer Presseerklärung als Zwischenbericht über wichtige Ereignisse veröffentlicht. Diese Themen sind, soweit sie nicht bereits abgeschlossen werden konnten, im vorliegenden Tätigkeitsbericht mit der weiteren Entwicklung wiedergegeben.

Im Sinne unserer Kundenorientierung haben wir im März 1999 erstmals ein Informationsblatt herausgegeben „Was tun wir für Sie?“. Damit soll noch besser darüber informiert werden, wie wir – mit fast 20 Mitarbeiterinnen und Mitarbeitern – bei der Durchsetzung der Datenschutzrechte beraten, wie wir Verwaltung und Wirtschaft in Hamburg kontrollieren, welche Veröffentlichungen erhältlich sind und wer bei uns wofür zuständig ist. Das Faltblatt ist ebenso wie das Datencheckheft auch über das Internet abrufbar unter unserer Adresse www.hamburg.datenschutz.de.

Auf unserer Pressekonferenz zur Jahresmitte 1999 sind wir auf die Charta der Patientenrechte eingegangen, in die die Gesundheitsministerkonferenz auch wichtige Aspekte des Datenschutzes aufgenommen hat (siehe 17.2). Wir haben außerdem gemäß einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder eine wirksame Kontrolle von Lauschangriffen durch die Bürgerschaft gefordert, weil ein entsprechendes Ausführungsgesetz zur Unterrichtung des Parlaments über das Abhören von Wohnungen in Hamburg noch nicht vorlag (siehe 14.2). Ferner sind wir auf die zahlreichen Beschwerden zur Registrierung neuer Kunden bei Online-Diensten eingegangen, weil immer wieder nicht erforderliche personenbezogene Daten bei der Registrierung erhoben und gespeichert werden (siehe 3.8.2).

Bei einem Pressegespräch am 1. Dezember 1999 haben wir den Internet-Wettbewerb „Mehr Datenschutz – mehr eCommerce“ angekündigt, den wir gemeinsam mit der Hamburger Datenschutzgesellschaft und der Initiative Hamburg newmedia@work ab 1. Januar 2000 durchführen. Im Hauptwettbewerb sollen als Beiträge praktikable Lösungen für eine datenschutzfreundliche Nutzung des Internet im Bereich des eCommerce eingereicht werden; der Hauptpreis von 10.000 DM wird von der Vereinsbank gesponsert. Im Sonderwettbewerb werden Informationsangebote über Datenschutz im Internet mit Preisen von je 2.000 DM von Adecco und Network Associates gesponsert.

26. Entwicklung der Dienststelle

Für die Daueraufsicht über den Datenschutz in der Wirtschaft ist eine personelle Verstärkung dringend notwendig.

Die Pressekonferenz zur Jahresmitte 1999 habe ich zum Anlaß genommen, über die Gefährdung einer effektiven Datenschutzkontrolle in der Hamburger Wirtschaft zu berichten. Die EG-Datenschutzrichtlinie und das in der Novellierung befindliche Bundesdatenschutzgesetz schreiben vor, daß die Verarbeitung personenbezogener Daten durch die Wirtschaft künftig generell auf Datenschutzverstöße zu überprüfen ist. Damit soll die Wirtschaft in gleicher Weise wie schon seit langem der öffentliche Bereich nicht nur bei konkreten Anlässen, sondern ständig auf Einhaltung der Datenschutzvorschriften kontrolliert werden. Der Senat hatte es jedoch bei seinen Beratungen zum Haushaltsplanentwurf 2000 abgelehnt, dafür auch nur eine zusätzliche Stelle vorzusehen.

Bei der Novellierung des Hamburgischen Datenschutzgesetzes (HmbDSG) im März 1997 wurde ausdrücklich geregelt, daß ich meine Anliegen auch unmittelbar an die Bürgerschaft richten kann; §23 Abs. 3 Satz 3 HmbDSG besagt:

> „ ... er kann sich jederzeit an die Bürgerschaft wenden.“

Diese umfassende Aussage bezieht sich – ebenso wie in den entsprechenden Vorschriften und der Praxis bei den meisten anderen Datenschutzbeauftragten – auch auf Haushaltsangelegenheiten. Vergleichsweise bin ich auch in den Tätigkeitsberichten seit jeher auf die Entwicklung der Dienststelle mit ihrer Personalausstattung vor dem Hintergrund der haushaltsrechtlichen Regelung in §22 Abs. 2 HmbDSG eingegangen. Daraufhin wurde diese Thematik jeweils im zuständigen bürgerschaftlichen Ausschuß beraten.

Gemäß meinem Anrufungsrecht habe ich der Bürgerschaft – mit Schreiben an die Präsidentin und anschließend an die Vorsitzenden des Rechtsausschusses und des Haushaltsausschusses – vorgeschlagen, eine neue Stelle für die Daueraufsicht über die Wirtschaft in den Haushaltsplan aufzunehmen. Die Personalkosten sollen insbesondere durch neue Einnahmen aus Gebühren für Datenschutzprüfungen der Wirtschaft finanziert werden.

Geschäftsverteilung (Stand: 1. November 1999)

Der Hamburgische Datenschutzbeauftragte
Baumwall 7, 20459 Hamburg
E-Mail:mailbox@datenschutz.hamburg.de
Internet-Adresse: www.hamburg.datenschutz.de

Tel: 040/42841-2044
Fax: 040/42841-2372

		Durchwahl
Dienststellenleiter:	Dr. Hans-Hermann Schrader	-2044-
Stellvertreter:	Peter Schaar	-2231-
Vorzimmer:	Heidi Nieman	-2045-
Verwaltungsangelegenheiten der Dienststelle		-2563-
DV-Verfahren der Dienststelle		-2063-
Informationsmaterial		-2047- -2045-
Grundsatzfragen des Datenschutzrechts, Datenschutzgesetze, Parlamentsangelegenheiten, Justiz, Strafvollzug, Verfassungsschutz, Sicherheitsüberprüfungen Meldewesen, Wahlen und Volksabstimmungen, Ausweis- und Paßangelegenheiten		-2046-
Polizei und Feuerwehr, Staatsanwaltschaft, Straßenverkehrsverwaltung, Verkehrsordnungswidrigkeiten, Gewerbeaufsicht		-2581-
Bauen, Wohnen, Vermessungswesen, Personenstandswesen, Umwelt, Statistik, Finanz-, Steuer- und Rechnungswesen		-2223-
Grundsatzfragen, Telekommunikation, Medien, Teledienste technisch-organisatorische Beratung und Prüfung		-2231-
Zentrale Informationstechnik (LIT), private Rechenzentren, Archivwesen, IuK-Leitung, IuK-Planung, technisch-organisatorische Beratung und Prüfung		-2236-
Betriebssysteme, Netzwerke, Chipkarten, Verschlüsselungstechnik, technisch-organisatorische Beratung und Prüfung		-2564-
Gesundheitswesen, Forschung, Ausländerwesen, Kultur		

Soziales, Allgemeine Bezirksangelegenheiten, Bildungswesen, Freie Berufe, Handels- und Handwerkskammer, Vereine und Verbände, Kirchen

-2089-

Auskunfteien, SCHUFA, Kreditwesen

-2556-

Versicherungswirtschaft, Handel, Industrie

-2541-

Adreßhandel, Werbung, Markt- und Meinungsforschung, Transport und Verkehr, Wirtschaftsverwaltung

-2562-

Arbeitnehmerdatenschutz/Personalwesen, Auftragsdatenverarbeitung, Register nach § 32 BDSG

-2468-

Stichwortverzeichnis

Veröffentlichungen zum Datenschutz

Beim Hamburgischen Datenschutzbeauftragten können folgende Veröffentlichungen kostenlos abgeholt werden oder per Post gegen Einsendung von Briefmarken im Wert von DM 1,50 (bei * DM 3,00) angefordert werden:

Broschüren

Hamburgisches Datenschutzrecht

Datenschutz in der Arztpraxis

Datenschutz bei Multimedia und Telekommunikation

Datenscheckheft, 5. Auflage

Informationsblätter

Was tun wir für Sie?

Tips zum Adressenhandel *

Datenschutz im privaten Bereich

Handels- und Wirtschaftsauskunfteien

Der betriebliche Datenschutzbeauftragte

Internet

Informationen und Veröffentlichungen des Hamburgischen Datenschutzbeauftragten können auch im Internet unter – www.hamburg.datenschutz.de – abgerufen werden.

Verlags-Veröffentlichungen

Schrader Datenschutzrecht in Hoffmann-Riem, Koch (Hrsg.) Hamburgisches Staats- und Verwaltungsrecht, Nomos Verlag, 1998

Bäumler, Breinlinger, Schrader (Hrsg.) Datenschutz von A – Z, Loseblattwerk,

Luchterhand Verlag, 1999

Kühn, Schläger Datenschutz in vernetzten Computersystemen,

Datakontext-Fachverlag, 1997

Schlüsselbegriff Selbstbestimmungsrecht,

das Recht des Einzelnen, die eigenen Angelegenheiten frei und selbstverantwortlich zu gestalten

Neuen und entscheidenden Auftrieb erfuhr die Selbstbestimmungsidee durch die Philosophie der Aufklärung im 18. Jahrhundert, die das Schlagwort prägte >Bestimme dich aus dir selbst<. Obwohl die Aufforderung mit ethischen Postulaten verknüpft war, die sich an den Einzelnen richteten, hatte sie dennoch auch einen politischen Aspekt: denn aus ihr ergab sich zwangsläufig die an den Staat gerichtete Forderung, die freie Entfaltung der Persönlichkeit des Einzelnen - unter Beachtung der durch das Gemeinwohl gesetzten Schranken - nicht nur zu dulden, sondern auch zu garantieren.

In diesem Sinne garantiert Art. 2 Abs. 1 GG das Recht eines jeden Menschen >auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt<. Mithilfe dieser Formel versucht das Grundgesetz, wie jede andere freiheitlich-rechtsstaatliche Verfassung, die Spannung zwischen individueller Autonomie und äußeren Bindungen zu lösen. Das Ringen um diese Problemlösung steht aber schon seit dem 19. Jahrhundert. nicht mehr unter dem Zeichen eines >individuellen Selbstbestimungsrecht<, sondern unter demjenigen des Persönlichkeitsrechts. Erst in jüngster Zeit ist der Ausdruck >Selbstbestimungsrecht< erneut auch im Bereich der individuellen Grundrechte verwendet worden, und zwar im Begriff des Rechts auf informationelle Selbstbestimmung.

(Auszug aus Brockhaus Enzyklopädie in 24 Bänden, 20. Aufl.)