BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG **Drucksache 15/320**

15. Wahlperiode **12. 01. 94**

Der Hamburgische Datenschutzbeauftragte

An die
Frau Präsidentin der Bürgerschaft

Betr.: 12. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

Gemäß § 23 Hamburgisches Datenschutzgesetz übersende ich der Bürgerschaft den 12. Tätigkeitsbericht*.

Dem Senat leite ich den Tätigkeitsbericht gleichzeitig zu.

Dr. Schrader

* Verteilt nur an die Abgeordneten der Bürgerschaft

Bürgerschaftsdrucksachen — außer Senatsvorlagen — sind — gedruckt auf chlorfrei gebleichtem Papier — zu beziehen bei Druckerei Wattenberg & Söhne GmbH Theodorstraße 41 w, 22761 Hamburg, Telefon 89 97 90-0

12. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten zugleich Tätigkeitsbericht der Aufsichtsbehörde für den nicht-öffentlichen Bereich

vorgelegt im Januar 1994
(Redaktionsschluß: 3. Dezember 1993)

Dr. Hans-Hermann Schrader

INHALTSVERZEICHNIS

Einzelne Probleme des Datenschutzes im öffentlichen Bereich

12. Tätigkeitsbericht 1993 HmbDSB

Einzelne Probleme des Datenschutzes im nichtöffentlichen Bereich

Zusammenfassung wichtiger Punkte

Grundrecht auf Datenschutz Die Aufnahme des Grundrechts auf Datenschutz in das Grundgesetz ist spätestens dann unerläßlich, wenn es zu Einschränkungen des Datenschutzes durch Zulassung des Lauschangriffs mit einer Änderung des Art. 13 GG kommt. Die schlechteste Variante muß vermieden werden: eine derart weitreichende Grundgesetzänderung mit Einschränkung des Persönlichkeitsrechts und immer noch keine Verankerung des Grundrechts auf Datenschutz im Grundgesetz (1.1).

Recht auf eigene Darstellung Die Rechte des Betroffenen könnten durch ein Recht auf eigene Darstellung gegenüber der speichernden Stelle verstärkt werden. Dieses Recht führt über die bisherigen Auskunfts- und Abwehrrechte hinaus zu einem aktiven Gestaltungsrecht im Sinne der informationellen Selbstbestimmung (1.3).

Untersuchungsausschußgesetz Für den Bereich der Bürgerschaft ist eine umgehende gesetzliche Regelung des Datenschutzes bei Untersuchungsausschüssen angebracht. Dabei ist dem Recht des Parlaments zur Aufklärung von Mißständen, aber auch dem Schutz der personenbezogenen Daten der Betroffenen Rechnung zu tragen (1.5.2).

Grundschutzkonzept Bei dem Ausbau der IuK-Infrastruktur muß mit technischen und organisatorischen Maßnahmen von vornherein ein ausreichendes Niveau der Datensicherheit gewährleistet werden. Schutzkonzepte haben davon auszugehen, daß auch sensible personenbezogene Daten verarbeitet werden. Zu fordern ist ein standardmäßig hoher Grundschutz, auf den nach Bedarf weitere Sicherheitsmaßnahmen aufgesetzt werden können (3.2).

Mobilfunk Die mit der Nutzung von Mobilfunkdiensten verbundenen Risiken – Gefährdung der Vertraulichkeit der Kommunikation und Bildung von Bewegungsprofilen – müssen soweit wie möglich abgestellt werden. Die Betreiber müssen ihre Kunden auf die Gefährdungen hinweisen (4.1).

Persönlichkeitsrechte in den Medien Rundfunk- und Fernsehsendungen – z.B. Reality TV – können Persönlichkeitsrechte beeinträchtigen. Obwohl für die Berichterstattung der elektronischen Medien weitgehend die Datenschutzvorschriften aufgrund des „Medienprivilegs" nicht gelten, können Betroffene ihre Rechte durch Auskunft, Gegendarstellung, Berichtigung und Hinzufügung einer eigenen Darstellung durchsetzen (4.3).

Umweltdatenverarbeitung Im Umweltbereich werden in großem Umfang personenbezogene Daten zum Teil noch ohne gesetzliche Grundlage verarbeitet. Es fehlt insbesondere nach wie vor ein Hamburgisches Bodenschutzgesetz (5.1).

Umfang der Auskunftspflicht bei Sozialhilfe Unterhaltspflichtige von Sozialhilfeempfängern müssen keine Auskunft über die Einkommens- und Vermögensverhältnisse ihrer Ehegatten geben (6.8.1).

Personalärztlicher Dienst Die Aufklärung des zu Untersuchenden über das Verfahren, die Fristen zur Aufbewahrung der Untersuchungsunterlagen, die Mitteilung von „Risikofaktoren" an die Beschäftigungsbehörde und die Einsichtnahme in die Probandenakten wurden einvernehmlich geklärt. Überarbeitet werden sollen darüber hinaus die Anamnese-Fragebogen des Personalärztlichen Dienstes und anderer ärztlicher Dienste (7.3).

Personaldatenverarbeitung bei den Personalräten Die Einführung eines Stammdatensatzes über die Beschäftigten, den die Personalräte unabhängig von einer Beteiligung im Einzelfall ständig verarbeiten dürfen, wird zur Zeit geklärt. Angestrebt wird eine einheitliche und klare Regelung, die dem informationellen Selbstbestimmungsrecht der Beschäftigten und auch dem Informationsanspruch des Personalrats gerecht wird (7.8).

Keine Meldeauskünfte an Parteien Rechtzeitig vor den Wahlen zum Europaparlament und zum Deutschen Bundestag ist entschieden worden, daß keine Melderegisterauskünfte mehr an Parteien erteilt werden (13.2.2).

Textverarbeitung bei der Polizei Die Einführung von PC's im Polizeivollzug darf nicht dazu führen, daß mit Hilfe der automatisierten Textverarbeitung erstellte Texte auf Dauer gespeichert werden. Hierdurch würden Speicherfristen und Zugriffsbeschränkungen für sensible polizeiliche Vorgänge unterlaufen (17.1.2).

Zuhälter- und Milieukartei Prostituierte dürfen in polizeilichen Dateien nicht allein wegen ihrer Tätigkeit gespeichert werden, sondern nur dann, wenn besondere Gründe der Verbrechensbekämpfung im Zuhältermilieu dies erfordern (17.5).

Datenschutz für Polizeibedienstete Polizeiinterne Mitteilungen über Strafanzeigen gegen Polizeibedienstete müssen wesentlich reduziert und nach Anlässen und Adressaten differenziert werden (17.10).

Justizvollzugsanstalten Eine Querschnittsprüfung der Datenverarbeitung von Justizvollzugsanstalten ergab erhebliche Mängel bei der Datensicherheit, insbesondere der Zugangskontrolle. Außerdem fehlen detaillierte gesetzliche Regelungen über die Art der Unterlagen, die in die Gefangenenpersonalakte aufzunehmen sind (20.2).

Hygienisches Institut Eine Reihe organisatorischer und datensicherheitstechnischer Verbesserungen zum Schutz der sensiblen Gesundheitsdaten wurde erreicht. Die Frage nach einer grundsätzlich anonymisierten Labor-Auftragserteilung und -durchführung ist weiter zu klären (21.8).

Euroscheck-Karten Die zunehmende Verwendung von Euroscheck-Karten im bargeldlosen Zahlungsverkehr darf nicht zum „gläsernen Verbraucher" führen (26.1). Problematisch ist deshalb auch der beabsichtigte bargeldlose Fahrkartenverkauf im Nahverkehr (27.1).

1. Zur Lage des Datenschutzes

1.1. Grundrecht auf Datenschutz

Nach der Entschließung der Datenschutzbeauftragten vom 28. April 1992 zum Grundrecht auf Datenschutz (siehe dazu 11. Tätigkeitsbericht – TB –, 1.3 mit näherer Begründung) hat sich die Gemeinsame Verfassungskommission von Bundesrat und Bundestag intensiv mit den Themen Informationelle Selbstbestimmung, Datenschutzbeauftragter, Auskunfts- und Datenzugangsrechte in mehreren Sitzungen befaßt.

Am 11. Februar 1993 ist über die Anträge abgestimmt worden. Dabei hat der nachstehende Vorschlag der SPD als einer der wenigen Anträge in der Verfassungskommission eine absolute Mehrheit erhalten, nicht aber die Mehrheit von 2/3 der Kommissionsmitglieder, die für einen Vorschlag zur Verfassungsänderung notwendig ist:

„Artikel 2a

(1) Jeder Mensch hat das Recht, über die Erhebung und Verarbeitung seiner persönlichen Daten selbst zu bestimmen. Jeder Mensch hat das Recht auf Auskunft über die Erhebung und Verarbeitung seiner persönlichen Daten und auf Einsicht in amtliche Unterlagen, soweit diese solche Daten enthalten.

(2) Diese Rechte dürfen nur durch Gesetz oder auf Grund eines Gesetzes eingeschränkt werden, soweit überwiegende Interessen der Allgemeinheit es erfordern.

Artikel 5

(2a) Jeder Mensch hat das Recht auf Zugang zu den Daten der vollziehenden Gewalt, soweit nicht schutzwürdige öffentliche Interessen oder Rechte Dritter verletzt werden. Das Nähere regelt ein Gesetz.

Artikel 45d

Der Bundestag wählt einen Bundesbeauftragten für den Datenschutz und Informationsfreiheit mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder für eine Amtszeit von 5 Jahren. Einmalige Wiederwahl ist zulässig. Der Bundesbeauftragte ist in der Ausübung seines Amtes unabhängig, frei von Weisungen und nur dem Gesetz unterworfen. Er kann sich jederzeit an den Bundestag wenden. Das Nähere regelt ein Gesetz."

Im Abschlußbericht der Verfassungskommission vom 28. Oktober 1993 ist es bei diesem Ergebnis geblieben. Demgemäß wird in dem Bericht keine Verfassungsergänzung vorgeschlagen. Es werden lediglich die Anträge und die Stellungnahmen mit Befürwortung und Gegenansicht dargestellt. Infolgedessen bleibt die Aufnahme des Grundrechts auf Datenschutz der weiteren Beratung der Verfassungsreform im Bundestag und im Bundesrat überlassen. Die Gruppe Bündnis 90/Die Grünen hat bereits am 20. September 1993 den Ent-

wurf eines Gesetzes zur Änderung des Grundgesetzes, mit dem der Datenschutz als Grundrecht in Art. 2a GG aufgenommen werden soll, in den Bundestag eingebracht (Drucksache 12/5695). Die SPD-Bundestagsfraktion hat einen Gesetzentwurf zur Grundgesetzergänzung gemäß dem obigen Vorschlag am 1. Dezember 1993 vorgelegt (Drucksache 12/6323).

Zur weiteren öffentlichen Behandlung hat auf meine Initiative am 11. Oktober 1993 ein Symposium mit Mitgliedern der Gemeinsamen Verfassungskommission einschließlich der Justizsenatorin über das „Grundrecht auf Datenschutz im Grundgesetz" stattgefunden.

Im Zusammenhang mit der aktuellen Diskussion über den Lauschangriff habe ich meine Auffassung auch bei dieser Gelegenheit eingebracht. Ich halte die Aufnahme des Grundrechts auf Datenschutz in das Grundgesetz spätestens dann für unerläßlich, wenn es zu Einschränkungen des Datenschutzes mit einer grundgesetzlichen Zulassung des Lauschangriffs durch Änderung des Art. 13 GG kommt. Es wäre nicht verständlich und vertretbar, wenn das Grundrecht auf Unverletzlichkeit der Wohnung und damit auch das Persönlichkeitsrecht – mehr oder weniger differenziert – eingeschränkt würde und andererseits die Aufnahme des Grundrechts auf informationelle Selbstbestimmung in das Grundgesetz weiter abgelehnt würde.

Damit wird nicht etwa ein Kompromißvorschlag gemacht, daß die Grundrechtseinschränkung bei Art. 13 GG gegen eine Grundgesetzergänzung mit einem Art. 2a GG hinzunehmen wäre. Vielmehr soll mit diesem Junctim erreicht werden, daß dem Bürger nicht die schlechteste Variante zugemutet wird: eine Grundgesetzänderung mit Einschränkung seines Persönlichkeitsrechts und immer noch keine Verankerung seines Grundrechts auf Datenschutz im Grundgesetz.

Auf dem Symposium haben dann nach einer Einleitung von Prof. Simitis die Sprecher der im Bundestag vertretenen Fraktionen sowie die Justizsenatorin ihre Positionen verdeutlicht.

In der Diskussion wurde betont, daß das Grundrecht auf Datenschutz das einzige moderne Grundrecht wäre, dessen ausdrückliche Aufnahme in das Grundgesetz zu erwägen ist. Hinsichtlich des „Mehrwertes" einer solchen Aufnahme in das Grundgesetz wurde herausgestellt, daß damit die Verfassungsrechtsprechung verfestigt würde, zugleich ein Signal für die Bedeutung dieses Grundrechts mit Auswirkung auf Rechtsprechung und Praxis gegeben würde und außerdem die Grundrechtsregelungen in verschiedenen Landesverfassungen insbesondere in den neuen Ländern bestätigt würden.

Im Ergebnis bestand inhaltlich Einigkeit, daß die von der SPD vorgeschlagene Formulierung für einen Art. 2a GG mit der Rechtsprechung des Bundesverfassungsgerichts übereinstimmt. Dennoch blieb es dabei, daß seitens der CDU/CSU-Fraktion und möglicherweise auch mehrheitlich der F.D.P.-Fraktion zur Zeit keine Bereitschaft zu einer förmlichen Ergänzung des Grundgesetzes besteht, weil dies von ihnen als überflüssig angesehen wird.

Das weitere Thema eines „Rechts auf Zugang zu den Daten der Verwaltung (Aktenöffentlichkeit, Informationsfreiheit)" gemäß der Entschließung der Datenschutzbeauftragten vom 28. April 1992 (11. TB, 1.3) ist in der Verfassungskommission mit dem oben wiedergegebenen SPD-Antrag aufgegriffen worden. Danach hat jeder Mensch das Recht auf Zugang zu den Daten der vollziehenden Gewalt, soweit nicht schutzwürdige öffentliche Interessen oder Rechte Dritter verletzt werden.

Wegen der vorrangigen Behandlung des Grundrechts auf Datenschutz im Grundgesetz ist dieses weitere Thema von den Datenschutzbeauftragten noch nicht vertieft worden. Der Grundgedanke wird aber im Zusammenhang mit dem Umweltinformationsgesetz (siehe unten 5.2) als einem bereichsspezifischen Ansatz weiter verfolgt.

1.2 Schwerpunkt Volkszählungsurteil und Datenschutzentwicklung

Vor 10 Jahren, am 15. Dezember 1983, hat das Bundesverfassungsgericht in den Leitsätzen zum Volkszählungsurteil die verfassungsrechtlichen Grundlagen des Datenschutzes festgehalten: „Das Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig."

Angesichts der aktuellen Entwicklung ist festzustellen, daß dieses Grundrechtsverständnis – mit der Selbstbestimmung des Bürgers als Regelfall und ihrer Einschränkung als Ausnahme – keineswegs als Selbstverständlichkeit akzeptiert ist. Vielmehr wirkt sich auch auf den Datenschutz die Tendenz aus, weg von einer angeblich egozentrischen Selbstbestimmung hin zu einer stärker betonten Gemeinschaftsverantwortung zu kommen. Dabei werden Individualrechte vielfach ohne zwingende Gründe zugunsten staatlicher Eingriffsrechte zurückgedrängt.

Es wird verkannt, daß in der Informationsgesellschaft der effektive Schutz der persönlichen Daten die Voraussetzung für eine breite Teilnahme der Bürger an der Gesellschaft ist. Nur wenn der Bürger sicher sein kann, daß seine dem Staat und der Wirtschaft überlassenen Daten soweit wie möglich geschützt werden, nimmt er aktiv am Gemeinschaftsleben teil. Nach wie vor gilt dafür der Satz von Prof. Simitis: „Datenschutz ist Demokratieschutz."

Zugleich ist Datenschutz auch Freiheitsschutz. Der Bürger kann seine Freiheit zur Kommunikation (und umgekehrt ebenso seine Entscheidung zur Freiheit von Kommunikation) nur verwirklichen, wenn der Staat seine Schutzpflichten für die Daten der Bürger ernst nimmt. In der Gesetzgebung sind demgegenüber inzwischen wiederholt die Leitsätze des Bundesverfassungsgerichts als Einladung mißverstanden worden, die informationelle Selbstbestimmung als ein Recht unter scheinbar unbeschränktem Gesetzesvorbehalt zu behandeln und den bestehenden Datenschutz zum Teil erheblich zu verschlechtern.

Aus dieser Situation des Datenschutzes hat sich das Querschnitt-Thema „10 Jahre Volkszählungsurteil und die Folgen" für den TB ergeben. Dabei wird in den einzelnen Bereichen jeweils als Schwerpunkt der Datenschutzabbau, oft in Verbindung mit einem Technikausbau, wiedergegeben. Andererseits wird auf die – oft mühsam – erreichten Datenschutzverbesserungen eingegangen.

Besonders drastische Beispiele für den Datenschutzabbau im Bundesbereich sind das Gesundheitsstrukturgesetz (21.1), die Sozialgesetzgebung einschließlich des Föderalen Konsolidierungsprogramms (6.2) und die Regelungsvorschläge zum Lauschangriff (19.1). Der Datenschutzabbau durch gesetzliche Vorschriften wiederholt sich dabei regelmäßig auf dieselbe Weise: Ein nachvollziehbares Allgemeininteresse wie die Kostenbegrenzung im Gesundheitswesen, weniger Sozialhilfemißbrauch oder eine wirksame Verbrechensbekämpfung führen dazu, zusätzliche persönliche Daten oft ohne Kenntnis des Betroffenen zu sammeln und möglichst automatisiert abzugleichen, auch wenn dadurch vielfach unbeteiligte Personen einbezogen werden.

Die grundlegende Kritik an diesem Verfahren hat der Bundesrat bei der neueren Sozialgesetzgebung zusammengefaßt: „Der vorgesehene Datenabgleich wird in der großen Mehrzahl völlig unverdächtige Personen, d.h. korrekte Antragsteller erfassen. Der damit verbundene Eingriff muß auf das zwingend erforderliche Maß beschränkt werden." Vergleichbar liegt bei den Vorschlägen zum Lauschangriff das Problem vor allem darin, daß auch unverdächtige oder unschuldige Bürger in der Wohnung heimlich abgehört werden können.

Es wird bei der weiteren Gesetzgebung unverändert darauf zu achten sein, daß der Grundsatz der Verhältnismäßigkeit – gemäß den Leitsätzen des Volkszählungsurteils – eingehalten wird. Dabei gibt es keine Begründungspflicht für die Erhaltung des Grundrechts auf Datenschutz, sondern immer nur einen Begründungszwang für Einschränkungen des Grundrechts als Ausnahme von der Regel. Das Bundesverfassungsgericht hat dazu verdeutlicht, daß „die Einschränkung nicht weiter gehen darf, als es zum Schutze öffentlicher Interessen unerläßlich ist".

Die Regelungen zum Datenschutzabbau gehen einher mit dem Einsatz neuer Technik. So führen z.B. programmierbare Chipkarten zu zusätzlicher Automatisierung, bei der personenbezogene Daten nunmehr verstärkt dezentral erhoben und zugleich verarbeitet werden können. Rechnernetze sorgen für eine Funktions- und Datenintegration in bisher getrennten Bereichen. Problematisch ist dabei für den Datenschutz die Art und Weise des Chipeinsatzes, auf denen eine Vielzahl persönlicher Daten gespeichert werden kann. Aus der Wirtschaft ist dafür der vom Hamburger Verkehrsverbund geplante bargeldlose Fahrkartenverkauf mittels eines zusätzlichen Chips auf der Euroscheck-Karte ein anschauliches Beispiel (siehe 27.); das Fahrverhalten des Bürgers soll automatisiert erfaßt und mit den Kontendaten zusammengeführt werden.

Für den öffentlichen Bereich haben wir im Anschluß an die Darstellung im 11. TB (insbesondere 3.1) in dem „Bericht über den Datenschutz bei Automation und Vernetzung der hamburgischen Verwaltung – IuK-Datenschutzbericht –" vom 9. Juli 1993 die Problemlage bei einer landesweiten Vernetzung mit den Auswirkungen auf die parlamentarische Kontrolle der Verwaltung und mit den Anforderungen an die Gesetzgebung behandelt. Diese Thematik wird zusammen mit dem Ansatzpunkt, einen vorgezogenen Datenschutz rechtlich und tatsächlich sicherzustellen (11. TB, 1.1), auch in diesem TB weiter verfolgt (1.4 und 3.1).

1.3 Weiterer Schwerpunkt „Recht auf eigene Darstellung"

Das Bundesverfassungsgericht hat bereits im Volkszählungsurteil festgestellt und in einem späteren Beschluß näher ausgeführt (NJW 1989, 3269), daß personenbezogene Informationen ein „Abbild sozialer Realität" darstellen, über das der Betroffene nicht ausschließlich bestimmen kann. Durch die sozialen Beziehungen in Kommunikation mit anderen ergibt sich ein soziales Abbild, „das dem Betroffenen ungeachtet etwa abweichender oder entgegenstehender eigener Vorstellungen und Absichten zugerechnet wird" und das sich in gewissem Umfang verselbständigt.

Der Betroffene steht damit aber nicht etwa schutzlos da. Er kann sich laut Bundesverfassungsgericht dagegen wenden, daß die ihm allein „zustehende Entscheidung über das Ob und Wie seiner Persönlichkeitsdarstellung unterlaufen und verfälscht wird".

Im Zuge der Automatisierung besteht verstärkt die Gefahr, daß die personenbezogenen Informationen in ihrer ursprünglichen Bedeutung verkürzt werden (Kontextverlust). Durch die Informationsverwendung mit reduziertem Kontext kann sich nicht nur die Gefahr ergeben, daß der Betroffene zum „gläsernen" Menschen wird; vielmehr besteht außerdem die noch größere Gefahr, daß er zu einem „anderen" Menschen wird.

Daher ist die Kenntnis des einzelnen durch Auskunfts- und Akteneinsichtsrechte und seine Einwirkung durch Berichtigungsrechte stärker abzusichern. Über diese Rechte hinaus muß der Betroffene die Möglichkeit zur Interpretation mit Alternativvorstellungen bei den Dritten haben, die die Information über ihn besitzen. Dies kann zum Beispiel durch ein Recht auf Hinzufügung einer eigenen Darstellung geschehen.

In den einschlägigen Abschnitten dieses TB ist jeweils die Frage behandelt worden, inwieweit eine solche gesetzliche Regelung des Rechts auf eigene Darstellung bereits besteht oder aber künftig eingeführt werden könnte. Im Bundesdatenschutzgesetz mit der Regelung für Archive in § 35 Abs. 5 BDSG und der Medienvorschrift in § 41 Abs. 2 BDSG sowie in den Rundfunkgesetzen und -staatsverträgen (siehe 4.3) finden sich derartige Bestimmungen. Am weitesten ist das Recht auf eigene Darstellung in den neuen Beamten- und Arbeitnehmerregelungen des Bundes- und Landesrechts insbesondere zur Personalakte (siehe 7.2.3) ausgestaltet. Außerdem wird das Thema z.B. bei der Schufa

(siehe 23.4), der Versicherungswirtschaft (siehe 24.8.5) und den Auskunfteien (siehe 25.2.6) relevant.

Überwiegend wird dieses Recht bisher im Zusammenhang mit dem Berichtigungsrecht behandelt. Dann ist Voraussetzung, daß die Daten unrichtig sind oder deren Richtigkeit bestritten ist. Die Besonderheit des Rechts auf eigene Darstellung besteht in diesem Falle darin, daß nicht lediglich die speichernde Stelle die jeweiligen Daten im ursprünglichen Text berichtigt oder sperrt; vielmehr kann der Betroffene seine eigene Darstellung den Daten der speichernden Stelle hinzufügen.

Es gibt aber durchaus andere Fälle, in denen richtige Daten einen unvollständigen oder mißverständlichen Eindruck hinterlassen. Das Recht auf eigene Darstellung würde dann bedeuten, eine ergänzende oder anders akzentuierte Stellungnahme zu den Fakten abzugeben. Bei dem Gegendarstellungsrecht in Presse und Rundfunk kommt es ebenfalls nicht auf die Richtigkeit oder Unrichtigkeit der angegriffenen Darstellung an; der Betroffene kann vielmehr ohne weiteres seine Darstellung dagegen setzen.

Soweit es sich dabei um verkürzte und durch diese Verkürzung verfälschte Daten handelt, mag das Berichtigungsrecht im Wege der Auslegung als Recht auf Ergänzung durchsetzbar sein. Allerdings besteht dann kein Anspruch auf Hinzufügung einer eigenen Darstellung, bei der die Textfassung des Betroffenen zu den Unterlagen zu nehmen ist. Erst recht kann es nicht mehr um eine Ausgestaltung des Berichtigungsrechts gehen, wenn die Begründetheit und Richtigkeit der Daten zugrunde gelegt wird (siehe 7.2.3).

Das Recht auf eigene Darstellung setzt dabei jeweils voraus, daß eine andere Darstellung bereits vorhanden ist. Unberührt davon bleiben die bereits bestehenden Vorschriften, wonach personenbezogene Daten grundsätzlich beim Betroffenen mit seiner Kenntnis erhoben werden sollen und nur unter bestimmten Voraussetzungen ohne seine Kenntnis bei anderen Stellen erhoben werden dürfen (§ 12 Abs. 2 HmbDSG). Wenn die Daten beim Betroffenen in der dafür festgelegten Weise (§ 12 Abs. 3 HmbDSG) erhoben werden, wäre es nur konsequent, daß der Betroffene von Anfang an die Möglichkeit zur eigenen Darstellung hat. In diesem Sinne sprechen schon die bisherigen Regelungen dafür, daß die Erhebung nicht einseitig ohne Einwirkungsmöglichkeit des Betroffenen stattfindet.

Während dem Betroffenen bisher mit den Rechten auf Auskunft, Berichtigung, Sperrung und Löschung nur Reaktionen hinsichtlich der eigenen Daten möglich sind, führt das Recht auf eigene Darstellung zu einem aktiven Gestaltungsrecht. Dem Grundgedanken des Selbstbestimmungsrechts gemäß dem Bundesverfassungsgericht, „selbst über die Verwendung seiner persönlichen Daten zu bestimmen", wird damit entsprochen.

Es bedarf der weiteren Erörterung und Klärung, ob für dieses Recht auf eigene Darstellung nur bereichsspezifische Regelungen in Betracht kommen. Weiterführend wäre demgegenüber die Überlegung, den generellen Katalog der Rechte der Betroffenen im Landes- und im Bundesdatenschutzgesetz um ein gesondertes Recht auf eigene Darstellung zu ergänzen.

Dabei wäre klarzustellen, daß es sich um ein zusätzliches Recht handelt, das die bisherigen weiterbestehenden Rechte des Betroffenen nicht teilweise ersetzt. Zu verdeutlichen wäre außerdem, daß die Wahrnehmung dieses Rechts in der freien Entscheidung des Betroffenen liegt und daß für ihn keine Nachteile entstehen, wenn er davon absieht. Wer schweigt, bestätigt keineswegs die bestehende Darstellung; dies gilt schon jetzt, wenn man keine presserechtliche Gegendarstellung abgibt. Darüber hinaus gibt es bereichsspezifisch geregelte Schweigerechte z. B. in der Strafprozeßordnung.

Die speichernden Stellen, die zur Auskunft, Berichtigung, Sperrung und Löschung verpflichtet sind, könnten den Betroffenen infolgedessen nicht etwa darauf verweisen, daß er eine eigene Darstellung abgeben könne. Diese Entscheidung – auch über die durchaus vorhandenen Risiken einer Selbstdarstellung – muß allein dem Betroffenen überlassen bleiben. Er hat damit wie bei seinen jetzigen Rechten eine Wahlmöglichkeit, in welcher Weise er auf die Verwendung seiner persönlichen Daten einwirken will.

Schließlich gehört es zu den sachgerechten Auswirkungen einer derartigen Regelung, daß bei einer Übermittlung der Daten die eigene Darstellung gemeinsam mit diesen Daten zu übermitteln ist. Nur dann ist gewährleistet, daß bei einer Weitergabe der Daten bis hin zu einer erstmaligen oder erneuten Veröffentlichung auch die eigene Darstellung des Betroffenen wiedergegeben wird. Für die herkömmliche Gegendarstellung ist diese ergänzende Pflicht bereits in den neuen Rundfunkbestimmungen enthalten (siehe unten 4.3).

1.4 Hamburgisches Datenschutzgesetz

Der wesentliche Änderungsbedarf war im 10. TB (1.2.1) und im 11. TB (1.4) beschrieben worden. Der Senat hatte in seiner Stellungnahme zum 11. TB angekündigt, einen Gesetzentwurf im Jahr 1993 in die Bürgerschaft einzubringen. Mit einem Referentenentwurf der Justizbehörde ist nunmehr in Kürze zu rechnen. Dabei können auch die Erfahrungen aus weiteren Landesdatenschutzgesetzen berücksichtigt werden, die 1993 erlassen wurden (Bayerisches Datenschutzgesetz, Niedersächsisches Datenschutzgesetz und Saarländisches Datenschutzgesetz).

Die wichtige Frage des Anwendungsbereichs, die vor allem bei der Zuordnung von öffentlichen Unternehmen wiederholt zu Unklarheiten geführt hatte, wird voraussichtlich bei der Novellierung des Hamburgischen Datenschutzgesetzes normenklar geregelt werden. Diese Frage war inzwischen mit den Datenschutzbeauftragten des Bundes und der Länder sowie den Aufsichtsbehörden für den nicht-öffentlichen Bereich soweit wie möglich abgestimmt worden; sämtliche neueren Landesdatenschutzgesetze enthalten dazu konkrete Regelungen (siehe dazu auch 1.6).

Der vorgezogene Datenschutz bleibt ebenfalls regelungsbedürftig, insbesondere hinsichtlich der Risikoanalyse und Folgenabschätzung. Die erwähnten Landesdatenschutzgesetze aus dem Jahr 1993 haben dieses Thema jeweils aufgegriffen und fortentwickelt. Im Niedersächsischen Datenschutzgesetz heißt es z. B., daß vor der Entscheidung über den Einsatz oder die wesentliche Änderung von automatisierten Verfahren zu prüfen ist, ob und in welchem Umfang mit der Nutzung der automatisierten Datenverarbeitung Gefahren für die Rechte der Betroffenen verbunden sind. Weiter ist dort bestimmt, daß automatisierte Verfahren nur eingesetzt oder wesentlich geändert werden dürfen, soweit derartige Gefahren durch technische oder organisatorische Maßnahmen wirksam beherrscht werden können; das Ergebnis und seine Begründung sind aufzuzeichnen. Daran zeigt sich, daß dieser Bereich durchaus gesetzlich regelungsfähig ist.

Im technischen Bereich sind weitere Punkte aufgrund der ständigen Fortentwicklung der Automation zu regeln. Nachdem nun gemeinsame Dateien mit lesendem und schreibenden Zugriff für verschiedene Behörden eingeführt werden (siehe zum Vermessungswesen 12.1), sind die Voraussetzungen und Vorkehrungen bei solchen Dateien im Hamburgischen Datenschutzgesetz näher zu bestimmen.

Die Frage, welche Rechtsbestimmungen auf die Wartung und Fernwartung anzuwenden sind, ist zwischen den Landesdatenschutzbeauftragten und auch den Aufsichtsbehörden eingehend erörtert worden. Weder die Bestimmungen zur Übermittlung von Daten noch die Vorschriften zur Auftragsdatenverarbeitung passen in allen Fällen eindeutig auf Wartung und Fernwartung. Deshalb ist wegen des im Einzelfall nicht auszuschließenden Zugriffs durch Wartungsunternehmen auf personenbezogene Daten eine gesetzliche Regelung notwendig.

Zum Datenschutz für die Mitarbeiter im hamburgischen öffentlichen Dienst ist die Fortschreibung der Regelung im § 28 HmbDSG eingehend mit dem Senatsamt für den Verwaltungsdienst und der Justizbehörde abgestimmt worden. Hier besteht ohnehin Änderungsbedarf, weil das Personalaktenrecht in Bund und Ländern neu geregelt wird (7.2).

Der Vorschlag, Jugendlichen ab vollendetem 14. Lebensjahr die datenschutzrechtliche Handlungsfähigkeit einzuräumen, wird aufrecht erhalten. Die Gegenargumente des Senats in seiner Stellungnahme zum 11. TB überzeugen nicht.

Es kann bei den oft gegenläufigen Interessen von Behörden und Betroffenen nicht der zuständigen Behörde überlassen bleiben, jeweils die Einsichtsfähigkeit des Betroffenen zu beurteilen und damit zu entscheiden, ob ihm eigene Rechte zustehen. Entgegen der Auffassung des Senats ist aber vor allem zweifelhaft, ob die Rechtsgrundsätze, die bei der Einwilligung gelten, entsprechend auf die Verfahrensrechte wie Auskünfte usw. übertragbar sind. Die Justizbehörde ist von unserer Argumentation unterrichtet worden.

Inzwischen gibt es z. B. in Berlin eine bereichsspezifische Regelung durch Änderung des Schulgesetzes, wonach nunmehr Schüler vom vollendeten 14. Lebensjahr an grundsätzlich selbst die Rechte auf Auskunft und Akteneinsicht auch ohne Zustimmung der Erziehungsberechtigten geltend machen können (siehe dazu 9.1).

Klärungsbedürftig ist außerdem, ob im Hamburgischen Datenschutzgesetz ein Recht auf eigene Darstellung zusätzlich zu den bisherigen Rechten der Betroffenen generell eingeführt werden soll. Zu diesem Schwerpunktthema wird auf die obigen Ausführungen (1.3) und die Darstellung in den jeweiligen einzelnen Abschnitten des TB verwiesen.

Schließlich braucht es auch nicht auf Dauer selbstverständlich zu bleiben, daß das Hamburgische Datenschutzgesetz für die Ausübung des Gnadenrechts keine Anwendung findet. In den anderen Landesdatenschutzgesetzen ist dies zwar bisher oft ähnlich geregelt. Mit dem Entwurf eines saarländischen Gnadengesetzes zeichnet sich nun aber eine neue Entwicklung ab. Daher ist zu prüfen, ob ein Gnadengesetz auch in Hamburg erlassen werden soll und dann ergänzend für diesen Bereich das Hamburgische Datenschutzgesetz gelten soll (19.5).

1.5 Hamburgische Gesetze und Richtlinien

Im Anschluß an das Ersuchen der Bürgerschaft vom 8./9. April 1992 an den Senat, die überfälligen Gesetzentwürfe mit Regelungen zum Datenschutz im Schulwesen, Vermessungswesen, Meldewesen und beim Verfassungsschutz vorzulegen (11. TB, 1.5), sind diese Gesetzentwürfe inzwischen unterschiedlich vorangekommen. Das Hamburgische Gesetz über das Vermessungswesen ist sogar noch kurz vor der Auflösung der Bürgerschaft beschlossen worden (12.1).

1.5.1 Gesetzentwürfe

Der Entwurf des neuen Hamburgischen Verfassungsschutzgesetzes ist der Bürgerschaft zugeleitet worden und steht zur Beratung im Ausschuß an (18.1). Die Änderung und Ergänzung des Schulgesetzes soll mit Verbänden und Kammern abgestimmt werden (9.1).

Für die Neufassung des Hamburgischen Meldegesetzes liegt zwar ein 2. Referentenentwurf vor; es fehlt aber noch – auch wegen des ausstehenden Melderechtsrahmengesetzes des Bundes – die abschließende Behörden- und Senatsberatung. Ein qualitativ neuer Sachstand ist gegenüber dem 10. TB (13.1.1) nicht erreicht worden.

Der Gesetzentwurf über den öffentlichen Gesundheitsdienst, mit dem das Gesundheitswesen insbesondere in den Bezirksämtern eine zeitgemäße gesetzliche Grundlage erhalten soll, ist noch nicht abzusehen; ein Konzept soll allerdings bis Ende 1993 vorliegen. Der Entwurf zur Novellierung des Hamburgischen Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krank-

heiten durchlief Anfang 1993 die Behördenabstimmung; eine Senatsvorlage gibt es jedoch noch nicht.

Zum Arbeitnehmerdatenschutz ist ein Entwurf zur Änderung des Hamburgischen Beamtengesetzes mit uns abgestimmt worden; nach der Beschlußfassung des Senats ist der Entwurf der Bürgerschaft zugeleitet worden (7.2). Mit dem Arbeitnehmerdatenschutz wird sich auch die angekündigte Fortschreibung des Hamburgischen Personalvertretungsgesetzes – einschließlich des vom Personalrat selbst einzuhaltenden Datenschutzes – zu beschäftigen haben; ein Entwurf ist hierzu noch nicht erarbeitet worden (7.8). Ferner fehlt ein Sicherheitsüberprüfungsgesetz (18.4).

Im Umweltbereich werden in großem Umfang personenbezogene Daten zum Teil noch ohne gesetzliche Grundlage verarbeitet. Es fehlt insbesondere nach wie vor ein Hamburgisches Bodenschutzgesetz; ein weiteres Warten auf ein Bundesbodenschutzgesetz zur inhaltlichen Orientierung ist nicht mehr angebracht (5.1).

Demnach besteht durchaus weiterhin Handlungsbedarf in der Gesetzgebung zum Datenschutz. Bereits Anfang 1992 hatte ich betont, daß selbst bei großzügiger Verfahrensweise der sog. Übergangsbonus mit Ende der Legislaturperiode der Bürgerschaft abgelaufen sein wird. Durch die Auflösung der Bürgerschaft und die Wahl vom September 1993 muß dieser Zeitablauf verlängert werden. Jedenfalls mit Ende der jetzigen Legislaturperiode der Bürgerschaft voraussichtlich im Herbst 1997 und damit fast 14 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts müßten die gebotenen gesetzlichen Regelungen spätestens beschlossen sein.

Dabei soll nicht verkannt werden, daß schon bisher in einem erheblichen Umfang Datenschutzregelungen in Gesetzen und Verordnungen vorliegen. Nach unserer Übersicht gab es Ende 1993 insgesamt 25 hamburgische Gesetze mit Datenschutzvorschriften und eine große Zahl von Verordnungen.

1.5.2 Untersuchungsausschußgesetz

Für den Bereich der Bürgerschaft selbst ist eine umgehende gesetzliche Regelung des Datenschutzes bei Aktenvorlagen des Senats – insbesondere an Untersuchungsausschüsse – angebracht. In fast allen Bundesländern ist dies bereits geschehen.

Die jetzige knappe Regelung über Untersuchungsausschüsse in der Hamburgischen Verfassung mit einer Verweisung auf die Strafprozeßordnung hat bekanntlich immer wieder zu langwierigen Meinungsverschiedenheiten zwischen Senat und Bürgerschaft geführt. Dem Recht des Parlaments zur Aufklärung von Mißständen, aber auch dem Schutz der personenbezogenen Daten der Betroffenen ist dies abträglich. Die Vorlage der Mieterakten im Untersuchungsausschuß „Städtische Wohnungen" war bis zuletzt streitig geblieben. Die Bedeutung des Datenschutzes zeigt sich auch bei Aktenvorlagen außerhalb von Untersuchungsausschüssen wie bei der Vorlage der UKE-Patientenakten an den zuständigen bürgerschaftlichen Ausschuß.

Die Enquete-Kommission „Parlamentsreform" hat deshalb zurecht bereits im Oktober 1992 eine Ergänzung der Hamburgischen Verfassung und ein Untersuchungsausschußgesetz vorgeschlagen. Der bürgerschaftliche Verfassungsausschuß hat diesen Vorschlag in seinem Zwischenbericht vom Mai 1993 aufgegriffen und die Vorbereitung eines Gesetzentwurfs veranlaßt. Die Vorschläge der Enquete-Kommission „Parlamentsreform" berücksichtigen den Datenschutz aber noch nicht genügend.

Mit den Grundsätzen des Bundesverfassungsgerichts über Untersuchungsausschüsse ist es unvereinbar, wenn der Ausschuß als einzigen Schutz bei einer Aktenvorlage mit zahlreichen personenbezogenen Daten – auch über unbeteiligte Bürger – lediglich Vorkehrungen über die Geheimhaltung schutzbedürftiger Daten trifft. Dann würden die Ausschußmitglieder entgegen dem Verfassungsgrundsatz der Verhältnismäßigkeit vielfach persönliche Daten erfahren, deren Kenntnis zur Durchführung des Untersuchungsauftrags im öffentlichen Interesse gar nicht erforderlich ist.

Nach dem Vorbild einer ganzen Reihe von Landesgesetzen müßte eine datenschutzgerechte Regelung folgenden Inhalt haben:

1. Die Aktenvorlage darf nicht erfolgen, soweit und solange schutzwürdige Interessen einzelner und damit insbesondere der Datenschutz der Vorlage entgegenstehen. Zunächst ist daher festzustellen,
   - — ob die Unterlagen im Einzelfall wirklich erforderlich sind
   - — und inwieweit der Betroffene einer Behandlung in öffentlicher oder nichtöffentlicher Sitzung zustimmt.
2. Soweit keine wirksame Zustimmung vorliegt, ist eine Aktenvorlage nur zulässig, wenn
   - — der unantastbare Bereich privater Lebensgestaltung von der Untersuchung ausgenommen ist,
   - — für die vorzulegenden personenbezogenen Unterlagen die erforderlichen Vorkehrungen gegen das Bekanntwerden schutzwürdiger Daten getroffen sind, z.B. durch vertrauliche Beratung,
   - — oder die personenbezogenen Daten geschwärzt worden sind.
3. Hält der Untersuchungsausschuß an seinem Aktenvorlageersuchen fest, ist der Senat verpflichtet, den Vorsitzenden des Ausschusses und seinen Vertreter vertraulich die angeforderten Unterlagen einsehen zu lassen.
4. Hält der Untersuchungsausschuß danach die Voraussetzungen der Verweigerung nicht für gegeben, kann er beschließen, das Hamburgische Verfassungsgericht anzurufen. Das Hamburgische Verfassungsgericht entscheidet darüber, ob die Verweigerung begründet ist.

Diese Regelungen könnten auch in Art. 32 der Hamburgischen Verfassung als Vorschrift über die Aktenvorlage an die Bürgerschaft und deren Ausschüsse aufgenommen werden. Für die Vorschläge der Enquete-Kommission zu dieser Vorschrift gelten die obigen Ausführungen entsprechend.

1.5.3 Öffentliche bürgerschaftliche Ausschußsitzungen

Im Vorgriff auf einen neuen Art. 24a Abs. 2 der Hamburgischen Verfassung nach den Vorschlägen der Enquete-Kommission „Verfassungsreform" hat die Bürgerschaft am 6. Oktober 1993 beschlossen, daß die Ausschußberatungen gemäß der Neufassung von § 64 Abs. 4 der Geschäftsordnung künftig grundsätzlich öffentlich sind. Ausgenommen ist dort allerdings insbesondere die Behandlung von Eingaben, so daß die dafür geltenden datenschutzrechtlichen Regelungen weiterhin anzuwenden sind.

Für die sonstige regelmäßige Ausschußarbeit ist die weitere Bestimmung in § 64 Abs. 4 der Geschäftsordnung von besonderer Bedeutung, wonach die Öffentlichkeit auszuschließen ist, „wenn überwiegende Belange des öffentlichen Wohls oder schutzwürdige Belange einzelner dies erfordern". Darüber „wird in nicht-öffentlicher Sitzung entschieden". Die Beachtung der „schutzwürdigen Belange einzelner" betrifft den Schutz personenbezogener Daten.

Im Rahmen meiner datenschutzrechtlichen Beratung der Bürgerschaft habe ich darauf hingewiesen, daß möglichst von Anfang an in geeigneter Weise eine Beeinträchtigung Betroffener hinsichtlich ihrer personenbezogenen Daten vermieden werden sollte. Dazu können die obigen Grundsätze für ein Untersuchungsausschußgesetz herangezogen werden. Deshalb empfiehlt es sich, vor der Behandlung personenbezogener Daten in öffentlicher Ausschußsitzung folgende Fragen zu beantworten:

1. Ist die personenbezogene Behandlung anstelle anonymisierter Angaben im Einzelfall erforderlich?
2. Liegt eine Einwilligung des Betroffenen vor?
3. Ist ohne Einwilligung der unantastbare Bereich privater Lebensgestaltung ausgenommen und gibt es keine entgegenstehenden Vorschriften?
4. Überwiegt das Interesse an einer öffentlichen Beratung gegenüber schutzwürdigen Interessen des Betroffenen?

Wenn es nach diesen Kriterien zu einer nichtöffentlichen Beratung kommt, ist nach wie vor der unantastbare Bereich privater Lebensgestaltung von der Beratung auszunehmen, falls keine Einwilligung des Betroffenen vorliegt. In der Niederschrift dürfen die übrigen personenbezogenen Daten nicht so wiedergegeben werden, daß auf bestimmte Personen geschlossen werden kann.

1.5.4 Richtlinien

Bei den Datenschutzverbesserungen in Hamburg sind die Richtlinien zu erwähnen, die vom Senatsamt für den Verwaltungsdienst in Abstimmung mit uns erarbeitet worden sind.

Die intensiv erörterte Telekommunikations-Richtlinie mit wichtigen Vorschriften über den Datenschutz bei der Nutzung von Telefon, Telefax usw. ist am 1. April 1993 in Kraft getreten (MittVw 1993 Seite 219). Zur Zeit werden die Durchführungsbestimmungen mit unserer Beteiligung vorbereitet. Die Paßwort-Richtlinie gilt bereits seit 1. Februar 1993 (MittVw 1993 Seite 83). Die Durchführungsbestimmungen für die Verarbeitung personenbezogener Daten zur Bearbeitung von Eingaben sowie Kleinen und Großen Anfragen sind am 1. Juli 1993 in Kraft getreten (MittVw 1993 Seite 288).

Wegen der datenschutzrechtlich relevanten Punkte wird insoweit auf die jeweilige frühere Darstellung verwiesen (10. TB 4.3; 11. TB, 3.8; 11. TB, 1.9.5).

1.6 Bundesdatenschutzgesetz

Zum Anwendungsbereich des Bundesdatenschutzgesetzes ist die Erörterung der Abgrenzung zwischen öffentlichen und nicht-öffentlichen Stellen (vgl. 11. TB., 1.4.1) im Berichtszeitraum intensiv fortgeführt worden. Zwischen den Datenschutzbeauftragten des Bundes und der Länder und den Aufsichtsbehörden wurde Einigkeit darüber erzielt, daß die Zuordnung von privatrechtlichen Vereinigungen zum öffentlichen Bereich der Länder den Landesdatenschutzgesetzen vorbehalten ist, soweit nicht der Bund im Rahmen seiner Gesetzgebungskompetenz für den nicht-öffentlichen Bereich eine Stelle als nicht-öffentlich eingestuft hat.

Unterschiedlich beurteilt wird dabei nach wie vor, welche Kriterien für die entsprechende Zuordnung erforderlich sind (Wahrnehmung einer Aufgabe der öffentlichen Verwaltung und/oder absolute Mehrheit der Anteile oder Stimmen bzw. anderweitige Beherrschung).

Für Hamburg wird insofern die Änderung des § 2 HmbDSG maßgeblich sein. Darüber hinaus ist nach einer Verabschiedung der EG-Richtlinie zum Datenschutz die Rechtsentwicklung im Rahmen der dann folgenden Anpassungen des Bundesdatenschutzgesetzes und der Landesdatenschutzgesetze weiter zu verfolgen.

Zweieinhalb Jahre nach dem Inkrafttreten des neuen Bundesdatenschutzgesetzes hat sich inzwischen der Schwerpunkt von den rechtlichen Zweifelsfragen (11. TB, 1.6) auf die praktische Anwendung verlagert. Unsere notleidende Kontrolltätigkeit als Aufsichtsbehörde ist aufgrund der Stellenverbesserung (11. TB,. 1.6.2) erheblich intensiviert worden.

Anhand eines selbst entwickelten Prüfkonzeptes für die Unternehmen, die nach dem Bundesdatenschutzgesetz einer ständigen Aufsicht unterliegen, ist

bereits im Jahre 1993 eine ganze Reihe von Unternehmen geprüft worden (siehe 29.). Das Prüfkonzept soll dazu beitragen, daß in einem überschaubaren Zeitraum die zum Register gemeldeten Unternehmen, die einer ständigen Aufsicht nach § 38 Abs. 2 BDSG unterliegen, auch tatsächlich geprüft werden. Unterstützt wird dieses Vorhaben dadurch, daß uns seit einiger Zeit ständig ein Trainee aus dem Bereich der Informations- und Kommunikationstechnik des Senatsamts für den Verwaltungsdienst zur Verfügung gestellt wird.

1.7 Entwicklung der EG-Datenschutzrichtlinie

Im Rahmen der Beratungen in der Gruppe „Wirtschaftsfragen" des Ministerrates konnte die erste Lesung des überarbeiteten EG-Richtlinienentwurfs abgeschlossen werden. Die zweite Lesung begann im Juli 1993 und soll zur Erarbeitung eines gemeinsamen Standpunkts der Mitgliedstaaten gemäß Art. 189 c EG-Vertrag führen.

Bei der zweiten Lesung sind noch eine Reihe wichtiger Fragen zu erörtern. Neben dem generellen Anwendungsbereich der Richtlinie ist dies u.a. die Frage nach der Festschreibung der Möglichkeit, im nationalen Recht über den Standard der Richtlinie hinauszugehen. Auch Umfang, Inhalt und Tragweite der Meldepflicht bedürfen der weiteren Erörterung, um ein erhöhtes Maß an bürokratischem Aufwand ohne gleichzeitige Verstärkung des Schutzes des einzelnen zu vermeiden.

Von deutscher Seite wird zudem darauf hingearbeitet, daß das System der Selbstkontrolle der Unternehmen durch einen betrieblichen Datenschutzbeauftragten in die Richtlinie aufgenommen oder zumindest vom Entwurf nicht beeinträchtigt wird. Dieses System hat sich in der Praxis bewährt. Die Kommission hat die Prüfung einer entsprechenden Klarstellung zugesagt.

Die Beratungen werden im 2. Halbjahr 1994 unter deutschem Vorsitz mit dem Ziel fortgeführt werden, die zweite Lesung in dieser Zeit abzuschließen. Der gemeinsame Standpunkt wird dann zur erneuten Beratung dem Europäischen Parlament vorgelegt werden. Eine Verabschiedung der Richtlinie dürfte kaum vor 1995 erfolgen.

Um die Interessen der Betroffenen auch vor Erlaß der EG-Datenschutzrichtlinie und deren Umsetzung in innerstaatliches Recht zu schützen, haben die Aufsichtsbehörden eine Checkliste zur Verbesserung des Datenschutzes beim grenzüberschreitenden Verkehr mit personenbezogenen Daten im nicht-öffentlichen Bereich erarbeitet. Die Checkliste soll von der Wirtschaft zur Beurteilung der Zulässigkeit von Vereinbarungen zwischen inländischen und ausländischen Datenempfängern herangezogen werden. Sie enthält u.a. Maßnahmen zur Sicherung des Auskunftsrechts, der Rechte auf Berichtigung, Sperrung und Löschung sowie Maßnahmen zur Datensicherheit und zur Haftung der Datenverarbeiter.

1.8 Verhältnis zum Bürger

Das Interesse der Bürger an Datenschutzfragen ist unverändert groß. Täglich wenden sich Bürger mit Anfragen zum Datenschutz an uns. Da wir keine festen Sprechzeiten haben, kann der Bürger jederzeit seine Fragen an uns richten.

1.8.1 Eingaben

Die Zahl der schriftlichen Eingaben, die als einzige zahlenmäßig festgehalten werden, ist weiterhin hoch. Bis Ende November 1993 gingen 339 schriftliche Eingaben zu folgenden Themen ein:

Öffentlicher Bereich	181
davon Polizei und Verfassungsschutz, Meldewesen und Verkehr	90
Gesundheits- und Sozialbereich	58
sonstige	33
Nicht-öffentlicher Bereich	158
davon Versandhandel	3
Versicherungswirtschaft	15
Kreditwirtschaft	8
Werbung	18
Arbeitnehmer-Datenschutz	11
Schufa und Auskunfteien	35
Gesundheitswesen	15
Markt- und Meinungsforschung	6
Wohnungswirtschaft	7
Verkehrswesen	6
sonstige	34

Zusätzlich werden weiterhin im zweimonatigen Abstand Bürgersprechstunden zu Datenschutzfragen ohne Themenvorgabe durchgeführt. Die Termine werden vorher über die Medien bekanntgegeben. Die Bürgersprechstunden sind daraufhin erneut insbesondere von Bürgern genutzt worden, denen es nicht um Eingaben zu akuten Fragen, sondern mehr um allgemeine Themen des Datenschutzes geht.

1.8.2 Öffentlichkeitsarbeit

Für den Kontakt zu den Bürgern ist die Veröffentlichung aktueller Datenschutzthemen besonders wichtig. Die bereits bisher intensive Öffentlichkeitsarbeit ist im Jahr 1993 noch erheblich verstärkt worden.

In der öffentlichen Vortragsreihe über Datenschutzfragen hat die Veranstaltung mit Bundesverfassungsrichter Prof. Grimm über „Verfassungsrechtliche Perspektiven des Datenschutzes" am 29. April 1993 große Resonanz gefunden. Prof. Grimm, der beim Bundesverfassungsgericht der Berichterstatter für Datenschutzverfahren ist, hat mit seinen Thesen die Fortentwicklung des

Datenschutzes beschrieben. Schwerpunkt seiner Konzeption ist dabei, daß die Beschränkung auf die bisherige Abwehrfunktion des Rechts auf informationelle Selbstbestimmung dessen Schutzgehalt nicht ausschöpft und der Ergänzung um eine Anspruchsdimension bedarf; deshalb sind Auskunfts- und Gestaltungsrechte zur Gewährleistung des Datenschutzes auszubauen (siehe 1.3).

Auf dem Symposium über das „Grundrecht auf Datenschutz im Grundgesetz" am 11. Oktober 1993 wurden die Argumente für und gegen eine Verfassungsergänzung eingehend öffentlich behandelt. Insoweit kann auf die obigen Ausführungen zum Grundrecht auf Datenschutz verwiesen werden (1.1).

Die vierteljährlichen Pressekonferenzen in der Dienststelle mit Vertretern der hamburgischen Zeitungen und des Rundfunks führten wiederum zu entsprechender Berichterstattung in den Medien. Dabei wurden so unterschiedliche Themen wie Datenschutz in der Arztpraxis, Reality TV und Persönlichkeitsrechte, bargeldloser Fahrkartenverkauf des HVV und Datenschutzfragen bei Wahlen behandelt.

In der Reihe der „Hamburger Datenschutzhefte" wurde nach der Schrift über das „Datenschutzkonzept für PC" als weiteres Heft im April 1993 das „Datenschutzkonzept für UNIX-Mehrplatzanlagen" veröffentlicht. Das Interesse auch an dieser Broschüre war über Hamburg hinaus wieder sehr groß. Die Reihe soll im Jahr 1994 mit einer Broschüre über Datenschutzprobleme bei Netzen fortgesetzt werden.

Für den öffentlichen Bereich wurde dieses wichtige Thema zum Teil bereits mit unserem „Bericht über den Datenschutz bei Automation und Vernetzung der hamburgischen Verwaltung – IuK-Datenschutzbericht –" vom Juli 1993 aufgearbeitet (siehe 3.1). Diese Ergänzung zum 11. TB wurde in der Reihe „Berichte und Dokumente" der Staatlichen Pressestelle veröffentlicht.

Zur allgemeinen Information über das Bundesdatenschutzgesetz ist außerdem ein Faltblatt über den „Datenschutz im privaten Bereich" mit einer Auflage von 10.000 Exemplaren herausgegeben worden, das mit den Aufsichtsbehörden der Länder und dem Bundesbeauftragten für den Datenschutz abgestimmt wurde. Es wird auch über die Verbraucherzentrale und die hamburgischen öffentlichen Bücherhallen verteilt.

Wegen der immer wieder gestellten Fragen zum Datenschutz bei der Werbung haben die Aufsichtsbehörden in Niedersachsen, Bremen und Hamburg Informationen mit „Tips zum Adressenhandel und gegen die Werbepapierflut im Briefkasten" gemeinsam herausgegeben. In Vorbereitung befindet sich ferner ein Leitfaden „Datenschutz in der Arztpraxis".

Schließlich ist nach Abstimmung zwischen den Aufsichtsbehörden eine Checkliste zur Verbesserung des Datenschutzes beim grenzüberschreitenden Verkehr mit personenbezogenen Daten im nicht-öffentlichen Bereich herausgegeben worden. Bis zum Erlaß und der Umsetzung der EG-Richtlinie zum Datenschutz gibt es damit für die Wirtschaft eine Orientierung hinsichtlich der Zulässigkeit oder Unzulässigkeit der Datenübermittlung ins Ausland (1.7).

1.9 Zusammenarbeit mit Verwaltung und Justiz

Der Kontakt mit Behörden und Kammern und auch mit der Justiz ist weiterhin insgesamt positiv. Gelegentlich schleppend ist die Zusammenarbeit mit der Behörde für Arbeit, Gesundheit und Soziales. In dieser großen Behörde steht für Datenschutzfragen lediglich eine halbe Stelle zur Verfügung, auf der zugleich noch andere Aufgaben wahrgenommen werden. In der größenmäßig vergleichbaren Behörde für Schule, Jugend und Berufsbildung stehen dafür immerhin 2 Stellen zur Verfügung. Ebenfalls mühsam war zuweilen die Kooperation mit der Geschäftsführung des Landesbetriebs Krankenhäuser (21.2).

Für die Zusammenarbeit mit der Verwaltung ist die Richtlinie zur Beteiligung des Hamburgischen Datenschutzbeauftragten von praktischer Bedeutung (11. TB, 1.9.3). Mit den weiteren Richtlinien, die bereits erwähnt wurden (1.5.4), sind eine Reihe von klärungsbedürftigen Punkten für die gesamte Verwaltung behandelt worden. Dazu gehören insbesondere die Durchführungsbestimmungen für die Beantwortung bürgerschaftlicher Anfragen.

Bei den großen Automationsprojekten wie dem Projekt Sozialhilfe-Automation (PROSA) und dem Projekt Personalwesen (PROPERS) wurde die positive Zusammenarbeit fortgesetzt. Der Datenschutz befindet sich dort nunmehr in der Bewährung, weil bei beiden Projekten die Umsetzung in die Praxis begonnen hat, bei PROSA in einer zunehmenden Zahl von Sozialhilfe-Dienststellen (6.1), bei PROPERS mit der Pilotierung in der Behörde für Schule, Jugend und Berufsbildung (7.1).

Schwerwiegende Auseinandersetzungen mit der Notwendigkeit, eine förmliche Beanstandung auszusprechen, konnten wieder vermieden werden. In mehreren Fällen mußten wir zwar eine Beanstandung ankündigen, wenn nicht unverzüglich für Abhilfe gesorgt würde. In diesen Fällen wurden dann jedoch Datenschutzmaßnahmen angekündigt, die eine Zurückstellung der Beanstandung rechtfertigten. Auf die zeitgerechte Umsetzung dieser Ankündigungen werden wir besonders achten; falls die Umsetzung ausbleibt oder nicht ausreichend ist, wird noch eine Beanstandung erfolgen.

Die zögerliche Klärung der Datenschutzkontrolle bei den Gerichten wurde erfreulicherweise mit der Stellungnahme des Senats vom 30. März 1993 zum Ersuchen der Bürgerschaft abgeschlossen. An der Erarbeitung der Senatsmitteilung wurden wir frühzeitig beteiligt. Meine Zuständigkeit hinsichtlich der Datenschutzkontrolle bei den Gerichten bezüglich der Verwaltungsangelegenheiten wurde durch eine detaillierte Auflistung der Angelegenheiten, die darunter fallen und die nicht darunter fallen, soweit wie möglich auch in Abstimmung mit den Gerichten geklärt.

2. Entwicklung der Dienststelle

Die personelle Ausstattung der Dienststelle hat sich weiter verbessert. Das Referat mit der Aufsicht im nicht-öffentlichen Bereich verfügt nun durch die Hebung der Stelle der Referatsleiterinnen sowie die Besetzung einer neuen Referentenstelle über dieselbe Struktur wie die anderen Referate.

Im übrigen hat es im Berichtsjahr vergleichsweise nur geringe Bewegung im Personalbestand gegeben. Die Stelle des Geschäftsstellenleiters wurde wegen der Umsetzung des bisherigen Stelleninhabers innerhalb der Dienststelle nachbesetzt.

Das jahrelange Problem, die Position des Stellvertreters des Hamburgischen Datenschutzbeauftragten angemessen zu bewerten (11. TB, 2.), konnte endlich positiv gelöst werden. Für den Stellenplan 1994 wurde vom Senat eine Hebung der Stelle zum Leitenden Regierungsdirektor vorgesehen. Diese Lösung wurde durch das Verständnis des Senatsamtes für den Verwaltungsdienst für dieses Problem und durch die Mitfinanzierung seitens der Justizbehörde ermöglicht.

Als Anhang ist wiederum der aktuelle Geschäftsverteilungsplan abgedruckt. Der Anteil der Teilzeitbeschäftigten mit einem Drittel der Mitarbeiter ist unverändert hoch. Auch der Frauenanteil mit ca. 40% der Gesamtzahl der Mitarbeiter ist gleich geblieben.

3. Informations- und Kommunikationstechnik

3.1 Diskussion des IuK-Datenschutzberichts

Bereits in den letzten Tätigkeitsberichten haben wir uns intensiv mit den Gefahren auseinandergesetzt, die mit dem zunehmenden Einsatz von Informations- und Kommunikationstechnik verbunden sind (vgl. 10. und 11. TB, jeweils 3.1).

Im Juli 1993 haben wir einen gesonderten Bericht über den Datenschutz bei Automation und Vernetzung der hamburgischen Verwaltung vorgelegt. In diesem IuK-Datenschutzbericht werden auf der Grundlage einer Darstellung des technischen und organisatorischen Rahmens des Einsatzes von IuK-Technik in der hamburgischen Verwaltung und einer Analyse der mit dem Technikeinsatz verbundenen Risiken Lösungsmöglichkeiten für diese Probleme aufgezeigt. Der Bericht setzt sich kritisch mit der Zielsetzung auseinander, Computer unabhängig von bestimmten Aufgaben zu vernetzen und so die technische Grundlage für einen unbegrenzten Datenaustausch zu schaffen (Infrastrukturansatz).

Neben dem eigentlichen Datenschutzaspekt setzt sich der Bericht auch mit der Frage auseinander, wie sich unter veränderten technischen Bedingungen die parlamentarische Kontrolle der Verwaltung realisieren läßt. Es werden Vorschläge diskutiert, wie die rechtlichen und technischen Kontrollmöglichkeiten der Bürgerschaft gestärkt werden können.

Der Bericht kommt zu dem Ergebnis, daß den Risiken bereits in der Planungsphase begegnet werden muß. Behördenübergreifende Netze dürfen nur eingerichtet werden, wenn sie für die Erfüllung konkreter Aufgaben erforderlich sind und eine klare gesetzliche Grundlage besteht.

3.2 Grundschutzkonzept als Voraussetzung für Automationsverfahren

3.2.1 Gesetzliche Anforderungen an die Datensicherheit

Unbeschadet aller Innovationen in der Informations- und Kommunikationstechnik sind die Vorschriften über „technische und organisatorische Maßnahmen zur Sicherstellung des Datenschutzes" aus dem ersten Bundesdatenschutzgesetz vom 27. Januar 1977 praktisch unverändert in die neueren Datenschutzgesetze (so in § 9 BDSG vom 20. Dezember 1990 und in § 8 HmbDSG vom 5. Juli 1990) übernommen worden.

Diese Datensicherungsvorschriften gehen von der Grundidee aus, daß sich die Maßnahmen, die von den datenverarbeitenden Stellen zu treffen sind, an den konkreten Gefährdungen für die jeweils zu schützenden personenbezogenen Daten zu orientieren haben. Daraus ist abzuleiten, daß die Anforderungen an die Datensicherheit mit der Sensibilität der verarbeiteten Daten korrespondieren, die Schutzmechanismen also umso stärker sein müssen, je größer die Schutzwürdigkeit der Daten ist.

Eine derartige Betrachtungsweise setzt voraus, daß es objektive, nachprüfbare Kriterien für die Datensensibilität gibt. Derartige klare Kriterien sind aber weder im BDSG noch in den anderen Datenschutzgesetzen zu finden. Das BDSG enthält lediglich einige nicht auf die Datensicherheit bezogene Sondervorschriften über solche Daten, die einem „besonderen Berufs- oder Amtsgeheimnis" unterliegen (§ 24 Abs.2, § 39 BDSG), ebenso das HmbDSG (§ 13 Abs.2 Satz 2, § 16 Abs. 1 Satz 1 Nr. 2 HmbDSG).

Ebensowenig definieren die gesetzlichen Vorschriften bestimmte Datengruppen als „unsensibel". Entsprechende Auslegungen der Übermittlungsregelungen in § 28 Abs. 2 Nr.1b BDSG hinsichtlich Beruf, Name, Anschrift und Geburtsjahr gehen an der Sache vorbei, da auch dort das schutzwürdige Interesse des Betroffenen überwiegen kann. An dieser Stelle sind immerhin – wenn auch unvollständig – regelmäßig sensible Daten über gesundheitliche Verhältnisse, strafbare Handlungen und Ordnungswidrigkeiten usw. besonders erwähnt. Die gesetzliche Formulierung „im allgemeinen" weist aber darauf hin, daß auch diese Daten im Einzelfall weniger schutzwürdig sein können. Zu erwähnen ist in diesem Zusammenhang die Pflicht zur Löschung derartig sensibler Daten, wenn die speichernde Stelle ihre Richtigkeit nicht beweisen kann (§ 35 Abs. 2 Satz 2 Nr. 2 BDSG).

Das Bundesverfassungsgericht hat 1983 im Volkszählungsurteil festgestellt, daß durch die Verknüpfungsmöglichkeiten automatisierter Datenverarbeitung

an und für sich belanglose Daten einen neuen Stellenwert bekommen können und es deshalb insoweit kein „belangloses" Datum mehr gibt (BVerfGE 65,1, S. 45).

Der Gesetzgeber hat daraus jedoch nicht die Schlußfolgerung gezogen, für alle personenbezogenen Daten denselben Schutz zu fordern, sondern er hat daran festgehalten, die geforderten Sicherheitsmaßnahmen an der Schutzwürdigkeit zu orientieren, wobei jeweils auch Aufwands-und Wirtschaftlichkeitsgesichtspunkte zu berücksichtigen sind. So heißt es in § 8 Abs.1 Satz 2 HmbDSG: „Erforderlich sind Maßnahmen zur Datensicherung nur, wenn ihr Aufwand in einem angemessenen Verhältnis zur Schutzwürdigkeit der Daten steht." Eine ähnliche Regelung enthält § 9 Abs. 2 BDSG.

In der Praxis ist daraus die Konsequenz gezogen worden, für jedes DV-Vorhaben eine Risikoanalyse zu fordern, die den spezifischen Gefährdungen der Verarbeitung bestimmter Daten Rechnung trägt. Das Ziel ist ein maßgefertigtes Sicherheitskonzept für das jeweilige Verfahren.

Maßgeschneiderte, auf einzelne Anwendungen bezogene Sicherheitskonzepte werden dann problematisch, wenn Daten unterschiedlicher Schutzwürdigkeit mit derselben Technik von verschiedenen Benutzern verarbeitet werden, wie dies nicht nur bei Großrechnern, sondern auch in Rechnernetzen üblich ist. Hier stellen sich viele praktische Fragen:

— Wie werden die Verfahren funktional voneinander abgeschottet, und zwar sowohl gegenüber den Anwendern als auch gegenüber den Systemverantwortlichen?

— Wie wird gewährleistet, daß durch zusätzliche Verfahren nicht die Sicherheit bestehender Verfahren gefährdet wird?

— Wie kann sichergestellt werden, daß Systemverwalter und andere Personen, die anwendungsübergreifend für die Funktionsfähigkeit der Technik verantwortlich sind, keinen unberechtigten Zugriff auf die Daten selbst erhalten?

3.2.2 Grundsicherung, Schwachstellen- und Risikoanalyse

Bei der Risikoanalyse wird üblicherweise in drei Schritten vorgegangen:

1. Erfassung der Schutzobjekte,
2. Erfassung und Bewertung der Bedrohungen,
3. Bestimmung der zur Risikobewältigung erforderlichen Maßnahmen (ggf. unter bewußter Inkaufnahme eines nicht abgedeckten Restrisikos).

Eine derartige system- und anwendungsspezifische Risikoanalyse bezüglich bestimmter personenbezogener Daten ist das Verfahren, das den Anforderungen des Datenschutzrechts am ehesten entspricht. Typisierende Verfahren (z.B. Schutzstufenkonzepte – vgl. 9.TB, 3.2.3 und unsere Datenschutzkonzepte für PC und für UNIX-Mehrplatzanlagen) orientieren sich an diesem Ansatz, indem sie entsprechend einer Klassifikation der Daten nach Schutzwürdigkeit für bestimmte Techniken jeweils Sicherungsmaßnahmen vorgeben.

Die Grenzen derartiger Ansätze sind jedoch bei multifunktionalen und vernetzten Systeme erreicht, die nicht ausschließlich für ein Verfahren, sondern als Infrastrukturmaßnahmen geplant und installiert werden. Wenn nicht vorab bekannt ist, welche Daten auf einem System verarbeitet werden sollen, kann eine an der Datensensibilität orientierte Sicherheitskonzeption keine Lösungen bringen.

Bei Großrechnern und anderen vernetzten Systemen ist es durchaus sinnvoll, von vornherein in einzelnen Punkten stärkere Sicherheitsvorkehrungen vorzusehen, als dies bei einer kurzfristig angelegten fallweisen Betrachtungsweise zunächst geraten scheint. Gefragt ist also die Entwicklung von Grundschutzkonzepten, die die mit typischen Anwendungen in typischen Einsatzgebieten verbundenen Risiken abdecken.

Den Kern eines Grundschutzkonzeptes bilden abstrakte Anforderungen an die Systemsicherheit. Sie sind unabhängig von der eingesetzten Hard- und Software, dem organisatorischen Umfeld, dem betroffenen Personenkreis, der Komplexität der Verfahren und der Sensibilität der Daten zunächst als Mindestanforderungen an die Datensicherheit festzulegen.

Die Anforderungen müssen so gestaltet sein, daß man auf ihnen aufbauend bei Bedarf zusätzliche Maßnahmen treffen und implementieren kann. Insbesondere dann, wenn sich bei bereits vorhandenen DV-Verfahren mit den Grundschutzanforderungen die Schutzwürdigkeit nachträglich erhöht, stellt sich ansonsten bei den nunmehr zusätzlich erforderlichen Datensicherungsmaßnahmen die Frage, inwieweit diese nachträglich überhaupt noch umsetzbar sind.

Zu fordern ist ferner, daß die datensicherheitsmäßigen Grenzen des Grundschutzes bei bestimmten technischen Lösungen (z.B. von UNIX-Anlagen) verdeutlicht werden. Diese Grenzen würden überschritten, wenn so sensible Daten verarbeitet werden sollen, daß für sie der Grundschutz allein nicht mehr ausreicht. Damit die Anwender diese Grenzen erkennen können, ist offenzulegen, für welche Art von Daten der Grundschutz gelten soll, also auch, bis zu welcher Schutzstufe personenbezogene Daten ohne zusätzliche Sicherheitsmaßnahmen verarbeitet werden dürfen.

Grundschutzkonzepte sind insbesondere in Bereichen relevant, in denen nicht vorab feststeht, welche personenbezogenen Daten verarbeitet werden sollen. Daher ist bei der Konzeption davon auszugehen, daß auch sensible personenbezogene Daten verarbeitet werden. Der Grundschutz muß also gerade bei Infrastrukturprojekten – z.B. bei einer vorsorglichen Gebäudeverkabelung – sehr hoch angelegt werden. Selbst wenn anfangs keine sensiblen Daten verarbeitet werden sollen, muß das System auch für künftige Anwendungen offen sein, die höhere Sicherheitsanforderungen benötigen (vgl. 3.3).

Die Ergebnisse eines Grundschutzkonzepts bilden die Basis für Schwachstellenanalysen. Im Unterschied zur Risikoanalyse wird dabei nicht von Schutzobjekten (bei rein datenschutzrechtlicher Betrachtung also von den personenbezogenen Daten) ausgegangen, sondern es sind vorab festgelegte Sicherheitsfunktionen abzuprüfen (z.B. Einhaltung von Paßwortkonventionen). Wenn sich ergibt, daß bestimmte Anforderungen nicht erfüllt werden können und somit die erforderliche Grundsicherheit nicht erreicht wird, dann sollte das entsprechende System nicht eingesetzt werden.

Ein wesentlicher Vorteil des Tandems Grundsicherung-Schwachstellenanalyse liegt darin, daß prinzipiell mit konfektionierten Sicherheitslösungen gearbeitet werden kann und damit Kosteneinsparungen realisiert werden. Für Verfahren mit weniger sensiblen Daten kann ein derartiger Ansatz jedoch dazu führen, daß Sicherheitsmaßnahmen stärker dimensioniert werden, als dies bei einzelfallbezogener Betrachtung angemessen erscheinen würde.

Auch bei einer Grundsicherungskonzeption kann nicht gänzlich auf Risikoanalysen verzichtet werden. Bei Daten, die eines stärkeren als des standardmäßigen Schutzes bedürfen, sind über den Grundschutz hinausgehende technische und organisatorische Sicherheitsmaßnahmen erforderlich. So wäre es z.B. denkbar, besonders sensible Daten generell nur kryptographisch verschlüsselt zu übertragen oder für logische Subnetze, auf denen solche Daten übertragen werden, zusätzliche andere Maßnahmen zu ergreifen (vgl. 3.3 und 21.7).

3.2.3 Arbeitsgruppe Datensicherheitskonzept

Seit dem Frühjahr 1993 arbeitet unter Federführung des Senatsamtes für den Verwaltungsdienst eine überbehördliche Arbeitsgruppe an der Erstellung eines generellen Datensicherheitskonzeptes. Die Arbeitsgruppe entwickelt ein detailliertes Raster zur Erkennung und Bewertung von Risiken in Form einer Schwachstellenanalyse, das auf einem Grundschutzkonzept beruhen wird.

Wir gehen davon aus, daß dieser Ansatz weiterverfolgt wird und kurzfristig zu Vorgaben führt, die für die Sicherheit der IuK-Technik in den verschiedenen Behörden verbindlich sind.

3.3 Datensicherheits-Mindeststandards bei Netzen

Nachdem in den letzten Jahren in fast sämtlichen Bereichen der hamburgischen Verwaltung zahlreiche UNIX-Rechner und Personalcomputer installiert worden sind, wird nun verstärkt deren Vernetzung in Angriff genommen. Die Vernetzung heterogener Rechnersysteme schafft nicht nur die Infrastruktur zu einem übergreifenden Rechner- und Datenverbund, sondern führt auch zu komplexen Datenschutz- und Datensicherungsrisiken. Die Diskussion um Datensicherheit kann sich daher – anders als bei Einzelplatzsystemen und UNIX-Mehrplatzanlagen – nicht mehr nur auf die Sicherheitsdefizite eines

konkreten und abgeschlossenen Systems beschränken, sondern muß bereits frühzeitig Risiken miteinbeziehen, die sich durch Daten- und Funktionsintegration zusätzlich ergeben können (vgl. 11.TB, 3.1.2).

Unabhängig von der konkreten Anwendung sollte daher bei denjenigen Netzkomponenten ein angemessener Mindest-Sicherheitsstandard gewährleistet werden, die nur sehr kostenintensiv verändert werden können oder gänzlich irreversibel sind: Netztopologie und Übertragungsmedien.

3.3.1 Filternde Sternkoppler

Sofern Daten unverschlüsselt über das Netz übertragen werden, besteht grundsätzlich die Gefahr, daß Unbefugte das Übertragungsmedium abhören und damit Kenntnis über personenbezogene Daten erhalten. Das Abhörrisiko wird verstärkt, wenn die Informationen nicht nur zum rechtmäßigen Empfänger, sondern an sämtliche Netzteilnehmer zugleich geschickt werden. Da sich jeder Netzrechner aus der Gesamtmenge der im Netz übertragenen Daten die für ihn relevanten Nachrichten heraussucht, entscheidet bei solchen broadcastorientierten Verfahren nicht mehr der Absender über den Kreis der zur Kenntnisnahme Berechtigten, sondern jeder potentielle Empfänger selbst.

Um das Abhörrisiko auf die Verbindung zwischen Sender und Empfänger zu reduzieren, sollte daher auf broadcastorientierte Systeme verzichtet werden. Dies schließt Bus- oder Ringtopologien aus, da die Daten hierbei über den gesamten Ring bzw. Bus geleitet werden. Beim Ring dienen die einzelnen Rechner sogar als aktive Netzkomponenten. Dagegen besteht bei Sternstrukturen die Möglichkeit, die Daten exklusiv zwischen dem zentralen Netzknoten und dem jeweiligen dezentralen Rechner zu übertragen.

Der zusätzliche Vorteil einer Sternstruktur besteht darin, daß der Zentralrechner die Interaktion der Rechner untereinander kontrollieren und unzulässige Übermittlungen verhindern kann. Sternstrukturen sind darüber hinaus ausfallsicherer als Bus- oder Ringstrukturen. Vom Ausfall eines Netzrechners oder von einer Leitungsunterbrechung ist nicht das gesamte Netz, sondern nur der jeweilige Rechner betroffen. Falls allerdings der Zentralrechner nicht mehr funktioniert, fällt das gesamte Netz aus.

Eine sternförmige Verkabelung reicht allein jedoch nicht aus, da auch Sternstrukturen so realisiert sein können, daß die Signale an alle Netzteilnehmer gesendet werden. Zusätzlich sind intelligente Sternkoppler mit entsprechenden Filterfunktionen erforderlich, die Daten nur an diejenigen Teilnehmer senden, für die die Nachrichten bestimmt sind.

Wie bei anderen Datenschutzanforderungen stellt sich natürlich der Anwender auch hier die Frage, inwieweit diese Forderungen umsetzbar sind bzw. welchen Mehraufwand sie bedeuten. Zwar basieren viele marktgängige Netzwerke auf Bustopologien. Dennoch stehen seit einiger Zeit Netzwerke zur Verfügung (beispielsweise der Standard Ethernet 10Base‍T), die auf einer Sterntopologie auf-

bauen. Ausgangsbasis ist ein Konzentrator, in dem die Kabel zusammenlaufen, die Signale verstärkt werden und ggf. auch gefiltert werden können.

Da die Filterfunktion bislang noch nicht herstellerunabhängig normiert ist, muß allerdings auf herstellerspezifische Lösungen zurückgegriffen werden. Angesichts der zunehmenden datenschutztechnischen Anforderungen an Netzwerke ist erfreulicherweise zu beobachten, daß die Zahl der Firmen stetig zunimmt, die filternde Sternkoppler anbieten.

3.3.2 Glasfaser- und Twisted-Pair-Kabel

Entsprechende Software und Hardware sowie Detailkenntnisse vorausgesetzt, können Kupferkabel relativ leicht abgehört werden. Bei Koaxialkabeln wie beispielsweise dem gelben Ethernet-Kabel ist hierfür nicht einmal das Auftrennen der Kabel erforderlich.

Gebäudeexterne Verkabelungen sind daher möglichst mittels Glasfaserkabel durchzuführen, die zwar ebenfalls nicht völlig abhörsicher sind, aber dennoch einen hohen Schutz bieten. Die gebäudeinterne Verkabelung sollte – falls Lichtwellenleiter nicht zur Verfügung stehen – mittels Twisted-Pair-Kabeln erfolgen, die aus paarig miteinander verdrillten Kabeln bestehen. Da beim Abhören von Twisted-Pair-Kabeln die Ummantelung aufgetrennt werden muß, können Abhörversuche zumindest nachträglich erkannt werden.

Auf drahtlose Übertragungsmedien, z. B. Funksignale oder Infrarotlicht, ist aufgrund des hohen Abhörrisikos grundsätzlich solange zu verzichten, wie die Daten unverschlüsselt übertragen werden.

3.4 Verbesserung der Sicherheit von UNIX-Systemen

3.4.1 Fernwartung von UNIX-Systemen

Immer häufiger wird auch bei UNIX-Anlagen aus Kostengründen auf die Möglichkeit der Fernwartung zurückgegriffen. Dabei arbeitet der Techniker nicht mehr im Rechnerraum des Kunden, sondern ist über Kommunikationsnetze (z. B. Telefon) an den zu wartenden Computer angeschlossen. Auf die damit verbundenen datenschutzrechtlichen Risiken wurde bereits in einigen Veröffentlichungen des Hamburgischen Datenschutzbeauftragten hingewiesen (vgl. 11. TB, 3.3; IuK-Datenschutzbericht, 2.9; Datenschutzkonzept für UNIX-Mehrplatzanlagen, 5.6).

Da in der hamburgischen Verwaltung sehr viele UNIX-Mehrplatzanlagen eingesetzt werden, bei denen zunehmend auch durch Fernwartung die Betriebsabläufe überwacht, neue Programmversionen eingespielt oder Fehler diagnostiziert und beseitigt werden, sollen die bei diesen Systemen erforderlichen Datenschutzmaßnahmen hier noch einmal zusammengefaßt werden:

Die Initiative zum Aufbau einer Fernwartungsverbindung muß von der lokalen Systemverwaltung ausgehen. Das Wartungspersonal muß sich durch seine

Benutzerkennung identifizieren sowie durch Paßworteingabe authentisieren. Zusätzlich müssen die Fernwartungsaktivitäten von lokaler Seite mitverfolgt, kontrolliert und revisionssicher aufgezeichnet werden sowie gegebenenfalls beendet werden können.

Ist die Dateistruktur des Systems so angelegt, daß die Anwendungsdateien strikt von den Sytemdateien getrennt sind und alle sensiblen Daten in einem Dateisystem abgelegt werden, bietet UNIX die Möglichkeit, mit dem Befehl „umount" Dateisysteme mit sensiblen Daten dem Zugriff durch den Fernwartungsservice zu entziehen. Nach der Wartung kann dann das Dateisystem mit den personenbezogenen Daten durch den Befehl „mount" wieder aktiviert werden.

Um bei diesem Verfahren den Datenschutz zu gewährleisten, darf das Wartungspersonal keinen Systemverwalterstatus erlangen.

Andernfalls müssen die personenbezogenen Daten mit dem Befehl „crypt" verschlüsselt oder auf einem externen Sicherungsdatenträger gespeichert und von der Festplatte physikalisch gelöscht werden („destroy"-Befehl).

Besonders problematisch ist die Wartung von Anwendungsprogrammen (z. B. Datenbanksystemen), bei denen auch Dateisysteme mit personenbezogenen Daten gewartet werden sollen. Die Wartungsaktivitäten sollten in diesem Fall vor Ort durchgeführt und die Daten möglichst anonymisiert werden.

3.4.2 Systemverwaltung mit Vier-Augen-Prinzip

Eine Hauptschwäche des Betriebssystems UNIX ist die Unkontrollierbarkeit des Super-Users (vgl. Datenschutzkonzept für UNIX-Mehrplatzanlagen, 4.2). Er besitzt uneingeschränkte Rechte für sämtliche Dateien und kann jederzeit sensible Daten lesen und verändern.

Wenn auf einem System sehr sensible personenbezogene Daten verarbeitet werden, sollte der Super-User nur dann Zugang zur Betriebssystemebene (Shell-Zugang) bekommen, wenn das „Vier-Augen-Prinzip" gewährleistet ist. Dies bedeutet, daß der Systemverwalter eine zweite Person beteiligen muß, um die umfassenden Rechte unter der Kennung „root" auf Betriebssystemebene zu erlangen.

Die einfachste Möglichkeit zur Realisierung des Vier-Augen-Prinzips ist die Verwendung eines geteilten Paßwortes für die Kennung „root", bei der der Systemverwalter und eine weitere Person jeweils vier Stellen des Paßwortes eingeben. Der Nachteil dieser Lösung besteht darin, daß beide Beteiligte ein maximal nur vier Zeichen umfassendes Teilpaßwort kennen müssen und daß der Systemverwalter nach dem Login stets die vollen Rechte – einschließlich des Betriebssystemzugangs – besitzt.

Eine andere, aus unserer Sicht bessere Lösung, auf die wir bei einer Prüfung aufmerksam geworden sind, differenziert zwischen einer routinemäßigen,

menügesteuerten Systemverwaltung und dem ausnahmsweisen Wechsel auf die Betriebssystemebene unter der Systemverwalterkennung.

Für die Standard-Arbeiten meldet sich der Systemverwalter wie jeder andere Benutzer an. Er unterliegt dabei zunächst nicht dem Vier-Augen-Prinzip, erhält jedoch auch keine Shell-Berechtigung. Der Zugriff auf Betriebssystemebene wird dadurch ausgeschlossen, daß über entsprechende Einträge in der „root"eigenen „.profile"Datei – sie enthält Kommandos, die bei der Anmeldung am System automatisch ablaufen – ausschließlich innerhalb eines vordefinierten Auswahlmenüs gearbeitet werden kann. Bei einer sachgemäßen Ausgestaltung des Menüsystems können auf diese Weise mehr als 95 % der Systemverwaltung ohne direkte Eingabe von Betriebssystemkommandos abgewickelt werden.

Nur die privilegierten und mit einem hohen Sicherheitsrisiko verbundenen Betriebssystemkommandos unterliegen dem Vier-Augen-Prinzip. Wenn besondere Systemverwalteraufgaben den Zugang zur Betriebssystemebene erfordern, muß sich zunächst eine zweite Person am System unter einer speziell dafür eingerichteten Kennung anmelden, deren Paßwort der Systemverwalter nicht kennt. Nach der korrekten Paßworteingabe wird durch eine automatisch ablaufende Routine (entweder direkt aus der Datei „passwd" oder aus der Datei „.profile") das „su"-Kommando gestartet, das zur Eingabe des „root"-Paßwortes auffordert. Gibt der Systemverwalter nun sein Kennwort ein, besitzt er Super-User-Status und kann auch privilegierte Betriebssystembefehle absetzen. Es ist zweckmäßig, in die „.profile-Datei" der zweiten Person das „exit"-Kommando einzutragen, damit bei fehlerhafter Eingabe des „root"-Paßwortes automatisch eine Abmeldung erfolgt. Durch eine entsprechende Rechte-Vergabe sollte dabei gewährleistet werden, daß andere Benutzer – auch wenn sie Shell-berechtigt sind – das „su"-Kommando nicht ausführen können.

Diese zweite Lösung erfordert also die Eingabe von zwei vollständigen Paßwörtern und ist deshalb sicherer als die erste Alternative. Außerdem können durch die weitgehend menügestützte Systemadministration routinemäßige Systemverwalter-Tätigkeiten von Personen ohne spezielle DV-Kenntnisse durchgeführt werden.

Es muß jedoch ausdrücklich darauf hingewiesen werden, daß diese beiden Alternativen zwar die Systemsicherheit erhöhen, jedoch grundsätzlich ein UNIX-immanentes Restrisiko bestehen bleibt.

3.5 Telekommunikationsrichtlinie

Mit der am 1. April 1993 in Kraft getretenen Telekommunikationsrichtlinie (TK-RL) gibt es nun endlich eine aktuelle und verbindliche Regelung über den Betrieb und die Nutzung der Einrichtungen und Dienste für die sprachliche und nicht-sprachliche Telekommunikation in der hamburgischen Verwaltung (vgl. 9. TB, 4.2.2 und 10. TB, 4.3).

Die Telekommunikationsrichtlinie enthält in den wesentlichen Punkten datenschutzfreundliche Vorgaben. So dürfen in der Sprachkommunikation die Zielrufnummern nur um drei Stellen gekürzt gespeichert werden, so daß keine Identifikation der angerufenen Anschlüsse möglich ist.

Ein weiterer wichtiger Aspekt ist die Festlegung von Löschungsfristen. Die je Kostenstelle erhobenen Verbindungsdaten dürfen nicht länger als drei Monate gespeichert werden.

Zu begrüßen ist ferner, daß auch bei dem Betrieb von Telekommunikationsanlagen die in § 8 HmbDSG geforderten organisatorischen und technischen Maßnahmen zum Schutz personenbezogener Daten realisiert werden müssen.

Als problematisch könnte es sich im Zuge der Integration von sprachlichen und nichtsprachlichen Kommunikationsdiensten erweisen, daß in der TK-RL einige dieser datenschutzfreundlichen Regelungen nur für die sprachliche Kommunikation gelten. So ist bei der Datenkommunikation grundsätzlich eine vollständige Speicherung der Verbindungsdaten weiterhin zulässig.

Zur Zeit werden Durchführungsbestimmungen zur TK-RL erarbeitet. Dabei werden auch drei datenschutzrechtlich bedeutsame Fragen zu regeln sein:

— Der Betrieb und die Benutzung von Telefax-Einrichtungen sollten detailliert geregelt werden. Die mit dem Telefax-Dienst verbundenen Gefahren sollten konkret benannt werden, und es sollten strikte Vorgaben über Sicherheitsvorkehrungen in solchen Bereichen vorgesehen werden, in denen sensible personenbezogene Daten per Telefax übertragen werden (z. B. paßwortgeschützte Ausgabesperre, verschließbares Empfangsbehältnis).

— Die Speicherfristen der manuellen Belegabrechnung für private Ferngespräche sollten an die Fristen der automatischen Verarbeitung angeglichen werden. Eine Speicherfrist wie früher von jeweils einem Jahr ist nicht vertretbar.

— Die Veröffentlichung von Mitarbeiterdaten in Teilnehmerverzeichnissen ist zu präzisieren. Dabei muß auf das Widerspruchsrecht des Telekommunikationsteilnehmers deutlich hingewiesen werden, um Probleme, wie sie etwa mit der Veröffentlichung von Mitarbeiternamen im Hamburg Handbuch aufgetreten sind (vgl. 11. TB, 7.6), in Zukunft zu vermeiden (siehe 7.6).

Da der Hamburgische Datenschutzbeauftragte auch in die Erstellung der Durchführungsbestimmungen eng einbezogen wird, ist zu erwarten, daß in diesen Fragen – wie bereits in der TK-RL selbst – eine befriedigende Lösung gefunden wird.

3.6 Modernisierung des Behördennetzes

Zu den Zuständigkeiten des Anfang 1993 eingerichteten Landesamts für Informationstechnik (LIT) gehört auch der Betrieb des Behördenfernsprechnetzes. Die Modernisierung des Netzes soll jedoch als Bestandteil planerischer und

ministerieller Grundsatzaufgaben unter der Federführung des Senatsamts für den Verwaltungsdienst – Organisationsamt – (SfV) betrieben werden.

Im 11. TB (4.3) hatten wir über ein Gutachten berichtet, das sich mit der Digitalisierung des Behördennetzes befaßt. Inzwischen ist unter der Leitung des SfV eine Projektorganisation eingerichtet worden, die sich mit Fragen der Modernisierung des Behördennetzes beschäftigt und an der wir beteiligt sind.

Es soll zunächst die Frage geklärt werden, inwieweit an einem eigenen behördenübergreifenden Netz festgehalten werden sollte und welche Alternativlösungen sich bieten (Nutzung von externen, z.B von der TELEKOM betriebenen Netzen und Diensten). Im Hinblick auf die zu erwartenden Kommunikationsbedarfe zwischen öffentlichen Stellen wird auch auszuloten sein, wie mit technischen und organisatorischen Maßnahmen die Vertraulichkeit von Kommunikationsinhalten und von Verbindungsdaten sichergestellt werden kann.

Dabei wird zu berücksichtigen sein, daß der Rückgriff auf verwaltungsexterne Unternehmen für die Erbringung von Telekommunikationsdienstleistungen auch datenschutzrechtliche Konsequenzen hätte. Während auf das derzeitige vom LIT betriebene eigene Netz das Hamburgische Datenschutzgesetz anzuwenden ist und die Gewährleistung des Datenschutzes einer uneingeschränkten Kontrolle durch den Hamburgischen Datenschutzbeauftragten unterliegt, wären bei externen Netz- und Dienstanbietern die telekommunikationsrechtlichen Vorschriften (Postverfassungsgesetz, Fernmeldeanlagengesetz und die darauf basierenden Rechtsverordnungen) einschlägig. Dies würde möglicherweise bedeuten, daß der Hamburgische Datenschutzbeauftragte nicht mehr für die Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften zuständig wäre und daß Prüfungen durch die dann zuständige Aufsichtsbehörde nur noch anlaßbezogen – bei Vorliegen eines konkreten Verdachts – vorgenommen werden könnten, soweit es sich nicht um Auftragsdatenverarbeitung durch einen Dienstleister handelt. Es muß aber sichergestellt werden, daß die Aufsicht durch den Hamburgischen Datenschutzbeauftragten in diesem Bereich erhalten bleibt.

Da sich der gesamte Telekommunikationsbereich gegenwärtig in einer Umbruchphase befindet (z.B. durch europarechtliche Vorgaben zur Liberalisierung und Privatisierung), ist heute noch nicht absehbar, welche rechtlichen Konsequenzen eine Neukonzeption der Telekommunikationsbeziehungen in der hamburgischen Verwaltung tatsächlich haben würde. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 1993 hat gefordert, daß durch die Privatisierung und Liberalisierung des Fernmeldewesens der Datenschutz nicht beeinträchtigt werden darf. Auch wenn in Zukunft private Unternehmen im Wettbewerb miteinander stationäre Telefonnetze betreiben und entsprechende Dienste anbieten, muß die Einhaltung der datenschutzrechtlichen Bestimmungen in diesen Netzen und Diensten von einer unabhängigen Stelle nach bundesweit einheitlichen Kriterien und von Amts wegen kontrolliert werden können.

Einzelne Probleme des Datenschutzes im öffentlichen Bereich

4. Telekommunikation/Neue Medien

4.1 Mobilfunk

4.1.1 Datenschutzrechtliche Risiken der Mobilkommunikation

Die Verbreitung mobiler Sprach- und Datenübertragungsdienste hat in jüngster Vergangenheit stark zugenommen. Es ist zu erwarten, daß sich die Teilnehmerzahl mobiler Kommunikationsdienste weiter vergrößern wird.

Die mit der Nutzung von Mobilfunkdiensten verbundenen Vorteile gehen mit Gefährdungen für den Datenschutz einher. Neben den auch bei leitungsgebundenen Telekommunikationsdiensten gespeicherten Angaben, wer wann mit wem in Verbindung war, wird bei der Mobilkommunikation auch erhoben, wo sich die mobilen Teilnehmer jeweils aufhalten, damit sie erreicht werden können. Diese Standortinformationen könnten durch den Netz- oder Dienstbetreiber – aber auch von Dritten – zur Bildung sog. „Bewegungsprofile" mißbraucht werden.

Darüber hinaus ist vielfach auch die Vertraulichkeit der Kommunikationsinhalte gefährdet, insbesondere dann, wenn Daten unverschlüsselt per Funk übertragen werden. Anders als bei leitungsgebundener Kommunikation können die übertragenen Signale auf der Funkstrecke nicht physikalisch gegen unbefugtes Mithören und Aufzeichnen abgeschirmt werden.

Bei satellitengestützten Diensten ist es sogar möglich, die übertragenen Daten im gesamten, teilweise viele tausend Quadratkilometer umfassenden Abstrahlbereich des Satelliten unbemerkt aufzuzeichnen.

4.1.2 Mobile Datenkommunikation – MODACOM

Neben der Sprachkommunikation werden seit einiger Zeit auch Dienste zur mobilen Datenübertragung eingesetzt. Auch bei diesen Diensten ist mit wachsenden Teilnehmerzahlen zu rechnen. Ein derartiger zellularer Dienst wird von der Deutschen Bundespost TELEKOM unter dem Namen MODACOM betrieben, der am 1. Juni 1993 in Regelbetrieb gegangen ist und auch in Hamburg verfügbar ist.

Bis Ende 1995 soll MODACOM mit etwa 900 Basisstationen eine bundesweite Flächendeckung von 80 Prozent erreichen, wobei die vorhandenen Basisstationen für das Funktelefonnetz nach geringfügiger Modifikation mitgenutzt werden sollen.

Die Funkmodems buchen sich nach dem Anschalten im Netz ein, d.h. sie senden ein Signal aus, das von der nächsten Basisstation empfangen und an das

Netzkontrollzentrum weitergeleitet wird. Dadurch wird der Standort der mobilen Terminals dem Netz bekanntgegeben. Die Terminals werden in Standby-Modus versetzt und können die für sie bestimmten Nachrichten empfangen.

Die Teilnehmerauthentifikation erfolgt mittels einer eindeutigen hardcodierten Kennung (ID) der Funkmodems. Die ID wird von den Herstellern so in das Funkmodem integriert, daß jeder Versuch der Veränderung eine irreversible Zerstörung des Geräts zur Folge hätte.

Die ID's werden im Netzkontrollzentrum verwaltet. Beim Einbuchen wird geprüft, ob die übertragene ID zu den zugelassenen Dienstteilnehmern gehört. Auf diese Weise soll sichergestellt werden, daß nur autorisierte Teilnehmer den Dienst nutzen können.

Neben der eindeutigen ID können in den Funkmodems noch zusätzliche „Flotten-ID's" (FID) gespeichert werden, die es – ähnlich wie geschlossene Benutzergruppen (GBG) bei anderen Diensten – ermöglichen, an einen definierten weiteren Empfängerkreis („Flotte") gerichtete Nachrichten zu empfangen.

Die Daten werden auf der Luftschnittstelle – anders als bei den digitalen Mobiltelefondiensten D1 und D2 – nicht kryptographisch verschlüsselt übertragen. Allerdings erfolgt die Übertragung – aus Gründen der Übertragungssicherheit (Reduzierung der Bitfehlerrate) – verwürfelt. Die Daten können auf der Anwendungsebene, d.h. durch die Benutzer selbst, kryptographisch verschlüsselt werden. Die Anwendungsverschlüsselung kann jedoch nicht die zur Abwicklung der Kommunikation übertragenen Steuerungs- und Vermittlungsinformationen umfassen.

Wie in broadcastorientierten leitungsgebundenen Netzen (z.B. Ethernet) suchen sich die Funkmodems die für sie bestimmten Informationen aus dem übertragenen Datenstrom heraus. Dabei wird das Modem jeweils nur dann aktiviert, wenn eine Nachricht mit der jeweiligen Modem-ID oder einer im Modem gespeicherten FID übertragen wird.

Sowohl der genaue Authentifikationsmechanismus als auch das für die Datenübertragung verwendete Protokoll werden vom Betreiber und von den Herstellern geheimgehalten.

Für MODACOM ergibt sich folgende datenschutzrechtliche Beurteilung:

— Eine Bewertung der Systemsicherheit von MODACOM wird durch die Tatsache erschwert, daß die wesentlichen Systemfeatures nicht öffentlich gemacht werden. Die Systemsicherheit beruht offenbar zum großen Teil auf der Geheimhaltung der genauen Funktionsweise des Dienstes und der dabei verwendeten Protokolle („security by obscurity").

— Die ausschließliche Authentifikation der Teilnehmer gegenüber dem Netz mittels hardcodierter Kennungen ist deshalb problematisch, weil durch Manipulation (Änderung der Hardware-Adresse oder softwaremäßige Emulation) bzw. durch unautorisierten Nachbau Maskeraden möglich werden könnten.

— Da die Datenübermittlung per Funk unverschlüsselt erfolgt, könnten die übertragenen Informationen abgehört, aufgezeichnet und ausgewertet werden. Die Codierung nach einem stets gleichen, aber noch geheimgehaltenen Verfahren bietet zwar noch einen gewissen Schutz gegen „Gelegenheitshacker", kann jedoch professionellen Angreifern schwerlich widerstehen. Diese Schwachstelle erscheint als besonders problematisch, wenn per MODACOM die Authentifizierung bei stationären Rechnern erfolgt und Kennungen, Paßwörter oder sonstige sensible Informationen übertragen werden sollen. Die Nutzung des Dienstes für die Übertragung sensibler Daten kann deshalb nur dann vertreten werden, wenn auf der Anwendungsebene eine kryptographische Verschlüsselung implementiert wird.

— Durch die Sendung und Registrierung von Informationen über den Standort können die Teilnehmer auch von unautorisierten Abhörern lokalisiert und somit sowohl vom Dienstbetreiber als auch durch Dritte Bewegungsprofile erstellt werden. Da die Funkzellen bei MODACOM z.Zt. noch wesentlich größer sind als in den Funktelefonnetzen, sind die Standorte in derartigen Profilen allerdings nur verhältnismäßig grob abzubilden.

4.1.3 Forderungen zum Datenschutz bei der Mobilkommunikation

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich am 26./27. Oktober 1993 mit den Risiken der Mobilkommunikation auseinandergesetzt und folgende Forderungen aufgestellt, um den Datenschutz zu gewährleisten:

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

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

Zusätzlich kompliziert wird die Datenschutzproblematik bei der Mobilkommunikation dadurch, daß unter Umständen bei verschiedenen Dienst- und Netzbetreibern, aber auch bei anderen Unternehmen – den sogenannten Service-

Providern, die lediglich Dienste vermarkten –, personenbezogene Daten gespeichert werden.

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

Besonders problematisch ist es, wenn bei der internationalen Mobilkommunikation auch in solchen Staaten personenbezogene Daten gespeichert werden, in denen kein ausreichendes Datenschutzniveau gewährleistet ist oder in denen das Fernmeldegeheimnis nicht sichergestellt wird. Deshalb ist es erforderlich, auf internationaler Ebene Regelungen zu treffen, die den Datenschutz bei mobilen Kommunikationsdiensten gewährleisten."

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

4.2 Interaktives Fernsehen

Fernsehen und Rundfunk sind klassische „Verteildienste", d.h. Sendungen werden nicht addressiert, sondern zeitgleich an eine unbestimmte Zahl von Empfängern gesandt (Broadcasting). Als Verteilwege werden hierfür terrestrischer Funk (festinstallierte Sender), Satellitenfunk und auch Kabel genutzt.

Eine neuere Form broadcastorientierter Verfahren kommt beim sog. Pay TV zum Einsatz. Dabei werden die Sendungen codiert übertragen und können nur mittels besonderer Zusatzgeräte decodiert und sichtbar gemacht werden.

Während beim Broadcasting die Kommunikation in nur einer Richtung erfolgt, gestattet der Fortschritt in der Glasfaser- und Vermittlungstechnik die Installation solcher Breitbandnetze, in denen Informationen – z.B. bestimmte Fernsehsendungen – gezielt an einen Benutzer oder an einen geschlossenen Benutzerkreis übertragen werden. Anders als beim herkömmlichen Pay TV werden die Signale nur an die Adressaten übermittelt.

Damit eröffnen sich viele neue technische Kommunikationsmöglichkeiten, angefangen vom Pay per View (Zugriff auf bestimmte an zentraler Stelle vorgehaltene Sendungen) bis hin zu einem Fernsehrückkanal, bei dem der Zuschauer selbst an laufenden Sendungen teilnehmen kann, ohne sich in ein Studio zu begeben. Eine andere Klasse von Anwendungen kann mit dem Stichwort „Teleshopping" beschrieben werden. Dabei holt sich der Kunde visuelle und akustische Informationen über ihn interessierende Produkte aus einer Zentrale und bestellt per Rückkanal.

Die neue Technik, die häufig auch als „interaktives Fernsehen" bezeichnet wird, bringt erhebliche datenschutzrechtliche Risiken mit sich, da – anders als beim klassischen Einwegfernsehen – das Fernsehverhalten registriert und ausgewertet werden kann. Im Bereich der Breitbandkommunikation stellen sich mithin ähnliche Probleme, wie sie in der schmalbandigen Kommunikation bereits seit einigen Jahren bekannt sind, z. B. beim Bildschirmtext (2. TB, 3.1.1), im ISDN (vgl. 8. TB, 2.3) oder bei Mailboxsystemen (11. TB, 4.6.1).

Das Medienrecht ist einer der wenigen Bereiche, in denen in dieser Frage die rechtliche Normierung der technischen Realisierungsmöglichkeit vorausgeeilt ist. So enthält das Hamburgische Mediengesetz von 1985 (HmbMedienG) detaillierte Regelungen über den Datenschutz insbesondere in Zusammenhang mit der Verarbeitung von Verbindungsdaten. § 47 HmbMedienG bestimmt, daß Daten über den Abruf bzw. Empfang von Sendungen nur solange gespeichert werden dürfen, wie dies für die Vermittlung und Abrechnung erforderlich ist. Dabei dürfen Abrechnungsdaten nur so gespeichert werden, daß sich der Zeitpunkt, die Dauer, die Art und der Inhalt der empfangenen Angebote nicht erkennen lassen.

Der vom Senat vorgelegte Entwurf einer Mediengesetznovelle knüpft an diese Vorschriften an und enthält darüber hinaus zusätzliche Vorgaben über den Datenschutz bei rundfunkähnlichen Kommunikationsdiensten (vgl. 4.3.2). Datenschutzrechtlich wird den neuen Problemen auf diese Weise so weit wie möglich Rechnung getragen.

4.3 Persönlichkeitsrechte in den Medien mit dem Recht auf eigene Darstellung

4.3.1 Reality TV

In der Öffentlichkeit wird diskutiert, wie den Gefährdungen des Persönlichkeitsrechts durch Reality TV entgegengewirkt werden kann. Derartige vor allem im privaten Fernsehen gesendete Beiträge geben zum Teil authentische Videos wieder und erreichen hohe Einschaltquoten.

Unfallopfer, Helfer und andere Beteiligte werden gegen ihren Willen in die Öffentlichkeit gezogen und zum Gegenstand von Unterhaltungssendungen, wenn sie nicht ausnahmsweise eine wirksame Einwilligung erteilt haben. Die Menschenwürde, das Persönlichkeitsrecht und der Datenschutz werden in schwerwiegender Weise beeinträchtigt, ohne daß ein überwiegendes Informationsinteresse der Öffentlichkeit besteht.

Aus datenschutzrechtlicher Sicht haben wir im März 1993 gegenüber der Behörde für Inneres erklärt, daß die Beteiligung von Mitarbeitern des öffentlichen Rettungsdienstes, der Hilfsorganisationen und beauftragten Unternehmen an derartigen Aufnahmen unzulässig ist. Aufnahmen, die Rettungsdienstmitarbeiter während ihrer Einsätze anfertigen, sind Datenerhebungen. Sie sind

nach dem Hamburgischen Rettungsdienstgesetz nur zum Zweck der Notfallrettung, nicht jedoch zur Fernsehberichterstattung zulässig. Das Gesetz untersagt auch die Weitergabe von Aufnahmen, die ursprünglich zur Einsatzdokumentation angefertigt wurden, wenn hierauf Unfallopfer oder andere beteiligte Personen zu erkennen sind.

Mit der Behörde für Inneres besteht über diese Rechtsauffassung Einvernehmen; der Senat erklärte auf bürgerschaftliche Anfragen, die Behörde für Inneres wirke „im Rahmen der Dienst- und Fachaufsicht darauf hin, daß sich Dienststellen von Polizei und Feuerwehr nicht an Sendungen beteiligen, in denen menschliches Leid und Elend zu Unterhaltungszwecken dargestellt werden."

Die Bundesvereinigung der Notärzte hatte bereits Anfang 1993 ihre Mitglieder aufgefordert, aus diesen Gründen an derartigen Sendungen nicht mehr mitzuwirken. Große private Hilfsorganisationen haben ebenfalls erklärt, sich nicht mehr an solchen Aktionen von Fernsehveranstaltern zu beteiligen. Auf Initiative des Bundesinnenministers hat sich schließlich die Innenministerkonferenz der Länder im Mai 1993 mit Reality TV beschäftigt und an die Medien appelliert, sich ihrer mit der Presse- und Rundfunkfreiheit verbundenen Verantwortung bewußt zu sein und von einer die Menschenwürde verletzenden Berichterstattung Abstand zu nehmen.

Damit läßt sich dieser Teil des Problems, wie im öffentlichen Bereich auf die Einhaltung des Datenschutzes hingewirkt werden kann, klar beantworten. Bei Verstößen können die Landesdatenschutzbeauftragten ggf. durch förmliche Beanstandungen dafür sorgen, daß die öffentlichen Stellen nicht an der Weitergabe von Filmmaterial an die Fernsehsender mitwirken.

Sehr viel schwieriger ist das weitere Problem zu lösen, ob und inwieweit der Datenschutz unmittelbar gegenüber den Fernsehveranstaltern durchgesetzt werden kann. Sowohl die Rundfunkfreiheit als auch das Persönlichkeitsrecht sind Grundrechte, die in diesem Konfliktfall miteinander zum Ausgleich gebracht werden müssen.

Die Rundfunkfreiheit – mit dem in den deutschen Rundfunkgesetzen geregelten Medienprivileg der Fernsehveranstalter – führt nicht etwa dazu, daß die Fernsehsender von der Achtung der Menschenwürde und des Persönlichkeitsrechts freigestellt sind. Beide sind vielmehr gemäß den gesetzlich vorgeschriebenen Programmgrundsätzen von jedem Fernsehsender zu beachten.

Zum Persönlichkeitsrecht gehört auch das ausdrücklich gesetzlich geregelte Recht am eigenen Bild; danach dürfen Bilder „nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden." Aufnahmen von Unfällen und Katastrophen können zwar als Teil der Zeitgeschichte auch ohne Einwilligung zulässig sein; die Befugnis erstreckt sich aber nicht „auf eine Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten verletzt wird." Deshalb sind Fernsehberichte mit Bildern von Opfern und anderen Beteiligten anerkanntermaßen nur zulässig, soweit ein berechtigtes

Informationsinteresse der Öffentlichkeit besteht und nicht nur Neugier und Sensationslust befriedigt werden sollen.

Bei einer Verletzung des Persönlichkeitsrechts durch Videoaufnahmen für Reality TV haben die Betroffenen selbst die Möglichkeiten, ihre Rechte auf Unterlassung, Schadensersatz usw. unmittelbar gegenüber dem Fernsehsender geltend zu machen. Bei einer schweren Verletzung des Persönlichkeitsrechts führen die Schadensersatzansprüche auch zu Schmerzensgeld. Die Datenschutzbestimmungen der neueren Rundfunkgesetze enthalten außerdem zusätzliche Verfahrensregelungen zugunsten der Betroffenen hinsichtlich Auskunft, Berichtigung usw. (vgl. 4.3.2).

Klärungsbedürftig sind schließlich die Handlungsmöglichkeiten der Landesdatenschutzbeauftragten gegenüber den Fernsehveranstaltern. Die Besonderheit bei diesen Fernsehsendungen besteht darin, daß die Verletzung der Menschenwürde und des Persönlichkeitsrechts einerseits einen Verstoß gegen die Programmgrundsätze darstellt, die von den dafür zuständigen Gremien zu überwachen sind, und zugleich einen Verstoß gegen die Datenschutzbestimmungen, deren Einhaltung von den Datenschutzbeauftragten kontrolliert wird.

Aufgrund der Rundfunkfreiheit und des Zensurverbots (Art. 5 GG) können die Datenschutzbeauftragten als staatliche Stellen sicherlich nicht die Fernsehsendungen verbieten. Gleichwohl ist es durchaus erwägenswert, den Datenschutzbeauftragten das Recht einzuräumen, sich bei festgestellten Datenschutzverstößen an den Fernsehsender zu wenden, ihn auf den Verstoß hinzuweisen und zur Stellungnahme aufzufordern. Die Datenschutzbeauftragten könnten auf diese Weise durchaus wirksam tätig werden. Sie können außerdem streitige Fälle notfalls der Öffentlichkeit mitteilen.

Die Landesmedienanstalten als staatsunabhängige Gremien für die Aufsicht über die Fernsehsender haben dann die abschließenden Entscheidungen zu treffen bis hin zu der Möglichkeit, dem Fernsehveranstalter notfalls die Zulassung wegen Programmverstößen zu entziehen. Gegenüber dem staatsfreien Rundfunk können damit die staatsfreien Aufsichtsgremien die notwendigen Maßnahmen zum Schutz des Persönlichkeitsrechts durchsetzen.

4.3.2 Entwurf des Hamburgischen Mediengesetzes

Das Hamburgische Mediengesetz enthält Bestimmungen über den privaten Rundfunk, über den Offenen Kanal und über die Weiterverbreitung von Programmen in Kabelanlagen. Der Senat hat im April 1993 den Entwurf eines neuen Hamburgischen Mediengesetzes (Bürgerschaftsdrs. 14/4001 vom 27. April 1993 – HmbMedienGE) vorgelegt, das den veränderten rundfunkrechtlichen Rahmenbedingungen (insb. novellierter Rundfunkstaatsvertrag, EG-Fernsehrichtlinie) Rechnung tragen soll. Die Novelle beinhaltet jedoch auch wichtige Veränderungen für die Gewährleistung des Persönlichkeitsrechts und den Datenschutz.

Bereits das alte Gesetz enthielt in § 13 HmbMedienG eine Regelung über das Gegendarstellungsrecht, die in das neue Gesetz unverändert übernommen werden soll. Neu ist jedoch die Vorschrift in § 56 Abs. 1 HmbMedienGE, daß Gegendarstellungen, Unterlassungserklärungen und Widerrufe nicht nur – wie bisher – zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren sind wie die Daten selbst, sondern daß sie darüber hinaus bei einer Übermittlung der Daten gemeinsam mit diesen weiterzugeben sind. Dies bedeutet konkret, daß die Fernsehveranstalter bei einem Verkauf der Sendungen diese Erklärungen dem Käufer mitgeben müssen und daß bei Abrufdiensten jeweils auch die Gegendarstellungen zu übertragen sind.

Zur Klärung seiner Ansprüche kann der Betroffene von dem Rundfunksender Auskunft über die zu seiner Person gespeicherten Daten verlangen, zu denen auch Ton- und Videoaufzeichnungen gehören. Das Auskunftsrecht ist gemäß § 56 Abs. 2 HmbMedienGE daran gebunden, daß eine Berichterstattung bereits erfolgt ist, und es ist auf die der Berichterstattung zugrunde liegenden Informationen beschränkt. Der Betroffene kann dabei allerdings nicht die Namen der Personen erfahren, die bei der Herstellung der Sendung mitgewirkt haben oder von denen die Informationen stammen. Ferner soll eine Auskunft dann verweigert werden dürfen, wenn durch Mitteilung der Daten die journalistische Aufgabe durch Ausforschung des Informationsbestandes beeinträchtigt würde.

Der Betroffene kann – wie auch sonst im Datenschutzrecht – die Berichtigung unrichtiger Fakten verlangen. Nach der neuen Regelung in § 56 Abs. 3 HmbMedienGE hat er sogar die Möglichkeit, eine eigene Darstellung von angemessenem Umfang hinzuzufügen. Der Betroffene hat damit ein Wahlrecht, ob er nur die Berichtigung durch den Rundfunkveranstalter veranlaßt oder eine eigene Darstellung abgibt. Dies bedeutet allerdings nicht, daß er verlangen kann, selbst „auf Sendung" zu gehen; er kann vielmehr seine schriftliche Darstellung dem Veranstalter zuleiten.

Konsequenterweise müßte die eigene Darstellung – wie die presse- und rundfunkrechtliche Gegendarstellung und andere Erklärungen nach § 56 Abs.1 HmbMedienGE – für dieselbe Zeit wie die Daten aufbewahrt und bei einer Übermittlung gemeinsam mit diesen Daten übermittelt werden. Insoweit ist der Gesetzentwurf noch zu ergänzen; eine solche Ergänzung würde der Regelung für Archive, z. B. Pressearchive, in § 35 Abs. 5 Satz 3 BDSG entsprechen (siehe 1.3), bei der auch über die presserechtlichen Gegendarstellungen hinaus sonstige eigene Darstellungen erfaßt sind.

Neu sind auch die Bestimmungen über „rundfunkähnliche Dienste". Dabei handelt es sich um Dienste, „mit denen Texte einschließlich stehender Bilder (Textdienste), Tondarbietungen mit Musik und Sprache (Tondienste) oder bewegte Bilder (Bewegtbilddienste) entweder aus einem Speicher zum Abruf bereitgestellt oder fortlaufend zum Zugriff verbreitet werden, und die nicht Rundfunk sind" (§ 2 Abs. 7 HmbMedienGE). Die Gesetzesbegründung stellt klar, daß Textdienste, die sich der Leerzeile eines Fernsehsignals oder des Datenkanals

eines Hörfunksignals bedienen (Fernseh- bzw. Hörfunktext) zum Rundfunk zu rechnen sind. Dagegen wäre das interaktive Fernsehen mit individuellem Programmabruf (vgl. 4.2) als rundfunkähnlicher Dienst zu qualifizieren.

Während für Textdienste gemäß § 53 Abs. 2 Satz 2 HmbMedienGE die Datenschutzvorschriften des Btx-Staatsvertrages entsprechend Anwendung finden sollen, gelten für sonstige rundfunkähnliche Dienste die Datenschutzvorschriften des § 53 Abs. 1 HmbMedienGE und – über die dortige Verweisung – die Bestimmungen des § 28 Rundfunkstaatsvertrag (vgl. 4.3.3). Diese Bestimmungen sind insbesondere auch dann anzuwenden, wenn die Daten nicht in Dateien verarbeitet werden. Damit sollen die neuen Dienste in bereits bewährte Datenschutzregelungen und deren aktualisierte Fassung einbezogen werden.

4.3.3 Medienstaatsverträge

Die Einigung Deutschlands und andere Änderungen der rundfunkrechtlichen Rahmenbedingungen haben auch die Neufassung verschiedener medienrechtlicher Staatsverträge erforderlich gemacht. Mit dem Staatsvertrag über den Rundfunk im vereinten Deutschland wurden der Rundfunkstaatsvertrag mit Vorschriften über den öffentlich-rechtlichen und über den privaten Rundfunk, der ARD- und der ZDF-Staatsvertrag, der Rundfunkgebührenstaatsvertrag, der Rundfunkfinanzierungsstaatsvertrag und der Bildschirmtextstaatsvertrag novelliert. Ferner wurde – nunmehr unter Einbeziehung Mecklenburg-Vorpommerns – auch der NDR-Staatsvertrag neu gefaßt.

Im Hinblick auf den Datenschutz ergeben die neuen Staatsverträge ein erfreuliches Bild. Beispielhaft sei hier auf § 28 Rundfunkstaatsvertrag verwiesen, der detaillierte Vorgaben über die Verbindungsdatenverarbeitung enthält. Personenbezogene Daten über die Inanspruchnahme einzelner Programmangebote dürfen nur erhoben, verarbeitet und genutzt werden, soweit und solange dies erforderlich ist für den Abruf der Programmangebote oder die Abrechnung der Entgelte. Die Speicherung der Abrechnungsdaten darf den Zeitpunkt, die Dauer, den Inhalt, die Art und die Häufigkeit bestimmter in Anspruch genommener Programmangebote nicht erkennen lassen, es sei denn, der Teilnehmer beantragt schriftlich eine entsprechende Abrechnung. Die Übermittlung von Abrechnungs- und Verbindungsdaten an Dritte ist grundsätzlich unzulässig. Abrechnungsdaten sind zu löschen, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind; Verbindungsdaten sind nach Ende der jeweiligen Verbindung zu löschen.

Diese Vorschriften sind – anders als die Regelungen des BDSG für den privaten Bereich – auch auf solche Daten anzuwenden, die nicht in Dateien gespeichert sind.

Hinsichtlich des journalistisch-redaktionellen Bereichs enthalten die Staatsverträge wegen des „Medienprivilegs" lediglich Vorgaben bezüglich der Datensicherheit und des Datengeheimnisses sowie die Regelung der Rechte der

Betroffenen (Auskunft, Berichtigung, Gegendarstellung, Hinzufügung einer eigenen Darstellung – vgl. 4.3.2). Hingegen ist für die Verarbeitung von Verwaltungsdaten der Rundfunkanstalten das jeweilige Landesdatenschutzgesetz oder der jeweilige Staatsvertrag – für den NDR der neue NDR-Staatsvertrag mit Verweisung auf das Hamburgische Datenschutzgesetz – anzuwenden.

Die Einhaltung der Datenschutzvorschriften wird sowohl im NDR als auch im ZDF (im Unterschied etwa zum Hessischen Rundfunk und zu Radio Bremen, wo die jeweiligen Landesbeauftragten für den Datenschutz die Verarbeitung von Verwaltungsdaten durch die Sender kontrollieren) insgesamt nicht durch die Landesbeauftragten für den Datenschutz, sondern durch eigene Datenschutzbeauftragte der Rundfunkanstalten überwacht.

5. Umweltschutz

5.1 Fehlende Rechtsgrundlagen für die Umweltdatenverarbeitung

Nicht nur bei der Umweltbehörde, sondern auch in den verschiedensten Stellen der öffentlichen Verwaltung werden Daten erhoben oder gespeichert, die sich auf den Zustand der Umwelt, auf die Wirkung von Umweltbedingungen auf den Menschen und auf umweltbeeinflussende Maßnahmen beziehen.

Viele dieser Umweltdaten sind personenbezogen, d.h. sie enthalten Aussagen über Verhältnisse von natürlichen Personen (§ 4 Abs.1 HmbDSG). Für die Qualifizierung eines Datums als personenbezogen ist es nicht ausschlaggebend, ob der Name eines Betroffenen verarbeitet wird. Auch solche Daten, bei denen mit Zusatzwissen auf die Person geschlossen werden kann, sind personenbezogen (vgl. die – allerdings andere Anwendungsbereiche betreffende – Diskussion über den Personenbezug im 9. TB., 3.5.1, und im 11. TB, 27). Dementsprechend reicht es häufig schon aus, daß ein Umweltdatum geographisch eindeutig zugeordnet wird, um den Personenbezug herzustellen. Ein derartiges Anwendungsbeispiel ist die Speicherung der Tatsache, daß eine Fläche als Verdachtsfläche für Altlasten im Flächenbezogenen Informationssystem (FIS vgl. 12.1 und IuK-Datenschutzbericht, Exkurs 2) ausgewiesen ist.

Die Umweltbehörde speichert Umweltdaten in einer Vielzahl von bereits installierten oder im Aufbau befindlichen Fachinformationssystemen und Katastern. Mit dem Aufbau des Hamburger Umweltinformationssystems (HUIS) sollen die Daten aus diesen Fachinformationssystemen miteinander verknüpft werden (vgl. 5.3).

Wie auch in anderen Bereichen bedarf die Datenverarbeitung für Umweltzwecke bereichsspezifischer Regelungen. Nur in Teilbereichen sind derartige Regelungen bislang in Kraft getreten (vgl. § 98 ff Hamburgisches Wassergesetz).

Überfällig sind vor allem Regelungen für den Bereich Bodenschutz, denn hier fallen umfangreiche personenbezogene Daten an, die in einem Bodeninformationssystem zusammengefaßt werden sollen (BIS). Leider hat die Umweltbehörde das Gesetzgebungsverfahren im Berichtszeitraum nicht weiter vorangetrieben (vgl. 11. TB, 5.4). Dies erklärt der Senat damit, daß erst dann ein hamburgischer Entwurf vorgelegt werden soll, wenn Klarheit über die Vorstellungen des Bundesgesetzgebers herrscht (Bodenschutzkonzept, Bürgerschaftsdrs. 14/4644 vom 31. August 1993, S. 5). Da sich abzeichnet, daß mit einem Bundes-Bodenschutzgesetz nicht mehr in der laufenden Legislaturperiode zu rechnen sein wird, erscheint uns ein weiteres Abwarten nicht mehr vertretbar.

Von besonderer Bedeutung ist die Zusammenführung umweltbezogener personenbezogener Daten in Systemen, deren Zweckbestimmung nicht eindeutig geklärt ist. Ein derartiges System ist das Dioxinkataster, ein Datenbanksystem mit allen möglichen Daten, die einen Bezug zu dem „Ultragift" aufweisen. Neben Daten über Dioxinquellen (Emissionsdaten) und Daten über festgestellte Belastungen (Immissionsdaten) sollten nach den ursprünglichen Planungen auch Untersuchungsergebnisse von Personen gespeichert werden, die einer Dioxinexposition ausgesetzt waren. Ziel des Dioxinkatasters sollte es gleichermaßen sein, neue Erkenntnisse über Kontaminationswege zu gewinnen, in Verdachtsfällen besser reagieren zu können und auf Anfragen aus der Öffentlichkeit und dem Parlament antworten zu können.

Ein solches System ist aufgrund seiner Multifunktionalität als Vorratsdatenhaltung anzusehen, die datenschutzrechtlich besonders problematisch ist. Gerade wenn hierbei auch sensible personenbezogene Daten gespeichert werden sollen, ist genau festzulegen, welche Stellen welche Daten erheben und in das System einspeichern dürfen und wer auf welche Daten zugreifen darf. Ohne bereichsspezifische Regelungen, die dem Grundsatz der Verhältnismäßigkeit entsprechen, kann ein derartiger Datenbestand nicht vorgehalten werden.

5.2 Umsetzung der EG-Umweltinformationsrichtlinie

Durch die EG-Richtlinie vom 7. Juni 1990 sind die Mitgliedsstaaten der Europäischen Gemeinschaften verpflichtet worden, bis zum 13. Dezember 1992 nationale Rechts- und Verwaltungsvorschriften zu erlassen, die den Zugang zu Informationen über die Umwelt ermöglichen (vgl. 11.TB, 5.1).

Die Datenschutzbeauftragten des Bundes und der Länder haben am 16./17. Februar 1993 betont, daß sie in der Gewährleistung eines freien Zugangs zu Umweltinformationen einen wesentlichen Beitrag zu größerer Transparenz des Verwaltungshandelns sehen. Informationsfreiheit und Datenschutz bilden keinen unlösbaren Gegensatz, auch wenn bei personenbezogenen Umweltdaten das informationelle Selbstbestimmungsrecht zu beachten sei. Soweit wie möglich sollte deshalb dem Informationsinteresse in anonymisierter bzw. aggregierter Form Rechnung getragen werden. Wenn auf diese Weise das Informationsinteresse nicht erfüllt werden kann, sind Eingriffe in das Persönlichkeitsrecht nur unter klaren gesetzlichen Voraussetzungen möglich, wobei die Verfahrensrechte der Betroffenen zu wahren sind.

5.2.1 Umweltinformationsgesetz des Bundes

Der inzwischen von der Bundesregierung vorgelegte Umweltinformationsgesetzentwurf (Bundesrats-Drucksache 797/93 vom 5. November 1993) berücksichtigt zwar im wesentlichen die von den Datenschutzbeauftragten aufgestellten Forderungen zum informationellen Selbstbestimmungsrecht. Das von der EG-Richtlinie verfolgte Ziel, Umweltinformationen jedermann ohne übermäßige bürokratische Hürden zur Verfügung zu stellen, wird jedoch weitgehend verfehlt.

Die Tendenz im Referentenentwurf von 1992, der Vertraulichkeit der von öffentlichen Stellen gespeicherten Daten Vorrang vor dem Informationsinteresse des Bürgers einzuräumen, wurde mit dem vorliegenden Regierungsentwurf noch verstärkt.

Der Gesetzentwurf nutzt sämtliche von der EG-Richtlinie gegebenen Spielräume, durch nationales Recht den Informationsanspruch zu begrenzen. Für Daten über Umweltbeeinträchtigungen, die ihren Ursprung im Ausland haben, besteht hiernach ebensowenig ein Auskunftsanspruch wie über Umweltbelastungen militärischen Ursprungs.

Ferner soll es keinen Anspruch geben für die Dauer eines Gerichtsverfahrens oder eines strafrechtlichen Ermittlungsverfahrens sowie eines verwaltungsbehördlichen Verfahrens hinsichtlich der Daten, die der Behörde aufgrund des Verfahrens zugehen. Damit wird z.B. die Bekanntgabe von Informationen, die im Zusammenhang mit die Umwelt betreffenden Planfeststellungsverfahren anfallen, ausgeschlossen.

Zum Teil wird der von der Richtlinie vorgegebene Rahmen sogar überschritten: So soll der Antrag auf Information abgelehnt werden, wenn er sich auf die Übermittlung noch nicht abgeschlossener Schriftstücke oder noch nicht aufbereiteter Daten oder verwaltungsinterner Mitteilungen bezieht (im Referentenentwurf war – der EG-Richtlinie entsprechend – eine Kann-Vorschrift vorgesehen).

Während nach dem Referentenentwurf der Antragsteller – der EG-Richtlinie entsprechend – zwischen der Auskunft und dem direkten Zugang zu den Informationsträgern mit den begehrten Informationen wählen konnte, soll es jetzt der Behörde überlassen bleiben zu entscheiden, wie sie die Informationen zur Verfügung stellt. Daß damit der direkte Informationszugang – etwa die Akteneinsicht – zur Ausnahme wird, liegt auf der Hand.

Durch die Vorgabe in § 10 des Entwurfs, für Amtshandlungen aufgrund dieses Gesetzes kostendeckende Gebühren zu erheben, ist ferner zu befürchten, daß der Zugang zu Umweltinformationen ein Privileg für finanzkräftige Bürger, Unternehmen und Organisationen bleibt.

Demgegenüber orientiert sich der im September 1993 von der Bundestagsgruppe Bündnis 90/Die Grünen vorgelegte Entwurf eines Umweltinformationsgesetzes an dem Grundsatz, den Informationsinteressen des Bürgers Vorrang vor staatlichen Geheimhaltungsinteressen einzuräumen. Datenschutzrechtliche Belange von Betroffenen sollen berücksichtigt und Betriebs- und Geschäftsgeheimnisse gewahrt werden, ohne daß dabei der Anspruch auf freien Informationszugang leerläuft.

5.2.2 Umsetzung der EG-Richtlinie in Hamburg

Auf Hamburger Ebene wurden – anders als in anderen Bundesländern – bislang keine gesetzgeberischen Aktivitäten auf diesem Gebiet entfaltet.

Wie der Senat in der Antwort auf eine Kleine Anfrage (Bürgerschaftsdrs. 14/4442) berichtet hat, waren in Hamburg bis Mitte Juli 1993 insgesamt neun Anträge auf Informationszugang gestellt worden. Im Hinblick auf das Auskunftsverfahren scheint es – trotz entsprechender Empfehlungen der Umweltbehörde – nicht immer eine einheitliche und bürgerfreundliche Praxis der verschiedenen Behörden zu geben.

Als besonders problematisch erscheint es, daß in Einzelfällen die Auskunftserteilung mit unzumutbar hohen Gebühren verbunden werden sollte (so sollten pro fotokopierte Seite 12 DM bezahlt werden – zusätzlich zu weiteren Bearbeitungsgebühren). Wenn mit der Gebührengestaltung der Auskunftserteilung eine faktisch kaum zu überspringende Hürde vorgelagert würde, liefe das Informationszugangsrecht leer. Eine Prohibitivgebühr würde der mit der EG-Richtlinie verbundenen Zielsetzung widersprechen.

In einem weiteren Fall wurde einem Bürgerschaftsabgeordneten eine Auskunft nur unter der Bedingung zugesagt, daß er nicht als Abgeordneter, sondern als Privatperson anfrage, da die EG-Richtlinie sich nicht auf Mitglieder von Verfassungsorganen beziehe. Einer derartigen Interpretation der EG-Richtlinie ist nicht zu folgen, da es sich bei dem Informationszugangsrecht um ein Recht handelt, das jedermann – auch Abgeordneten – zusteht. Das Recht, durch bürgerschaftliche Anfragen die Verwaltung zu kontrollieren, ist ein zusätzliches Recht des Abgeordneten.

Die aufgezeigten Fälle machen deutlich, daß eine Verbesserung der Praxis der Auskunftserteilung und deren Absicherung in einer verbindlichen Regelung dringend geboten sind. Die nur mit Empfehlungscharakter gegebenen Hinweise der Umweltbehörde reichen offenbar nicht aus.

5.3 Hamburger Umweltinformationssystem (HUIS)

In der Umweltbehörde wird zur Zeit ein fach- und medienübergreifendes Informationssystem für die Verarbeitung und Aufbereitung umweltrelevanter Informationen entwickelt. Dieses soll einerseits die Planungs-, Auskunfts-, und Arbeitsfähigkeit der Umweltbehörde auch bei den zukünftigen Anforderungen sichern und effektivieren, andererseits den wachsenden Informationsbedarf von Öffentlichkeit, Politik und Verwaltung über den Zustand und die Entwicklung der Umwelt decken.

Durch unsere Beteiligung bereits während der Projektvorlaufphase konnten datenschutzrechtliche Risiken diskutiert und organisatorisch-technische Maßnahmen zum Datenschutz frühzeitig in der Gestaltung der HUIS-Konzeption berücksichtigt werden.

Datenschutzrechtlich problematisch ist insbesondere die Zusammenführung und Aufbereitung von personenbezogenen Daten aus unterschiedlichen Fachinformationssystemen, da diese Daten zweckgebunden erhoben wurden und innerhalb des HUIS nicht für einen anderen Zweck verarbeitet werden dürfen. Wir haben darauf hingewiesen, daß eine Zweckdurchbrechung nur in den in § 13 Abs. 2 HmbDSG normierten Ausnahmefällen zulässig ist. Die Umweltbehörde hat zugesichert, bei der Realisierung der HUIS-Konzeption auf diese Problematik zu achten und uns weiterhin über die Fortentwicklung von HUIS zu informieren.

6. Sozialwesen

6.1 Projekte Sozialhilfe-Automation (PROSA) und Jugendamts-Automation (PROJUGA)

PROJUGA (vgl. 11. TB, 6.3) hat in der Zwischenzeit keine inhaltliche Entwicklung erfahren und ist im Juli 1993 beendet worden. Die Automation der Jugendamtsbereiche soll durch PROSA abgedeckt werden.

Die Diskussion um statistische Auswertungen des PROSA-Datenbestandes (siehe 11. TB, 6.2) hat inzwischen eine neue Grundlage erhalten, da im Rahmen des Gesetzes zur Umsetzung des Föderalen Konsolidierungsprogrammes (FKPG) neue Statistikregelungen in das Bundessozialhilfegesetz eingefügt worden sind. Diese neuen Regelungen werfen allerdings einige schwierige Fragen auf.

Von den zahlreichen Daten, die statistisch ausgewertet werden sollen, sind einzelne nicht relevant für die Entscheidung über die Leistungsgewährung; beispielsweise gilt dies für die Staatsangehörigkeit und die Gründe für die Einstellung der Leistungen. Da das Gesetz keine Auskunftspflicht der Leistungsempfänger vorsieht, können diese Daten daher nur erhoben werden, wenn die Leistungsempfänger schriftlich ausdrücklich auf die Freiwilligkeit ihrer Angaben sowie auf andere nach dem Bundesstatistikgesetz vorgesehene Punkte hingewiesen werden.

Selbst wenn es auf freiwilliger Grundlage gelingen sollte, alle statistisch relevanten Angaben zu erheben, muß noch die verfassungsrechtlich erforderliche Trennung von Statistik und Verwaltungsvollzug realisiert werden. Daher dürfen die nur zu statistischen Zwecken erhobenen Daten mit den für die Leistungsgewährung erhobenen Daten nicht zusammengeführt werden. Auch die nach dem Bundesstatistikgesetz erforderliche Trennung der Hilfs- und Erhebungsmerkmale ist bei einer gleichzeitigen Speicherung im automatisierten Verfahren nicht gegeben.

Diese Fragen, zu denen wir mit PROSA in der Diskussion stehen, sind bislang noch ungelöst.

6.2 Entwurf des Zweiten Gesetzes zur Änderung des Sozialgesetzbuchs

Über den Gesetzentwurf haben wir zuletzt im 11. TB (6.1) berichtet. Nach dessen Redaktionsschluß haben wir erfahren, daß die Behörde für Arbeit, Gesundheit und Soziales (BAGS) in ihrer Stellungnahme gegenüber dem Bundesminister für Arbeit und Sozialordnung gerade die wesentlichen Mängel des Gesetzentwurfes nicht angesprochen hat, obwohl wir auf diese ausdrücklich aufmerksam gemacht hatten.

Der Gesetzentwurf ist in der Zwischenzeit überarbeitet worden. Nach der Stellungnahme des Bundesrates und einer Gegenäußerung der Bundesregierung hat der Bundestagsausschuß für Arbeit und Sozialordnung eine Beschlußempfehlung vorgelegt. Daraufhin hat der Bundestag den Gesetzentwurf am 3. Dezember 1993 angenommen.

Leider hat es in den wesentlichen Fragen noch keine durchgreifende Verbesserung gegeben. Zu diesen wesentlichen Punkten zählen die Regelungen der Datenerhebung, der Zweckbindung und der Kontrollbefugnisse der Landesdatenschutzbeauftragten. Die Datenerhebung soll nach dem Gesetzentwurf künftig weitgehend hinter dem Rücken der Betroffenen erfolgen können, eine Zweckbindung soll es künftig praktisch nicht mehr geben und die Landesdatenschutzbeauftragten sollen deutlich weniger kontrollieren dürfen als bei anderen öffentlichen Stellen wie z.B. Schulen. Sogar die Abschaffung der seit vielen Jahren bewährten Institution des betrieblichen Datenschutzbeauftragten bei Sozialleistungsträgern wird erwogen.

Damit droht das Sozialgesetzbuch zu einem eindrucksvollen Beispiel dafür zu werden, wie Datenschutz zwar bereichsspezifisch geregelt wird, aber ohne dabei die weiteren vom Bundesverfassungsgericht im Volkszählungsurteil genannten Kriterien für eine verfassungsgemäße Datenverarbeitung einzuhalten. Statt eine verfassungsgerichtliche Überprüfung abzuwarten, wäre es vorzuziehen, daß Hamburg im Gesetzgebungsverfahren noch auf eine verfassungskonforme Datenschutzregelung hinwirken würde.

6.3 Entwurf des Ausführungsgesetzes zum Kinder- und Jugendhilfegesetz

Bald drei Jahre nach dem Inkrafttreten des Kinder- und Jugendhilfegesetzes gibt es in Hamburg noch kein Ausführungsgesetz. Ein erster Referentenentwurf (nachfolgend: AGKJHG) ist uns aber im Berichtszeitraum zugegangen. Er soll das Ausführungsgesetz zum Jugendwohlfahrtsgesetz (AGJWG) ersetzen.

Aus datenschutzrechtlicher Sicht verdienen im Zusammenhang mit dem Gesetzentwurf drei Punkte besondere Beachtung: Die Regelungen der Zusammensetzung und Stellung des Jugendhilfeausschusses, die Regelungen zur

Kinder- und Jugendhilfestatistik und die notwendige Abgrenzung der privatrechtlichen von den öffentlich-rechtlichen Aufgaben des Jugendamtes.

6.3.1 Jugendhilfeausschuß

Im 11. TB (6.7.1) haben wir bereits darauf hingewiesen, daß die gegenwärtige Regelung des § 2 Abs. 9 Satz 4 AGJWG, nach der dem Jugendhilfeausschuß Aufgaben eines Fachausschusses der Bezirksversammlung übertragen werden dürfen, problematisch ist. Zwar ist die Preisgabe personenbezogener Daten im Rahmen des jeweils Erforderlichen sowohl gegenüber dem Hauptausschuß der Bezirksversammlung als auch gegenüber dem Jugendhilfeausschuß zulässig. Die das Maß des Erforderlichen bestimmenden Kriterien sind jedoch unterschiedlich. Die Wahrnehmung von Kontrollaufgaben, bei der ein Fachausschuß beratend hinzugezogen werden könnte, wird typischerweise in stärkerem Maße der Kenntnis personenbezogener Daten bedürfen als die nur anregende Tätigkeit des Jugendhilfeausschusses. Wenn der Jugendhilfeausschuß in einer gleichzeitigen Funktion als Fachausschuß einen erweiterten Zugang zu solchen personenbezogenen Daten erhält, die ihm „eigentlich" nicht zustehen, handelt es sich um eine datenschutzrechtlich bedenkliche Folge mangelnder funktionaler Aufgabentrennung. Eine strikte Zweckbindung für Daten wird sich kaum gewährleisten lassen.

Im jetzigen Gesetzentwurf ist vorgesehen, die bislang lediglich fakultativ mögliche Aufgabenübertragung auf den Jugendhilfeausschuß durch eine obligatorische Aufgabenzuweisung zu ersetzen. Damit würde die bereits latent vorhandene Problematik künftig zwangsläufig häufiger akut werden.

Diese Bedenken werden zusätzlich verstärkt durch die im Entwurf vorgesehene Zusammensetzung des Jugendhilfeausschusses. Neben den von der Bezirksversammlung gewählten stimmberechtigten Mitgliedern sollen dem Jugendhilfeausschuß noch dreizehn beratende Mitglieder angehören, die aus dem kirchlichen Bereich, aus verschiedenen Behörden bis hin zur Polizei und aus dem nicht-institutionalisierten Bereich kommen sollen. Darüber hinaus soll es auch möglich sein, daß der Jugendhilfeausschuß sogar Unterausschüsse bilden darf unter Einbeziehung von Personen, die nicht Mitglied des Jugendhilfeausschusses sind.

Mit Blick auf die vorgesehene Einbeziehung eines Vertreters der Polizei in den Jugendhilfeausschuß und vor dem Hintergrund der öffentlichen Diskussion um bestimmte Jugendliche („Autokids") bedarf es wohl keiner näheren Ausführung, daß Interessenkonflikte unvermeidbar sind, wenn der Jugendhilfeausschuß personenbezogene Daten erhält.

Nach Möglichkeit sollte daher ganz darauf verzichtet werden, daß der Jugendhilfeausschuß zugleich Fachausschuß der Bezirksversammlung ist. Mindestens müßte aber ausgeschlossen werden, daß die beratenden Mitglieder Kenntnis von personenbezogenen Daten erhalten, die dem Jugendhilfeausschuß zur Verfügung gestellt wurden.

6.3.2 Kinder- und Jugendhilfestatistik

Nach dem Gesetzentwurf sollen im Rahmen einer Landesstatistik auch Straßen und Hausnummern zu den Erhebungsmerkmalen gehören. Dies begegnet erheblichen datenschutzrechtlichen Bedenken, da mit der genauen Adreßangabe praktisch immer eine Identifizierung des Betroffenen möglich ist. Soweit aus erhebungstechnischen Gründen die Daten adreßgenau erhoben werden sollen, käme es allenfalls in Betracht, die Hausnummer als Hilfsmerkmal zu erheben und nach Durchführung der Vollständigkeits- und Plausibilitätskontrollen frühestmöglich von den Erhebungsmerkmalen zu trennen und zu löschen.

Weiter ist vorgesehen, daß dem Senat und der zuständigen Fachbehörde auch Tabellenfelder übermittelt werden dürfen, die nur einen einzigen Fall ausweisen. Dies ist äußerst problematisch, weil sich diese Daten auch bei Verzicht auf die Hausnummer als Erhebungsmerkmal relativ leicht einzelnen Personen zuordnen lassen. Deshalb sollte auf diese Regelung verzichtet werden. Sollte es gleichwohl bei dieser Regelung bleiben, bedürfte es einer Klärung durch das Gesetz, in welcher Weise solche statistischen Daten verwendet werden dürfen. Anders als § 6 Abs. 3 Hamburgisches Statistikgesetz (HmbStatG) enthält der Regelungsentwurf aber keine Aussage darüber, zu welchen Zwecken der Senat bzw. die Fachbehörde einzelfallbezogene Tabellenfelder erhalten dürfen. Anzustreben wäre dabei eine auf rein interne Planungszwecke beschränkte Zweckbindung.

Eine Übernahme der Regelung des § 6 Abs. 3 HmbStatG auch insoweit, als Tabellen mit Einzelfällen gegenüber der Bürgerschaft, also öffentlich, verwendet werden dürfen, wäre im Bereich des Sozialdatenschutzes als unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht abzulehnen.

Darüber hinaus muß auch ausgeschlossen sein, daß Statistiken, die nicht aggregierte, sondern personenbezogene Daten enthalten, im Jugendbericht veröffentlicht werden.

6.3.3 Abgrenzung verschiedener Aufgaben des Jugendamtes

Während die Aufgaben und Tätigkeiten des Jugendamtes grundsätzlich öffentlich-rechtlicher Natur sind, ist dessen Tätigkeit als Amtsvormund oder -pfleger bürgerlich-rechtlicher Natur. Frühere Streitfragen insoweit sind durch die neuen Regelungen des Kinder- und Jugendhilfegesetzes ausgeräumt. Demnach ist die Führung von Amtspflegschaften und -vormundschaften durch das Jugendamt nicht zu den Sozialleistungen zu rechnen. Damit läßt es sich kaum vereinbaren, wenn in den bezirklichen Jugendämtern vom Amtspfleger in Personalunion auch zusätzlich Aufgaben der Jugendhilfe, die nicht zur Führung der Amtspflegschaft zu rechnen sind, hinsichtlich derselben Jugendlichen wahrgenommen werden.

Vordergründige praktische Auswirkung dieser Aufgabenvermengung ist, daß der Jugendamtsmitarbeiter zwei Akten über dieselbe Person führt, die Jugend-

hilfeakte und die Amtspflegschaftsakte. Unmittelbare datenschutzrechtliche Relevanz bekommt diese Aufgabenverquickung, wenn der Mitarbeiter entscheiden muß, welche Daten er erheben und wie er sie weiter verarbeiten darf. In diesem Zusammenhang muß er nicht nur klären, welches Datenschutzrecht anzuwenden ist. Er läuft vielmehr Gefahr, in einer Funktion Daten zu erheben, die er in der anderen Funktion nicht erheben dürfte. Bei der Klärung des anzuwendenden Datenschutzrechts muß er stets vorher klären, im Rahmen welcher Tätigkeit (bürgerlich-rechtliche Pflegschaft/Vormundschaft oder öffentlich-rechtliche Kinder- und Jugendhilfe) er bestimmte Informationen erhalten hat. Ihm wird insoweit gewissermaßen eine „funktionale Persönlichkeitsspaltung" abverlangt.

Unsere Bedenken dagegen, daß diese verschiedenen Aufgaben durch eine Person wahrgenommen werden, werden von der Behörde für Schule, Jugend und Berufsbildung (BSJB) geteilt. Sie hat dies dem Senatsamt für Bezirksangelegenheiten (SfB) mitgeteilt, das für Organisationsangelegenheiten in den Bezirken zuständig ist. Das SfB will die gebotenen organisatorischen Änderungen im Rahmen der Neuorganisation erzieherischer Hilfen (Projekt NERZ) und und der Neuorganisation der bezirklichen Jugendämter vornehmen. Aus Anlaß des AGKJHG sollte die insoweit gebotene Änderung der Strukturen der bezirklichen Jugendämter gesetzlich abgesichert werden. Mit diesen Änderungen ließe sich zugleich die auch verfassungsrechtlich gebotene Gleichbehandlung von behördlich und nicht-behördlich geführten Vormundschaften, Pflegschaften, Beistandschaften und Gegenvormundschaften erreichen.

Wir haben der BSJB diese verschiedenen Probleme dargestellt und auch einen Formulierungsvorschlag für den Gesetzentwurf gemacht.

6.4 Prüfung zweier Betriebskrankenkassen

Im Berichtszeitraum haben wir zwei Betriebskrankenkassen (BKKen) allgemein datenschutzrechtlich überprüft und einige ergänzende Feststellungen beim Landesverband-Nord der Betriebskrankenkassen getroffen. Dabei haben wir festgestellt, daß die BKKen nicht alle datenschutzrechtlichen Anforderungen erfüllen.

— Existenzberechtigung

Klärungsbedürftig ist bei einer der BKKen, ob sie überhaupt noch existieren darf, da die Zahl der versicherten Beschäftigten bei ihr sehr gering ist. Sofern dadurch die Leistungsfähigkeit der BKK nicht mehr auf Dauer gesichert ist, müßte sie gemäß § 153 Satz 1 Nr. 3 Sozialgesetzbuch/Fünftes Buch (SGB-V) geschlossen werden. Da die Zulässigkeit der Existenz der BKK Grundvoraussetzung für die Zulässigkeit ihrer Datenverarbeitung ist, haben wir diese Frage an die Behörde für Arbeit, Gesundheit und Soziales als Aufsichtsbehörde herangetragen.

— Personalkrankenkasse

Unbefriedigend gelöst ist die Bearbeitung von Krankheitsfällen der Mitarbeiter beider BKKen. Diese erfolgt durch den Geschäftsführer, der der Vorgesetzte dieser Mitarbeiter ist. Nach § 284 Abs. 4 SGB-V muß aber sichergestellt sein, daß Personen, die kasseninterne Personalentscheidungen treffen oder an ihnen mitwirken dürfen, keinen Zugriff auf Versicherungs- und Leistungsdaten dieser Beschäftigten haben.

— Dienstanweisungen

Für beide BKKen gibt es jeweils nur eine Dienstanweisung, die gemäß § 286 SGB-V die automatisierte Datenverarbeitung regeln soll. Sie ist jedoch recht allgemein gehalten und erfüllt die Anforderungen der Vorschrift inhaltlich nur unzureichend. Die nach § 35 SGB-I grundsätzlich vorgesehene Dienstanweisung, mit der sichergestellt werden soll, daß die Versichertendaten nur Befugten zugänglich sind, halten wir für ausnahmsweise entbehrlich; der Personalkörper der BKKen ist so klein, daß sich auch ohne förmliche interne Regelung eine Einhaltung des Sozialgeheimnisses erreichen läßt. Wir haben die BKKen aber darauf hingewiesen, daß der BKK-Bundesverband allen seinen Mitgliedskassen eine Arbeitshilfe zur Verfügung gestellt hat, in der zahlreiche Beispiele zu den gesetzlichen Offenbarungstatbeständen aufgeführt werden.

— Löschungen

Nicht eingehalten werden die Löschungsfristen für die Versichertendaten. Hier gilt, daß Leistungsdaten gemäß § 304 Abs. 1 Satz 1 Nr. 1 SGB-V grundsätzlich nach zehn Jahren zu löschen sind. Für Mitgliederdateien nehmen beide BKKen eine Aufbewahrungsdauer von dreißig Jahren nach Beendigung der Versicherung an. Dies entspricht § 45 der früher geltenden Verwaltungsvorschriften über das Rechnungswesen bei den Krankenkassen und wird auch von vielen anderen Krankenkassen so gesehen (vgl. Bundestagsdrucksache 12/5441). Unter den im Archiv gesichteten Unterlagen befanden sich jedoch auch Leistungskarten, die deutlich älter als zehn Jahre (vom Datum des Ausscheidens an gerechnet) waren. Auf Nachfrage wurde dazu erklärt, die Leistungskarten hätten früher zugleich die Mitgliederkartei gebildet. Allerdings reichten die Karteikarten teilweise bis in die 50er Jahre zurück, waren also älter als 30 Jahre.

— Vordrucke und Schweigepflichtentbindungserklärungen

Kritik mußten wir auch an zahlreichen von den BKKen verwendeten Vordrucken üben. Anders als vom Gesetz gefordert, werden die Versicherten darin nicht auf eine etwaige Mitwirkungspflicht oder die Freiwilligkeit ihrer Angaben hingewiesen. Besonders bedenklich ist aber das Verfahren zur Erhebung von Daten bei Ärzten. Bei einem solchen Auskunftsbegehren muß die BKK den Arzt darauf hinweisen, welche Rechtsgrundlage ihn zur Aus-

kunft verpflichtet. In aller Regel gibt es eine solche Rechtsgrundlage aber nicht, so daß die BKK dem Arzt eine Schweigepflichtentbindungserklärung des Versicherten vorlegen müßte. Die BKKen lassen sich eine solche Erklärung für den Arzt aber nicht geben, sondern fordern den Arzt ohne Nennung einer Rechtsgrundlage und ohne Vorlage einer Schweigepflichtentbindungserklärung zur Auskunft auf. Erstaunlich daran ist, daß die Ärzte diese Auskünfte in aller Regel trotzdem erteilen. Insoweit kann nur gehofft werden, daß die Ärzte sich vorher unmittelbar von ihren Patienten eine Schweigepflichtentbindungserklärung geben lassen.

— Externe Überprüfungen

Gemäß ihren Satzungen werden beide BKKen von ihrem jeweiligen Vorstand überprüft; dagegen ist datenschutzrechtlich nichts einzuwenden. Daneben erfolgen aber auch regelmäßige Überprüfungen durch den BKK-Landesverband. Hierfür gibt es jedoch nach unserer Auffassung keine Rechtsgrundlage.

— Schlußfolgerungen

Unsere Kritik haben wir den BKKen im einzelnen mitgeteilt und sie aufgefordert, erforderlichenfalls in Zusammenarbeit mit dem BKK-Landesverband und der Aufsichtsbehörde zu Verbesserungen zu kommen.

6.5 Aufdeckung von Sozialhilfemißbrauch

Seit einiger Zeit wird eine öffentliche Diskussion um den Mißbrauch von Sozialhilfe geführt. Sie wird dazu genutzt, im Sozialhilfebereich mit sehr weitreichenden Regelungen den Datenschutz erheblich abzubauen (siehe 1.2). Die undifferenzierte Diskreditierung der Sozialhilfeberechtigten und ihrer Angehörigen wird dabei in Kauf genommen.

6.5.1 Datenabgleiche

Diese Diskussion schlägt sich auch nieder im Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms (FKPG), mit dem ein neuer § 117 in das Bundessozialhilfegesetz (BSHG) eingefügt wurde. Diese Vorschrift schafft die Grundlage für automatisierte Datenabgleiche der Sozialhilfeträger mit der Bundesanstalt für Arbeit, den gesetzlichen Unfall- und Rentenversicherungsträgern und mit anderen Sozialhilfeträgern.

Mit den Datenabgleichen soll verhindert werden, daß unberechtigt Leistungen bei diesen verschiedenen Stellen gleichzeitig bezogen werden. Zu diesem Zweck müßten die Sozialhilfeträger bestimmte Daten aller ihrer Hilfeempfänger an die genannten anderen Leistungsträger übermitteln. Diese würden dann prüfen, ob auch sie diesen Personen Leistungen gewähren und das ggf. dem anfragenden Sozialhilfeträger mitteilen. Unmittelbar im Anschluß an diese Überprüfung müßten die Datensätze gelöscht werden.

Das Grundproblem dieser Regelung liegt darin, daß der anfragende Sozialleistungsträger wahllos alle seine Leistungsempfänger an die anderen Leistungsträger offenbart, obwohl der ganz überwiegende Teil der Betroffenen sich völlig korrekt verhält. Praktiziert werden können diese Verfahren allerdings gegenwärtig noch nicht, da Einzelheiten noch in Rechtsverordnungen geregelt werden müssen, die noch nicht vorliegen. Im übrigen schaffen diese Vorschriften nur eine Befugnis, nicht jedoch eine Verpflichtung zur Vornahme dieser Datenabgleiche.

Ob in Hamburg der politische Wille besteht, diese Verfahren zu praktizieren, ist uns bislang nicht bekannt. Immerhin hatte der Senat bereits in der Bürgerschaftsdrucksache 14/2174 zutreffend darauf hingewiesen, daß ein systematischer Abgleich der Daten bestimmter Gruppen von Sozialhilfeempfängern unverhältnismäßig und damit unzulässig wäre, sofern nicht belegt werden könnte, daß eine nennenswerte Anzahl der betroffenen Personen unberechtigt Sozialhilfe bezieht und sich damit des Unterstützungsbetruges schuldig macht.

Die Richtigkeit dieser Einschätzung und damit der Unzulässigkeit des beschriebenen regelhaften Abgleiches wird im übrigen durch die noch unveröffentlichten Erkenntnisse der Arbeitsgruppe „Aufdeckung und Bekämpfung von Mißbräuchen des Asylrechts" belegt. Danach führen Fälle des Sozialhilfebezuges trotz gleichzeitiger Erwerbstätigkeit nur in geringem Umfang zu mißbräuchlicher Inanspruchnahme der Sozialhilfe und könnten zudem in aller Regel durch bessere Beratung vermieden werden.

6.5.2 Auskunftsverpflichtungen

Des weiteren enthält § 117 Abs.3 BSHG eine unmittelbar anwendbare Vorschrift, nach der die Sozialhilfeträger zur Vermeidung rechtswidriger Inanspruchnahme der Sozialhilfe bei anderen Stellen der Verwaltung bestimmte Daten der Leistungsempfänger überprüfen dürfen. Dies ist zwar grundsätzlich nichts Neues, sondern war nach §§ 20, 21 des Sozialgesetzbuches/Zehntes Buch (SGB-X) auch bislang schon möglich. Diese für alle Sozialleistungsträger geltenden Amtsermittlungs-und Beweiserhebungsvorschriften werden hinsichtlich der zulässigen Datenkränze durch § 117 Abs.3 BSHG für die Sozialhilfeträger konkretisiert und dadurch zugleich eingeschränkt. Neu ist allerdings, daß eine Auskunftsverpflichtung für die anderen Stellen der Verwaltung geschaffen wurde. Eine solche Auskunftsverpflichtung enthalten die §§ 20, 21 SGB-X bisher und weiterhin nur für die Finanzbehörden.

6.5.3 Unbedenkliche Maßnahmen

Unbestreitbar ist, daß wohl jede Form staatlicher Leistungen in einem gewissen Maße mißbraucht werden kann. Dies ist der hinzunehmende Preis in einem demokratischen freiheitlichen Staat. Einen völligen Ausschluß solcher Mißbräuche könnte man nur durch die totale Überwachung der Bürger erreichen, die aber verfassungswidrig wäre. Sie ist auch schon deshalb nicht anzustreben,

weil sie mit Sicherheit teurer ist als ein gewisses Maß des Mißbrauchs. Die öffentliche Diskussion sollte aber nicht den Blick dafür verstellen, daß es ein ausgeklügeltes System gibt, mit dem Leistungsmißbräuche verhindert oder aufgedeckt werden.

Zu den datenschutzrechtlich unbedenklichen Maßnahmen, mit denen einem Sozialhilfemißbrauch begegnet werden kann, gehören eine bessere Beratung der Sozialhilfeempfänger, die Zentralisierung der Zuständigkeit der Sozialhilfedienststellen für Asylbewerber, die Verkürzung der Auszahlungszeiträume für Sozialhilfe und auch die in Schleswig-Holstein bereits praktizierte Stichtagslösung. Der nicht zweckentsprechenden Verwendung von Sozialhilfe kann im begründeten Einzelfall dadurch begegnet werden, daß anstelle von Bargeld Gutscheine für Sachleistungen vergeben werden.

6.5.4 Sozialversicherungsausweis

Während den Sozialhilfeempfängern oft kriminelle Energie unterstellt wird, soll hier im übrigen einmal klargestellt werden, daß der unzulässige Sozialhilfebezug bei gleichzeitiger Erwerbstätigkeit in aller Regel ein rechtswidriges Verhalten des Arbeitgebers voraussetzt. Nach § 95 SGB-IV erhält jeder Beschäftigte einen Sozialversicherungsausweis (SVA), den er im Falle des Sozialhilfebezugs grundsätzlich beim Sozialhilfeträger hinterlegen muß (§ 100 SGB-IV). Den SVA muß sich jeder Arbeitgeber vor der Einstellung zeigen lassen; in bestimmten Branchen (Bau, Schausteller, Gebäudereinigung u.ä.) gilt sogar eine Mitführungspflicht für den Beschäftigten (§ 99 SGB-IV).

Hat der Beschäftigte bis zum Beginn der Beschäftigung keinen SVA vorgelegt, z.B. weil er ihn beim Sozialhilfeträger hinterlegen mußte, muß der Arbeitgeber dies der Einzugsstelle für den Gesamtsozialversicherungsbeitrag melden (§ 102 SGB-IV). Diese darf dem zuständigen Träger der Sozialhilfe oder AFG-Mittel die Nicht-Vorlage des SVA und weitere ihr bekannte Daten offenbaren, die zur Beurteilung der Rechtmäßigkeit des Leistungsbezuges erforderlich sind. Dieses Verfahren greift natürlich dann nicht, wenn ein Arbeitgeber sich darüber hinwegsetzt, daß ein Beschäftigter keinen SVA besitzt.

6.6 Rückforderung überzahlter Renten

Bereits seit geraumer Zeit beschäftigt uns ein Problem der Krankenkassen, das zwar bundesweite Bedeutung, aber bei Krankenkassen in anderen Ländern und im Bund bislang offenbar vergleichsweise wenig Aufmerksamkeit erfahren hat. Es geht dabei um Ermittlungen des Rentenversicherungsträgers, wenn er im Falle des Todes eines Rentners zuviel gezahlte Renten zurückfordern muß.

Im einzelnen stellt sich die Problematik wie folgt dar: Ausgezahlt werden Renten nicht unmittelbar durch die Rentenversicherungsträger, sondern durch die Rentenrechnungsstelle der Deutschen Bundespost. Das Rentenbezugsrecht endet mit dem Ablauf des Todesmonats des Berechtigten. Damit die Rentenrechnungsstelle vom Todesfall frühzeitig erfährt, sind im Melderechtsrahmengesetz und in der Zweiten Meldedaten-Übermittlungsverordnung des Bundes Regelungen getroffen worden, nach denen die Meldebehörden dem Rentendienst der Deutschen Bundespost Sterbefälle mitteilen. Die Mitteilungen an den Rentendienst gehen jedoch oft erst dann ein, wenn bereits mindestens eine Rente zuviel überwiesen wurde. Bei der Landesversicherungsanstalt Hamburg (LVA) macht dies nach unseren Informationen mehrere tausend Fälle jährlich aus. Wenn der Rentendienst eine solche Todesfallmitteilung erhalten hat, fordert er die überzahlten Beträge vom kontoführenden Kreditinstitut zurück und teilt dies dem Rentenversicherungsträger mit, der selber nicht tätig werden muß. Das Kreditinstitut muß die überzahlten Beträge grundsätzlich zurücküberweisen.

Die Rückzahlungsverpflichtung des Kreditinstituts entfällt jedoch, wenn über die überzahlten Beträge zwischenzeitlich bereits anderweitig verfügt wurde, wie dies durch Erben oder Bevollmächtigte geschehen kann. In diesen Fällen ist der Rentenversicherungsträger verpflichtet, die Überzahlung zurückzufordern. Da die Rentenversicherungsträger aber zunächst nicht wissen, wem gegenüber sie diese Forderung geltend machen können, fragen sie in solchen Fällen bei der Krankenkasse an, wer der Empfänger des Sterbegeldes ist. Dieser ist zwar in seiner Eigenschaft als Sterbegeldempfänger lediglich zufällig identisch mit demjenigen, der über die überzahlten Beträge verfügt hat. Nach den Erfahrungen der LVA führt der Weg einer Rückfrage beim Sterbegeldempfänger jedoch in einer Vielzahl von Fällen zum Erfolg. Anfragen bei anderen Stellen, wie z.B. dem Nachlaßgericht, haben wesentlich seltener Erfolg.

Die entsprechende Auskunft durch die Krankenkasse ist zum einen bereits dadurch problematisch, daß sie unter Änderung des ursprünglichen Erhebungszweckes im Interesse des Offenbarungsempfängers erfolgt. Für solche Fälle besteht keine ausdrückliche gesetzliche Regelung. Grundvoraussetzung für eine Offenbarung durch die Krankenkasse ist zudem, daß die Offenbarung erforderlich sein muß. Daran bestehen bei den beschriebenen Fällen jedoch erhebliche Zweifel, weil primär das Kreditinstitut über die relevante Information verfügt, nämlich über die Kenntnis, wer tatsächlich über die Beträge verfügt hat bzw. wer insoweit, insbesondere durch Kontovollmacht, verfügungsberechtigt war. Die Banken berufen sich jedoch in aller Regel auf das Bankgeheimnis. Damit entsteht die Situation, daß das gesetzlich geregelte Sozialgeheimnis gebrochen werden muß, weil das vertragliche Bankgeheimnis gewahrt bleiben soll. Als Folge davon werden Daten anstatt bei der zuvörderst zur Auskunft berufenen Stelle (Kreditinstitut) regelhaft bei Dritten (Sozialleistungsträgern) erhoben, bzw. bei Vierten, da das Kreditinstitut bereits Dritter ist.

Eine denkbare Lösung dieses Problems wäre, den Antrag auf unbare Rentenzahlung für die hier in Rede stehenden Fälle um eine Schweigepflichtentbindungserklärung zu erweitern. Eine solche Schweigepflichtentbindungserklärung würde jedoch gegenüber Rechtsnachfolgern nicht wirken. Daher sollte

eine gesetzliche Lösung durch Änderung des § 118 Abs. 3 SGB-VI angestrebt werden. Eine solche gesetzliche Lösung könnte so aussehen, daß am Ende des Absatzes 3 ein neuer Satz 5 angefügt wird, der lautet: „Sofern nach Satz 3 eine Rücküberweisung nicht erfolgen kann, hat das Kreditinstitut der überweisenden Stelle oder dem Träger der Rentenversicherung mitzuteilen, wer über die zu Unrecht erbrachten Geldleistungen verfügt hat oder wer über das Konto verfügungsberechtigt ist; hierbei sind der vollständige Name und die Anschrift anzugeben".

Wir haben diese Problematik und unseren Lösungsvorschlag der Behörde für Arbeit, Gesundheit und Soziales mitgeteilt. Diese teilt im Ergebnis unsere Auffassung, daß die beschriebene Ergänzung des § 118 Abs. 3 SGB-VI angestrebt werden sollte. Sie will dies an das Bundesministerium für Arbeit und Sozialordnung mit dem Ziel einer entsprechenden Rechtsänderung herantragen.

6.7 Offenbarung des zweiten Arbeitgebers

Wenn Arbeitnehmer mehrere geringfügige Beschäftigungsverhältnisse ausüben, werden diese zusammengerechnet und bei Überschreitung der Geringfügigkeitsgrenze sozialversicherungspflichtig. In der Praxis verschweigen aber Arbeitnehmer ihrem Arbeitgeber häufig, daß sie noch einer weiteren geringfügigen Beschäftigung nachgehen. Da auch geringfügige Beschäftigungsverhältnisse der Einzugsstelle für den Gesamtsozialversicherungsbeitrag (Krankenkasse) und von dort weiter an die Datenstelle der Rentenversicherungsträger zu melden sind, informiert die Datenstelle dann die Einzugsstelle, damit diese weitere Überprüfungen vornehmen kann. Wenn die Krankenkasse nach Überprüfung zu dem Ergebnis kommt, daß eine Sozialversicherungspflicht besteht, macht sie die Sozialversicherungsbeiträge anteilig bei dem jeweiligen Arbeitgeber geltend. Dabei handelt es sich um einen Verwaltungsakt.

Zu der Frage, ob bei der Begründung dieses Verwaltungsakts auch angegeben werden muß, bei welchem anderen Arbeitgeber der Arbeitnehmer noch beschäftigt war bzw. ist oder ob dies aus Datenschutzgründen unzulässig ist, sind uns zwei gegensätzliche gerichtliche Entscheidungen bekannt. Das Sozialgericht Gießen hat die Auffassung vertreten, die Angabe des zweiten Arbeitgebers würde dessen berechtigte Geheimhaltungsinteressen verletzen, der erste Arbeitgeber habe dadurch auch keine Vorteile und im übrigen könne der Arbeitgeber seinen Arbeitnehmer dazu befragen. Das Sozialgericht Münster hat entschieden, diese Angabe sei selbstverständlich erforderlich, um den Verwaltungsakt substantiell zu begründen und damit für den zur Zahlung herangezogenen Arbeitgeber nachvollziehbar zu machen.

Wir sind der Auffassung und haben dies der AOK-Hamburg mitgeteilt, daß zur substantiellen Begründung des Verwaltungsaktes auch die Angabe gehört, bei welchem weiteren Arbeitgeber der Arbeitnehmer beschäftigt war und in welchen Zeiträumen er bei beiden beschäftigt war (Überschneidungszeiträume). Nur so wird für den betroffenen Arbeitgeber transparent, weshalb er die nachgeforderten Beträge zahlen muß. Mit rechtsstaatlichen Grundsätzen wäre es nicht zu vereinbaren, wenn der Arbeitgeber allein darauf vertrauen müßte, daß die Krankenkasse „schon alles richtig gemacht" hat. Schließlich würde auch kein Falschparker ein Verwarnungsgeld zahlen, wenn ihm nicht mitgeteilt wird, wann und wo er falsch geparkt haben soll.

6.8 Unzulässige Datenerhebung der Sozialämter

6.8.1 Ehegatten Unterhaltspflichtiger

Wir hatten im 11. TB (6.10) kritisiert, daß die Sozialämter in Fragebögen zur Prüfung der Einkommens- und Vermögensverhältnisse Unterhaltspflichtiger behaupten, die Auskunftspflicht nach § 116 BSHG beziehe sich auch auf die Einkommens- und Vermögensverhältnisse der Ehegatten der Unterhaltspflichtigen. Der Senat hatte in seiner Stellungnahme zum Tätigkeitsbericht unsere Kritik zurückgewiesen. Die Praxis der Sozialämter sei rechtmäßig, weil eine gesetzliche Auskunftspflicht bestehe.

Im Januar 1993 ist zu dieser Frage ein Urteil des Bundesverwaltungsgerichts ergangen, in dem ausdrücklich klargestellt wird, daß die Auskunftspflicht aus § 116 BSHG sich nicht auf Ehegatten und andere Angehörige des Unterhaltspflichtigen erstreckt. Wir haben die Behörde für Arbeit, Gesundheit und Soziales entsprechend informiert. Sie hat uns daraufhin mitgeteilt, daß in dem Vordruck, in dem bislang unzutreffend auf eine Auskunftspflicht hingewiesen wurde, künftig ausdrücklich auf die Freiwilligkeit der entsprechenden Angaben hingewiesen wird. Damit verbunden wird ein Hinweis, daß diese Angaben im Interesse des Unterhaltspflichtigen lägen, weil sie Einfluß auf die Beurteilung seiner Unterhaltsfähigkeit haben. Es bleibt abzuwarten, ob dieser im Prinzip richtige Hinweis von den Betroffenen richtig verstanden wird. Erforderlichenfalls wird er redaktionell überarbeitet werden müssen.

6.8.2 Personalien von Untermietern

Ein Beispiel dafür, wie man Sozialhilfeempfänger geradezu für ihre Ehrlichkeit bestraft, wurde uns aus dem Bezirksamt Eimsbüttel bekannt. Ein sozialhilfebedürftiger Bürger hatte dort wahrheitsgemäß angegeben, daß er ein Zimmer seiner Drei-Zimmer-Wohnung an einen Studenten untervermietet hatte. Er legte sogar freiwillig eine Kopie des Untermietvertrages vor, um die Höhe der Einnahmen nachzuweisen. Allerdings hatte er in der Kopie vernünftigerweise die Personalien des Untermieters unkenntlich gemacht, um von vorneherein zu verhindern, daß sich das Sozialamt aus irgendwelchen Gründen an den Untermieter wendet und damit die Sozialhilfebedürftigkeit des Vermieters offenbart. Das führte dazu, daß ihm zwar laufende Hilfe zum Lebensunterhalt gewährt wurde. Der durch seine eigenen Mietkosten begründete weitere Bedarf wurde ihm aber mit der Begründung verweigert, diese Leistung würde erst gewährt werden, wenn er die Personalien des Untermieters angibt.

Tragfähige Gründe für das Verlangen des Sozialamtes nach Kenntnis der Personalien des Untermieters gab es nach unserer Auffassung nicht; die Befugnisse zur Amtsermittlung nach §§ 20, 21 Sozialgesetzbuch/Zehntes Buch (SGB-X) wurden überschritten. Zum einen ist diese Amtsermittlung auf den Leistungsfall zu beschränken. Die Personalien des Untermieters können also nicht mit der Begründung verlangt werden, man wolle prüfen, ob auch dieser Sozialhilfe bezieht und dabei alle Angaben wahrheitsgemäß gemacht hat.

Im übrigen kann man zwar mutmaßen, daß möglicherweise eine eheähnliche Gemeinschaft im Sinne des § 122 Bundessozialhilfegesetz (BSHG) zwischen Mieter und Untermieter bestehen könnte. Gegen eine solche Annahme sprach aber ersichtlich der Umstand, daß der Leistungsempfänger die Einnahmen aus dem Untermietverhältnis freiwillig angegeben hatte, obwohl sie sich auf seinen Hilfeanspruch nur mindernd auswirken konnten. Außerdem ist für die Richtigkeit einer solchen Mutmaßung der Name des Untermieters unerheblich.

Leider wollte der Betroffene keine weitere Unterstützung durch uns. Er hatte möglicherweise Sorge, daß diese Aufklärung zu noch weiteren Schritten gegen ihn führen könnte.

6.9 Rechnernetz des Landesbetriebs Pflegen & Wohnen

Im Rahmen der Einführung eines kaufmännischen Rechnungswesens, bei dem u.a. sehr sensible personenbezogene Daten über Bewohner von Heimen und Wohnunterkünften verarbeitet werden sollen, wird nunmehr auch die Vernetzung des Landesbetriebs Pflegen & Wohnen vorangetrieben. Vernetzt werden sämtliche Heime, die Wohnunterkünfte sowie die Zentrale des Landesbetriebs. Die Besonderheit der Vernetzung besteht darin, daß die Rechnerkopplung im Unterschied zu den meisten anderen Verwaltungsnetzen nicht nur über Standleitungen des LIT und der TELEKOM realisiert wird, sondern auch über Wählverbindungen im Rahmen von digitalen Nebenstellenanlagen.

Bei einer auf Wählverbindungen basierenden Rechnervernetzung besteht grundsätzlich das Risiko, daß die Wählleitung von Hackern manipuliert wird, um personenbezogene Daten von einem unberechtigten Telefonanschluß abrufen zu können. Diesem Mißbrauchsrisiko ist der Landesbetrieb Pflegen & Wohnen dadurch begegnet, daß der Aufbau der Wählleitung grundsätzlich über Rückrufmodem erfolgt: Zunächst muß sich der Anrufende gegenüber dem Rückrufmodem durch Eingabe eines Paßwortes autorisieren. Nach erfolgreicher Prüfung bricht das Rückrufmodem die Verbindung zum Anrufenden ab und baut die Verbindung über eine fest gespeicherte Anschlußnummer wieder selbständig auf. Die Leitung bleibt nur dann endgültig bestehen, wenn sich der dann Angerufene nochmals mittels Paßwort autorisiert. Die beim Rückruf anzurufende Anschlußnummer kann nicht über den Übertragungsanschluß manipuliert werden.

Eine nähere Prüfung bei Inbetriebnahme des Systems behalten wir uns vor. Wegen der zögerlichen Beteiligung durch den Landesbetrieb erhielten wir bisher die jeweiligen Unterlagen leider nur verspätet.

7. Personalwesen

7.1 Projekt Personalwesen (PROPERS)

Im 11. TB (7.1) hatten wir darüber berichtet, daß im Rahmen des Automationsvorhabens Personalwesen eine verteilte Datenverarbeitung entwickelt wird. Dazu soll ein seit Jahren auf dem Markt befindliches Software-Produkt verwendet werden; es sollen die in der hamburgischen Verwaltung eingesetzten arbeitsplatzunterstützenden Bürofunktionalitäten einbezogen werden.

Diesen Aspekt der behördenweiten Vernetzung haben wir auch im IuK-Datenschutzbericht vom 9. Juli 1993 aufgegriffen. Bislang besteht eine organisatorische und technische Trennung zwischen den Personaldaten, die im Rahmen der Bezügeabrechnung und des Beihilfeverfahrens von der Besoldungs- und Versorgungsstelle auf den Großrechnern im Landesamt für Informationstechnik (LIT) verarbeitet werden, und denen, die darüber hinaus von den einzelnen Behörden über ihre eigenen Beschäftigten verwaltet werden. Durch die angestrebte Automatisierung (Zentral- und Abteilungsrechnerlösung) wird diese örtliche Trennung zumindest technisch aufgehoben: Es bestehen dann für die Verarbeitung von Beschäftigtendaten direkte Leitungsverbindungen zwischen den Abteilungsrechnern der Behörden und den Großrechnern des LIT. Um zu verhindern, daß von Bildschirmarbeitsplätzen anderer Behörden auf Personaldaten zugegriffen werden kann, die nicht für deren eigene Aufgabenbereiche bestimmt sind, müssen umfassende Sicherheitsvorkehrungen getroffen werden.

Die entsprechenden Planungen des Projektes Personalwesen, an denen wir weiterhin umfassend beteiligt werden, gehen deshalb auch nicht von einer Online-Verbindung zwischen den Behörden und dem LIT aus. Vielmehr werden die abrechnungsrelevanten Daten auf den Rechnern der Behörden jeweils gezielt für einen Datentransfer bereitgestellt und abgesetzt auf den Zentralrechner im LIT übertragen. Nach den Abrechnungsterminen werden die Lohnkonten auf die Behördenrechner zurückübertragen. Jede Behörde erhält dadurch technisch nur den Zugriff auf die Daten ihrer Beschäftigten.

Hinsichtlich der vorgesehenen Standardsoftware werden mit dem Hersteller noch abschließende Verhandlungen über einzelne Verbesserungen und Erweiterungen des Produktes geführt. Inzwischen ist für eine Pilotanwendung in der Behörde für Schule, Jugend und Berufsbildung (BSJB) ein Abteilungsrechner installiert worden. In einer ersten Stufe wird eine Textverarbeitungsunterstützung zur Verfügung stehen. Dabei kann ein großer Teil der Vordrucke, die für die Aufgaben der Personalverwaltung wesentlich sind, in Form von Textbaustei-

nen genutzt werden. Die vorläufige Planung sieht danach die Erweiterung um die Stammdatenverwaltung und darauf aufbauend die Pilotierung der Bezügeabrechnung vor.

Daneben werden zur Zeit in einem Teilprojekt in der BSJB in Zusammenarbeit mit dem Projekt Personalwesen die behördenspezifischen Anforderungen an die Personalplanung erhoben. Auf dieser Grundlage wird eine Bewertung von geeigneten Softwareprodukten für den Bereich der Personalplanung erfolgen. Zum Redaktionsschluß erreichte uns der Zwischenbericht der Lenkungsgruppe (Stand Oktober 1993), der den aktuellen Stand der Planung und Erprobung zusammenfaßt.

7.2 Neues Personalaktenrecht

7.2.1 Änderung des Hamburgischen Beamtengesetzes

Zu dem Entwurf eines Zweiten Gesetzes zur Änderung dienstrechtlicher Vorschriften haben wir bereits im 11. TB (7.2) ausführlich Stellung bezogen. Der Entwurf ist inzwischen mehrmals überarbeitet worden. Aus datenschutzrechtlicher Sicht ist jedoch kein neuer Handlungsbedarf entstanden.

Nachdem der Senat den Entwurf der Bürgerschaft zugeleitet hat, ist mit der Verabschiedung des Gesetzes bald zu rechnen. Wie schon im 11. TB (7.2) hervorgehoben, wird es nach Inkrafttreten des Gesetzes insbesondere einer grundsätzlichen Neufassung der Anordnung zur Führung und Verwaltung von Personalakten bedürfen.

7.2.2 Änderungen in § 28 Hamburgisches Datenschutzgesetz

Im Zuge der Diskussion um die Novellierung des Hamburgischen Datenschutzgesetzes haben wir nach einem Meinungsaustausch mit der federführenden Justizbehörde und dem Senatsamt für den Verwaltungsdienst den Entwurf eines neuen § 28 HmbDSG vorgelegt, der die Datenverarbeitung bei Beschäftigungsverhältnissen regelt.

Wir stimmen mit den genannten Behörden überein, daß die neuen beamtenrechtlichen Vorschriften über das Personalaktenrecht (vgl. oben 7.2.1) für alle Beschäftigungsverhältnisse und damit auch für die Arbeiter und Angestellten im hamburgischen öffentlichen Dienst gelten sollen. Deshalb soll eine entsprechende Verweisung in den neuen § 28 HmbDSG aufgenommen werden.

Außerdem haben wir vorgeschlagen, daß bei medizinischen oder psychologischen Untersuchungen „möglichst tätigkeitsbezogene Risikofaktoren" (vgl. unten 7.3) mitgeteilt werden, soweit sich medizinische oder psychologische Bedenken ergeben. Ergeben sich keine Bedenken, soll nach unserem Vorschlag nur das Ergebnis der Untersuchung ohne weitere Zusätze übermittelt werden. Letzteres entspricht im übrigen bereits der Praxis beim Personalärztlichen Dienst (vgl. 7.3).

7.2.3 Recht auf eigene Darstellung

Die neuen personalaktenrechtlichen Vorschriften bestätigen das Recht des Betroffenen auf eigene Darstellung (vgl. 1.3), das in diesem Bereich bereits besteht.

Gemäß § 96 Hamburgisches Beamtengesetz (HmbBG) in der geltenden Fassung ist der Beamte über Beschwerden und Behauptungen tatsächlicher Art, die für ihn ungünstig oder nachteilig werden können, vor deren Aufnahme in die Personalakte zu hören. Die Äußerung des Beamten ist zu seiner Personalakte zu nehmen. Eine nahezu identische Regelung enthält der Entwurf des neuen § 96 c HmbBG. Darüber hinaus sieht der Entwurf von § 96 c HmbBG für den Betroffenen genau wie § 90 b Bundesbeamtengesetz (BBG) ein Recht auf eigene Darstellung auch bei nachteiligen oder ungünstigen Bewertungen vor.

Hervorzuheben ist in diesem Zusammenhang, daß es auf die Richtigkeit der Darstellung des Betroffenen in keinem Fall ankommt. Die Gesetzesbegründung zu § 90 b BBG betont im Gegenteil, daß bei Zweifeln über die Richtigkeit oder Begründetheit der Beschwerden oder Behauptungen diese nicht zur Personalakte zu nehmen sind. Damit geht der Gesetzgeber grundsätzlich davon aus, daß die zur Personalakte genommenen Beschwerden und Behauptungen zutreffen (müssen). In diesem Fall bezieht sich demnach das Recht zur Gegenäußerung auf voraussichtlich richtige, aber für den Betroffenen nachteilige Darstellungen und Bewertungen. Zweck des Gegenäußerungsrechts ist es, daß der Beamte die Angaben, die zur Personalakte genommen werden, vorsorglich mit seiner abweichenden Sachdarstellung versehen kann. Er kann damit dem Risiko vorbeugen, daß gerade auch bei komplexen Sachverhalten aus einer Darstellung negative Schlußfolgerungen gezogen werden.

Das Bundesarbeitsgericht geht für Angestellte davon aus, daß bis zur ordnungsgemäßen Anhörung des Bediensteten mit der Möglichkeit zur Gegenäußerung das fragliche Schriftstück aus der Personalakte zu entnehmen ist. Es kann dann nach Würdigung des Vorbringens des Angestellten ggf. wieder zur Personalakte genommen werden (BAG NJW 1990, 1933). Die Schutzfunktion wird dadurch für den Betroffenen noch verstärkt. Bei schuldhafter Verletzung der Anhörungspflicht hat der Dienstherr wegen Amtspflichtverletzung dem Beamten Schadensersatz zu leisten (BVerfGE 15,3,14).

Das Recht auf eigene Darstellung ist demnach im öffentlichen Dienstrecht am weitesten entwickelt. Als Teil des Persönlichkeitsrechts ist hier das Recht zur Äußerung des Betroffenen hinsichtlich der eigenen Daten unabhängig von deren Richtigkeit oder Unrichtigkeit; außerdem ist die Pflicht der speichernden Stelle zur Aufbewahrung anerkannt.

7.3 Personalärztlicher Dienst (PÄD)

Im 10. und 11. TB (jeweils 7.3) hatten wir uns ausführlich mit dem PÄD befaßt. Wir haben die bislang strittigen Fragen mit dem PÄD nochmals erörtert. In allen Punkten konnte nunmehr Einvernehmen erzielt werden.

Die Probanden werden jetzt auf Wunsch in einem persönlichen Gespräch darüber aufgeklärt, was der Personaldienststelle mitgeteilt werden soll (vgl. 10. TB, 7.3). Nach herkömmlichem Verfahren werden bei auffälligen Befunden mit dem Probanden ohnehin Einzelgespräche geführt, gegebenenfalls mit dem Ratschlag, sich ärztlich behandeln zu lassen. Auch wird den Betroffenen jetzt ein Einsichtsrecht in ihre personalärztlichen Unterlagen gewährt (vgl. 11. TB, 7.3).

Einigkeit herrscht nunmehr auch in der Frage der Aufbewahrungsfrist (vgl. 10. TB, 7.3). Bei Bewerbern, mit denen ein Beschäftigungsverhältnis nicht zustande kommt, werden die Unterlagen grundsätzlich ein Jahr aufbewahrt (vgl. bereits 11. TB, 7.3), im übrigen grundsätzlich zehn Jahre.

Gesundheitliche Risikofaktoren (vgl. 11. TB, 7.3) werden nur mitgeteilt, wenn das Untersuchungsergebnis „gesundheitliche Bedenken" ergibt; bei dem Ergebnis „keine gesundheitlichen Bedenken" erfolgt die Mitteilung an die Personaldienststelle ohne weitere Zusätze. Gegen diese Verfahrensweise bestehen keine datenschutzrechtlichen Einwände. Die weitergehende Fragestellung, ob lediglich tätigkeitsbezogene Risikofaktoren oder auch darüber hinausgehende Risiken mitgeteilt werden (vgl. 11. TB, 7.3), ist letztlich nur auf gesetzlicher Ebene zu lösen (vgl. oben 7.2.2).

Entsprechend einer Anregung von uns verfügt der PÄD jetzt über ein eigenes Telefax-Gerät. Zuvor gingen Telefaxe für den PÄD im Amt für Allgemeine Verwaltung der Wirtschaftsbehörde ein.

Mehrere Eingaben haben wir schließlich zum Anlaß genommen, mit dem PÄD und den arbeitsmedizinischen Diensten die verschiedenen Anamnese-Fragebögen dieser Dienststellen zu erörtern. Die zu untersuchenden Personen sollen diese Fragen zu Vorerkrankungen und Krankheiten in der Familie zu Hause schriftlich beantworten und zur Untersuchung mitbringen.

Bei dem Gespräch ergab sich, daß Fragen nach Vorerkrankungen für eine Gesamtbeurteilung der gesundheitlichen Eignung grundsätzlich erforderlich sind. Die Antworten sind auch zu dokumentieren. Frühere Krankheiten sind dabei nicht automatisch Anlaß zu „gesundheitlichen Bedenken", sondern zunächst nur zu weiteren klärenden Fragen der Ärztin bzw. des Arztes. Die ausgefüllten Anamnesebögen unterliegen der ärztlichen Schweigepflicht und verbleiben beim ärztlichen Dienst.

Wir regten allerdings an, die Probanden besser über Aufgabe und Ziel der Untersuchung und des Anamnese-Bogens zu informieren und auf die Möglichkeit einer mündlichen Erörterung einzelner besonders sensibler Fragen hinzuweisen. Auch werden die ärztlichen Dienste die medizinische Erforderlichkeit und die Verständlichkeit der einzelnen Fragen noch einmal besonders überprüfen. Zum Redaktionsschluß erreichte uns ein neuer Anamnese-Bogen der PÄD, der die genannten Anregungen umsetzt und den datenschutzrechtlichen Anforderungen gerecht wird.

Wenn ein Proband bestimmte Fragen nicht beantworten will, sollte der ärztliche Dienst genau prüfen, ob die gutachterliche Stellungnahme nicht auch ohne eine Antwort auf diese Frage möglich ist. Dies wird auch von dem Auftrag und dem Zweck der Untersuchung abhängen. Immerhin wird ein Proband auch nicht speziell nach Drogenkonsum oder einer HIV-Infektion gefragt, obwohl eine Antwort hierauf für eine verantwortungsvolle medizinische Anamnese durchaus wichtig sein kann.

7.4 Bewerbungen aus den neuen Bundesländern

Im 11. TB (7.4) hatten wir uns mit dem Verfahren bei Bewerbungen aus den neuen Bundesländern auseinandergesetzt. Offen geblieben war die Frage, ob und inwieweit die Einstellungsbehörden Maßnahmen treffen können, die über Fragen nach Tätigkeiten für den Staatssicherheitsdienst und über gezielte Auskunftsersuchen bei dem Bundesbeauftragten für die personenbezogenen Unterlagen des Staatssicherheitsdienstes hinausgehen.

Die Behörde für Wissenschaft und Forschung (BWF) hat für hochschulrechtliche Berufungsverfahren einen Vordruck eingeführt, mit dem nach einer Mitarbeit beim Staatssicherheitsdienst der ehemaligen DDR gefragt wird. Hierbei handelt es sich nur um eine andere Form der Nachfrage, nicht jedoch um eine weitergehende Frage.

In der Justizbehörde wird zusätzlich eine Einverständniserklärung des Bewerbers eingeholt, die sich auf die Einholung von Auskünften bei der Zentralen Erfassungsstelle in Salzgitter bezieht. Praktische Verwendung findet diese Einverständniserklärung und die für die „Gauck-Behörde" fast ausschließlich im Strafvollzugsbereich, da in anderen Bereichen kaum Bewerbungen aus den neuen Bundesländern erfolgen. Beide Erklärungen werden erst verlangt, wenn der Einstellungstest bestanden wurde und ein Vorstellungsgespräch zur Einstellungsabsicht geführt hat. Außerdem wird nach leitenden Funktionen in ehemaligen DDR-Betrieben gefragt.

Die Einstellungsstelle der Landespolizeischule Hamburg fragt gegebenenfalls durch eine gesonderte „Erklärung zum Bewerbungsbogen" frühere Tätigkeiten in der Nationalen Volksarmee, in der SED und in sonstigen Massenorganisationen sowie für den Staatssicherheitsdienst näher ab. Die Erklärung schließt das Einverständnis mit Anfragen bei der „Gauck-Behörde" und der Zentralen Erfassungsstelle in Salzgitter ein.

Nach Abstimmung mit dem Senatsamt für den Verwaltungsdienst haben wir keine Bedenken gegen die Einholung der zusätzlichen Informationen in den beiden erwähnten sicherheitsrelevanten Behördenbereichen. Wir gehen davon aus, daß sich die Einholung der zusätzlichen Informationen auf diese Bereiche beschränkt, und daß im übrigen gemäß den Empfehlungen der Personalabteilungsleiterbesprechungen vom 21. Januar 1991 und vom 26. August 1991 verfahren wird.

7.5 Weitergabe von Personaldaten an Versicherungsgesellschaften

Im 11. TB (7.5) hatten wir angekündigt, uns näher mit Nebenbeschäftigungen von Mitarbeitern für Versicherungsunternehmen zu befassen. Es konnte nicht gänzlich ausgeschlossen werden, daß insbesondere Krankenversicherungen immer wieder aus der Verwaltung gezielte Hinweise etwa auf einzustellende Personen erhalten.

Auf unsere Veranlassung hatten die Personalabteilungsleiter bereits auf ihrer Sitzung vom 10. April 1984 die Behörden darauf hingewiesen, daß eine Kollision mit den dienstlichen Interessen und Aufgaben besteht, wenn Personalsachbearbeiter eine Nebentätigkeit etwa als Werber oder Vermittler im Zuständigkeitsbereich der Personalabteilung ausüben. Gemäß § 69 Abs. 2 HmbBG ist in diesen Fällen die Nebentätigkeit regelmäßig zu versagen.

Vor diesem Hintergrund haben wir im Berichtszeitraum die Personalabteilung einer großen Behörde geprüft. Keiner der dort Beschäftigten verfügte über eine Nebentätigkeitsgenehmigung für Tätigkeiten im Versicherungswesen.

Im Berichtszeitraum sind beim Hamburgischen Datenschutzbeauftragten keine weiteren Eingaben zu diesem Themenkomplex eingegangen. Sobald sich hieran etwas ändert, wird auf die Angelegenheit zurückzukommen sein.

7.6 Mitarbeiterdaten im Hamburg Handbuch

Auf unsere Anfrage hin hat uns das Senatsamt für den Verwaltungsdienst (SfV) mitgeteilt, daß die Herausgabe des nächsten Hamburg Handbuches für das Frühjahr 1994 vorgesehen ist.

Wie beim aktuellen Hamburg Handbuch soll auch künftig auf den Abdruck der Dienstbezeichnungen der Beschäftigten verzichtet werden. Allerdings soll das neue Handbuch im Gegensatz zur aktuellen Ausgabe die Vornamen der Beschäftigten enthalten.

Schon im 11. TB (7.6) hatten wir auf das Interesse von Mitarbeitern an der Geheimhaltung ihrer Vornamen und auf das Widerspruchsrecht (§ 16 Abs. 1 Satz 1 Nr. 4 HmbDSG) hingewiesen, das den Betroffenen gegebenenfalls zusteht. Die Betroffenen müssen über die geplante Veröffentlichung ihrer Vornamen im Hamburg Handbuch unter Hinweis auf das Widerspruchsrecht vorab informiert werden (§ 16 Abs. 1 Satz 2 HmbDSG). Nur unter diesen Voraussetzungen und soweit kein Widerspruch erfolgt, ist die Veröffentlichung zulässig.

Das SfV teilt diese Beurteilung nicht. Es hat nun in Aussicht genommen, aus Fürsorgegründen die Vornamen oder auch Nachnamen derjenigen Mitarbeiter nicht mehr im Hamburg Handbuch wiederzugeben, die ihre Vor- oder auch Nachnamen dort nicht genannt haben wollen. Die Behörden sollen in eigener Verantwortung einzelfallorientiert entscheiden, in welcher Form qualifizierten Gegenvorstellungen wegen der Veröffentlichung des Vornamens Rechnung getragen werden kann; sie sollen bei der Anforderung von Beiträgen für das Handbuch auf diese Verfahrensweise hingewiesen werden.

Aus datenschutzrechtlicher Sicht kommt es – unbeschadet der Frage der Fürsorgepflicht – auf die informationelle Selbstbestimmmung der Mitarbeiter an, die ihr Widerspruchsrecht wahrnehmen. Die Widersprüche sind daher unabhängig von der Entscheidung der Beschäftigungsbehörde zu berücksichtigen.

Es bleibt abzuwarten, ob im Ergebnis hier entsprechend verfahren wird, da nach dem Entwurf der Durchführungsbestimmungen zur Telekommunikations-Richtlinie (siehe 3.5) eine Veröffentlichung schon dann unterbleibt, wenn Risiken für die Mitarbeiter nicht ausgeschlossen werden können. Auf die Angaben der Mitarbeiter kommt es daher in jedem Fall maßgeblich an.

7.7 Verwendung der Beschäftigtendaten der Besoldungs- und Versorgungsstelle (BVSt) für Rundschreiben

Bei der Versendung von verwaltungsinternen Rundschreiben an die Beschäftigten wird regelmäßig auf die Datenbestände der BVSt zurückgegriffen, die auch sonst bei Schreiben an die Mitarbeiter – zum Beispiel für Besoldungsmitteilungen und Beihilfebescheide – Verwendung finden. Im Anschluß an das Jahresrundschreiben 1992 des Ersten Bürgermeisters wurde in Presseberichten die Frage aufgeworfen, inwieweit die Nennung der Privatadresse bei diesen (Rund-)Schreiben die Mitarbeiter gefährde, die in sicherheitsempfindlichen Bereichen tätig sind und deren Privatadresse der Geheimhaltung unterliegt.

Auf unsere Anfrage hin hat uns das Senatsamt für den Verwaltungsdienst mitgeteilt, daß Beschäftigte in sicherheitsempfindlichen Bereichen diese Mitteilungen bereits seit Jahrzehnten in geschützter Form erhalten. Name und Anschrift werden durch Sternchendruck ersetzt. Lediglich die für die Zustellung erforderlichen Merkmale Personalkennziffer, Kapitel- und UT-Nummer sind vermerkt. Bei dieser Sachlage haben wir keine datenschutzrechtlichen Bedenken gegen die Versendung von Rundschreiben unter Verwendung der vorhandenen Adressenbestände.

Zuletzt erreichte uns eine Anfrage des Senatsamtes für den Verwaltungsdienst, die eine Einladung zu einer UNICEF-Veranstaltung der Hamburger Hochschulen zum Gegenstand hatte. Die Einladung sollte an die bei den Hamburger Hochschulen Beschäftigten versandt werden. Bedenken hiergegen haben wir nicht erhoben.

7.8 Personaldatenverarbeitung bei den Personalräten

Im Berichtszeitraum sind hier zahlreiche Anfragen von Personalräten eingegangen, welche die Datenverarbeitung bei den Personalvertretungen zum Gegenstand hatten. Unsicherheit herrscht insbesondere in der Frage, ob und inwieweit die Personalräte unabhängig von einer Beteiligung im Einzelfall (Mitbestimmung, Mitwirkung, Anhörung oder Stellungnahme) einen sogenannten Stammdatensatz verarbeiten dürfen. Dabei wurde deutlich, daß die Personalräte regelmäßig die Auffassung vertreten, sie benötigten einen solchen Stamm-

datensatz, um ihre allgemeinen Aufgaben gemäß § 78 Hamburgisches Personalvertretungsgesetz (HmbPersVG) erfüllen zu können. Wir können dieses Argument nachvollziehen.

Um diese Frage und insbesondere den Umfang eines solchen Stammdatensatzes zu klären, haben wir uns an das Senatsamt für den Verwaltungsdienst (SfV) gewandt. Als Diskussionsgrundlage haben wir einen Stammdatensatz mit folgenden Daten vorgeschlagen:

— Name, Vorname

— Geburtsjahr

— Hinweis auf Ausbildung (z. B. Volkswirt, Krankenschwester)

— Eintritt in den Vorbereitungsdienst

— Ernennungsdaten

— Abteilungs-/Dezernatszugehörigkeit

— Beurlaubung (von–bis)

— Ermäßigung der Arbeitszeit (von–bis)

Zusätzlich bei allen Arbeitnehmern:

— Datum der letzten Eingruppierung

— Vergütungs- oder Lohngruppe und Fallgruppe

— feste Zulagen

Das SfV hat uns bestätigt, daß gegen eine regelmäßige Weitergabe dieser Daten an den Personalrat in Listenform keine Bedenken bestehen. Dies könnte bei der Novellierung des HmbPersVG gesetzlich geregelt werden.

Noch nicht abschließend geklärt ist die Frage, ob die Personalräte diese in Listenform erhaltenen Daten auch automatisiert verarbeiten dürfen. Das SfV hat insoweit noch Bedenken. Wir sehen datenschutzrechtlich keine Bedenken gegen eine gesetzliche Regelung, daß der Personalrat die regelmäßig erhaltenen Personaldaten auch automatisiert verarbeiten darf.

Solange es eine solche Regelung zur automatisierten Verarbeitung der Stammdaten nicht gibt, sollte davon ausgegangen werden, daß die Personalräte, die über einen dienstlichen PC verfügen, diesen von der Dienststelle zulässigerweise erhalten haben und ihn daher auch für die Verarbeitung der Stammdaten verwenden dürfen. Der Personalrat hätte dabei die gesetzlich vorgesehenen Sicherungsmaßnahmen (§ 8 Abs. 2 HmbDSG) einzuhalten.

Voraussetzung für die automatisierte Verarbeitung der Stammdaten ist selbstverständlich, daß der Personalrat über einen dienstlichen PC überhaupt verfügt. Allein die regelmäßige Unterrichtung des Personalrates mit Personaldaten sollte nicht dazu führen, daß der Personalrat einen PC erhält, um diese Daten

zu verarbeiten. Insoweit ist jeweils im Einzelfall unter Berücksichtigung von § 46 Abs. 3 HmbPersVG zu entscheiden.

Wir haben das SfV hinsichtlich der automatisierten Verarbeitung der Stammdaten um eine ergänzende Stellungnahme gebeten.

7.9 Beihilfe

Im 10. TB (7.5.2) hatten wir uns mit dem Beihilfeverfahren für Angehörige von Bediensteten beschäftigt. Das Beihilferecht sieht vor, daß die Angehörigen ihre Aufwendungen in der Weise zurückerstattet bekommen, daß die Bediensteten einen entsprechenden Antrag auf Beihilfe stellen. Insbesondere bei Beziehungsstörungen innerhalb der Familie ist dieses mit Nachteilen für die Angehörigen verbunden.

In einer Entschließung zum Datenschutz im Recht des öffentlichen Dienstes forderten die Datenschutzbeauftragten des Bundes und der Länder im September 1991 die gesetzliche Festlegung eines eigenen Beihilfeanspruchs der Angehörigen. Diese Forderung konnte nicht durchgesetzt werden.

Im Anschluß an eine erneute Eingabe in dieser Angelegenheit hat uns das Senatsamt für den Verwaltungsdienst mitgeteilt, daß den datenschutzrechtlichen Anliegen der Angehörigen im Rahmen des geltenden Rechts Rechnung getragen wird. In der Mehrzahl der Fälle würden die Anträge in Vollmacht des Berechtigten (Bediensteten) gestellt; im übrigen könnten die Angehörigen ihre Belege auch direkt einreichen und würden sie dann unmittelbar zurückerhalten (vgl. auch Bürgerschaftsdrucksache 14/4003, A., Stellungnahme des Senats zum Ersuchen der Bürgerschaft vom 27./28. Januar 1993 – Verfahrensverbesserungen bei der Beihilfe für Angehörige –).

Der Hamburgische Datenschutzbeauftragte begrüßt die flexible Handhabung des Problems durch das Senatsamt für den Verwaltungsdienst und hält weitere Bemühungen jedenfalls auf gesetzlicher Ebene bei diesem Sachstand für entbehrlich.

7.10 Bewerberdaten bei der Polizei

Im Berichtszeitraum haben wir uns mit dem Bewerbungsverfahren bei der Landespolizeischule beschäftigt.

Die Einstellungsstelle der Landespolizeischule unterhält eine – manuell geführte – Kartei über abgelehnte Bewerber. Auf den einzelnen Karteikarten sind Stammdaten über die abgelehnten Bewerber vermerkt. Hierbei handelt es sich um Name, Vorname, Geburtsdatum und -ort, Schulbildung, Beruf, Privatanschrift einschließlich Telefon, Gründe bei sofortiger Ablehnung, abgeleistete Prüfungen (Datum, bestanden, nicht bestanden, Wiederholung), ärztliche Untersuchung (Datum, tauglich, nicht tauglich) sowie um ein weiteres Feld „Bemerkungen". In diesem Feld werden insbesondere gesundheitliche Daten

verarbeitet, welche die Ablehnung eines Bewerbers begründen. Es existieren ca. 10.000 solcher Karteikarten, die grundsätzlich bis zu dem Zeitpunkt aufbewahrt werden, an dem der Betroffene schon aus Altersgründen für den Polizeidienst nicht mehr in Betracht kommt.

Über diese Karteikarten hinaus verbleiben bei der Polizei keine weiteren Unterlagen mit personenbezogenen Daten der abgelehnten Bewerber. Die Unterlagen werden vielmehr nach Ablauf der Rechtsmittelfristen vernichtet, an den Bewerber zurückgeschickt oder aber für statistische Zwecke anonymisiert.

Zur Begründung für die Karteikartensammlung führte die Polizei aus, daß ca. 25 % Wiederholungsbewerber zu verzeichnen seien, die dann gegebenenfalls ohne weitere Veranlassungen (erneute ärztliche Untersuchung usw.) negativ beschieden werden können. Außerdem versehe die Einstellungsstelle viele Karteikarten über zunächst abgelehnte Bewerber mit einer Wiedervorlagefrist, um die Betroffenen im Hinblick auf eine erneute Bewerbung gezielt anschreiben zu können. Viele Ablehnungen seien mit Verabredungen mit dem Betroffenen verbunden, geeignete Maßnahmen zur Beseitigung der Ablehnungsgründe zu treffen. Gerade bei Bewerbern mit positiver Prognose hinsichtlich ihrer Polizeidiensttauglichkeit bestehe ein dienstliches Interesse, den Kontakt aufrechtzuerhalten.

An der Rechtmäßigkeit der Karteikartensammlung bestehen zwar erhebliche Zweifel (§ 28 Abs. 5 Satz 1 HmbDSG). Auf der anderen Seite darf nicht verkannt werden, daß das Bewerbungsverfahren bei der Polizei sich durch Besonderheiten auszeichnet. So sind die gesundheitlichen Voraussetzungen in der PDV 300 (Ärztliche Beurteilung der Polizeidiensttauglichkeit und der Polizeidienstfähigkeit) präzise und umfassend geregelt. Sonst geeignete Bewerber können aus behebbaren Gründen zunächst scheitern. Auch muß berücksichtigt werden, daß ein berechtigtes öffentliches Interesse an einer möglichst optimalen Personalauswahl bei der Polizei besteht. Nach unserem Eindruck ist es fraglich, ob die Einstellungsstelle auch dann eine optimale Personalauswahl gewährleisten könnte, wenn sie im wesentlichen allein auf die eingehenden Bewerbungen zurückgreifen könnte. Insoweit unterscheidet sich die Situation bei der Polizei von der bei anderen Behörden. Dies gilt auch für die hohe Quote von Wiederholungsbewerbern.

Vor diesem Hintergrund haben wir das Anliegen der Polizei, Stammdaten abgelehnter Bewerber über einen längeren Zeitraum zu speichern, im Grundsatz als berechtigt nachvollziehen können. Wir haben deshalb bei der Novellierung des § 28 HmbDSG (vgl. 7.2.2) die Einfügung einer Regelung vorgeschlagen, wonach bei überwiegenden berechtigten Interessen der speichernden Stelle eine längere Verarbeitung der Daten abgelehnter Bewerber möglich ist.

Bei den Stammdaten im einzelnen bedürfen vor allem die Gesundheitsdaten der Klärung. Die Behörde für Inneres verfügt über einen eigenen Ärztlichen Dienst. Uns ist daran gelegen, daß das Verfahren bei der Polizei den Grundsätzen entspricht, die nunmehr für den Personalärztlichen Dienst (vgl. 7.3) gelten. Danach dürfen lediglich bei der Untersuchung festgestellte Risikofaktoren, nicht jedoch Befunde mitgeteilt werden.

Im übrigen haben wir zum Datenfeld „Bemerkungen" Einvernehmen dahingehend erzielt, daß dort nur noch Feststellungen tatsächlicher Art (etwa mehrmaliges unentschuldigtes Nichterscheinen zu vereinbarten Terminen) eingetragen werden, soweit sie bei erneuter Bewerbung zu einer sofortigen Ablehnung führen.

7.11 Personalentwicklungskonzept

Im Rahmen der Umsetzung des Personalentwicklungskonzepts sind unter anderem Mitarbeiter- und Vorgesetztengespräche geplant, die in regelmäßigen Abständen stattfinden sollen. In diesem Zusammenhang hat uns das Senatsamt für den Verwaltungsdienst den Entwurf eines Gesprächsleitfadens mit der Bitte um Stellungnahme übersandt.

Im Grundsatz haben wir uns auf den Standpunkt gestellt, daß nach heutigem Verständnis derartige Mitarbeiter- und Vorgesetztengespräche für Personalentwicklungszwecke durchaus „erforderlich" sind. Soweit im Rahmen dieser Gespräche die Verarbeitung von personenbezogenen Daten erforderlich ist, ist diese Verarbeitung gemäß § 28 HmbDSG zulässig.

Im einzelnen haben wir betont, daß die Freiwilligkeit der Mitarbeitergespräche deutlich zum Ausdruck kommen muß. Klärungsbedürftig erscheint, inwieweit die vorgesehenen schriftlichen „Zielvereinbarungen" der Personalakte zuzuordnen sind. In jedem Fall besteht nach dem neuen Dienstrecht (vgl. oben 7.2.1) ein Akteneinsichtsrecht der Betroffenen. Die vorgesehene Vernichtung von vorangegangenen Zielvereinbarungen nach jedem stattgefundenen Gespräch kann so überprüft werden. Überdies sollten die Zielvereinbarungen nicht automatisiert verarbeitet werden dürfen.

Schließlich wäre zu klären, ob ein Mitbestimmungsfall gemäß § 86 HmbPersVG vorliegt. Bei Nichtbeachtung von bestehenden Mitbestimmungsrechten des Personalrates wäre eine Datenverarbeitung grundsätzlich unzulässig, weil sie unbefugt erfolgen würde.

7.12 Bewerbungs- und Prüfungsverfahren für MTA-Schüler

Im Anschluß an die Diskussion um ein Attest zum Nachweis der Ausbildungs- und Berufstauglichkeit von MTA-Schülern (siehe 11. TB, 7.8) haben wir das Bewerbungs- und Prüfungsverfahren insgesamt datenschutzrechtlich geprüft. Während die Ausbildung im AK St. Georg erfolgt, wird die staatliche Abschlußprüfung von der Behörde für Arbeit, Gesundheit und Soziales (BAGS) unmittelbar durchgeführt, die auch die Berufsausübungserlaubnis erteilt. Bei beiden Stellen sind nach dem Ergebnis der Prüfung einzelne Punkte verbesserungs- oder zumindest klärungsbedürftig. Für ein automatisiertes Verfahren in der BAGS ist zudem bislang keine Dateimeldung erfolgt.

Klärungsbedürftig sind im wesentlichen die Aufbewahrungsfristen für die verschiedenen anfallenden Unterlagen, wozu Schülerbögen, Lehrgangskarteien, Lehrgangsakten und Berufserlaubnisurkunden gehören. In der Ausbildungs- und Prüfungsordnung sind lediglich für Prüfungsunterlagen Aufbewahrungsfristen vorgesehen. Verbesserungsbedürftig ist die Häufigkeit der ärztlichen Untersuchungen. Bislang müssen sich die Schüler vor Erlangung der Berufsbezeichnung grundsätzlich dreimal ärztlich untersuchen lassen, und zwar zweimal vor Ausbildungsbeginn und ein weiteres Mal vor der Lehrgangsprüfung. Eine einmalige Untersuchung vor Beginn der Ausbildung wäre nach unserer Auffassung jedoch künftig ausreichend, da das MTA-Gesetz keine weiteren Untersuchungen vorsieht.

Unsere Bedenken haben wir im einzelnen dem AK St. Georg und der BAGS dargestellt. Das AK St. Georg ist unserem Vorschlag, eine der ärztlichen Untersuchungen wegfallen zu lassen, bislang nicht gefolgt; die Diskussion dauert aber an. Unbeantwortet ist hier noch die Frage nach den Aufbewahrungsfristen. Die von der BAGS erbetene Dateimeldung ist uns noch nicht zugegangen. Ungeklärt ist dort sowohl die Frage nach dem Wegfall der ärztlichen Untersuchung als auch die Frage der Aufbewahrungsfristen.

7.13 Weitergabe personalärztlicher Stellungnahmen in der Justizbehörde

Durch eine Eingabe wurden wir auf ein nicht datenschutzgerechtes Verfahren in der Justizbehörde aufmerksam. Wenn dort ein Mitarbeiter aus gesundheitlichen Gründen einen Antrag auf Beschaffung besonderer Büroausstattung (z. B. ein besserer Stuhl wegen Rückenbeschwerden) stellt, richtet er diesen an das Personalreferat (A 12). Dieses übersendet den Antrag in Kopie an den Personalärztlichen Dienst (PÄD) mit der Bitte um gutachtliche Äußerung. Der PÄD wiederum übersendet nach erfolgter Untersuchung seine gutachtliche Äußerung an A 12. Die Beschaffung der Büromöbel erfolgt dann allerdings nicht durch A 12, sondern durch das Referat Haushalts- und Beschaffungswesen (A 13), das eine entsprechende Mitteilung von A 12 erhalten muß.

In der Justizbehörde war es nun üblich, daß über diese Mitteilung hinaus gleich die ganze personalärztliche Stellungnahme von A 12 an A 13 gegeben wurde. In dem der Eingabe zugrunde liegenden Fall war die personalärztliche Stellungnahme dabei ganz verlorengegangen. Die Justizbehörde rechtfertigte dieses Verfahren damit, daß in den personalärztlichen Stellungnahmen keine Hinweise zum Gesundheitszustand des betroffenen Mitarbeiters enthalten seien. Diese Darstellung ist jedoch nachweislich falsch. Uns liegt aus dem Eingabevorgang eine personalärztliche Stellungnahme vor, nach der der betroffene Mitarbeiter an einer Minderbelastbarkeit seines Bewegungsapparates leide. Solche Mitteilungen in der Behörde weiterzugeben, ist nicht vertretbar.

Wir haben daher der Justizbehörde empfohlen, die Weitergabe solcher personalärztlichen Stellungnahmen von A 12 an A 13 künftig zu unterlassen. Unserer Bitte, dies zu bestätigen, ist die Justizbehörde jedoch nicht nachgekommen.

Sie hat lediglich die Kenntnisnahme dieser Empfehlung bestätigt. Wir werden daher beobachten müssen, ob sich die Justizbehörde in dieser Frage wenigstens künftig datenschutzgerecht verhält.

8. Statistik

8.1 Handels- und Gaststättenzählung

In mehrjährigen Abständen, zuletzt 1985 und 1993, führte das Statistische Landesamt eine Erhebung bei allen Unternehmen des Handels und des Gastgewerbes durch. Die Rechtsgrundlage für die Handels- und Gaststättenzählung bildet das Handelsstatistikgesetz (HdlStatG). Aufgrund einer Eingabe hatten wir uns mit der im Jahr 1993 durchgeführten Erhebung auseinanderzusetzen.

Ein Zollbeamter hatte einen Fragebogen für die Handels- und Gaststättenzählung erhalten. Obwohl er dem Statistischen Landesamt telefonisch mitgeteilt hatte, daß er kein Handels- oder Gaststättengewerbe betreibe und den Fragebogen am folgenden Tag mit einem entsprechenden Vermerk zurückgesandt hatte, wurde er Ende Juni 1993 vom Statistischen Landesamt gemahnt, den Fragebogen ausgefüllt innerhalb von zwei Wochen zurückzusenden. Daraufhin hat er dem Statistischen Landesamt nochmals schriftlich erläutert, daß er den Fragebogen nicht ausfüllen könne, da er nicht zu den Auskunftspflichtigen gehöre. Seine Hoffnung, daß die Angelegenheit damit erledigt wäre, erwies sich leider als unbegründet. Zwar erhielt er Ende Juli ein Schreiben des Leiters des Statistischen Landesamts, in dem dieser versicherte, daß die Daten des Petenten gelöscht würden; Anfang September folgte jedoch eine weitere, energische Aufforderung zur Auskunftserteilung. Nach einer erneuten Beschwerde teilte das Statistische Landesamt dem Petenten schließlich mit, nun seien seine Daten aber wirklich gelöscht worden.

Dieser Vorgang weist nicht nur auf eine fehlerhafte Sachbearbeitung im Einzelfall hin, sondern er offenbart auch ein grundsätzliches Problem. Das dem Statistischen Landesamt von der Steuerverwaltung übermittelte Adressenmaterial enthält viele Anschriften von Personen, die nicht zum Kreis der Auskunftspflichtigen gehören.

§ 6 Abs. 2 HdlStatG sieht vor, daß die Finanzbehörden den mit der Durchführung der Zählung betrauten statistischen Behörden die Anschriften und Gewerbekennziffern aller Unternehmen des Handels und des Gastgewerbes mitteilen.

Nach Auskunft des Statistischen Landesamts steht jedoch ein hinlängliches Abgrenzungskriterium dafür, welche Unternehmen zu diesem Wirtschaftsbereich gehören, nicht zur Verfügung. Die von den Finanzämtern gespeicherte Gewerbekennziffer liefere jeweils nur einen gewissen Anhaltspunkt für die Branchenzugehörigkeit; nur etwa zwei Drittel der Unternehmen mit einer entsprechenden Gewerbekennziffer seien tatsächlich diesem Bereich zuzurech-

nen. Auf der anderen Seite fänden sich im Bestand der Unternehmen, die mit Gewerbekennziffern anderer Wirtschaftsbereiche oder ohne Kennziffer gespeichert sind, eine Vielzahl von Unternehmen, die zum Handel und Gastgewerbe gehörten.

Nach Auffassung des Statistischen Landesamts müßte ihm die Steuerverwaltung für eine vollständige statistische Erfassung des Handels und des Gastgewerbes eigentlich sämtliche Unternehmensanschriften übermitteln, damit sodann alle Unternehmen angeschrieben und nach ihrer Zugehörigkeit zum Handels- und Gastgewerbebereich befragt werden könnten. Darauf habe man jedoch aus Kostengründen verzichtet. Statt dessen habe sich das Statistische Landesamt darauf beschränkt, die Steuerverwaltung auch um die Hergabe derjenigen Unternehmensanschriften zu bitten, die zwar Gewerbekennziffern außerhalb des Erhebungsbereichs haben, bei denen jedoch aufgrund „früherer Erfahrungen" ein größerer Anteil von Handels- und Gastgewerbeunternehmen zu vermuten sei, z. B. für die Kraftfahrzeugreparaturbranche und für solche Unternehmen, für die gar keine Gewerbekennziffer gespeichert ist.

Da es sich bei § 6 Abs. 2 HdlStatG um eine abschließende Regelung handelt, darf die Steuerverwaltung nur die Anschriften von Unternehmen aus dem Handels- und Gastgewerbebereich und keine weiteren Anschriften übermitteln. Daten von Unternehmen, bei denen nicht einmal ihre Gewerbekennziffer darauf schließen läßt, daß sie zum Erhebungsbereich gehören, dürfen nicht übermittelt werden.

Solange von den Unternehmen, die mit Gewerbekennziffern aus dem Handel und dem Gastgewerbe bei der Steuerverwaltung gespeichert sind, nahezu ein Drittel tatsächlich nicht zu diesem Wirtschaftsbereich gehören, ist es auch nicht zulässig, daß diese Anschriften übermittelt werden. Die Steuerverwaltung muß zunächst die Richtigkeit der Zuordnung der Gewerbekennziffern überprüfen, die weitere Speicherung unrichtiger Daten abstellen und damit auch der Vorgabe von § 19 Abs. 1 HmbDSG (Berichtigung unrichtiger Daten) nachkommen.

9. Schulwesen

9.1 Schulgesetz- und Verordnungsentwurf

Nachdem die datenschutzrechtlichen Bestimmungen im Entwurf der Schulgesetznovelle stark gekürzt worden waren (siehe 11. TB, 9.1), war eine ergänzende Rechtsverordnung unerläßlich geworden. Hierzu ist uns ein Referentenentwurf zugeleitet worden, zu dem wir auch bereits Stellung genommen haben. In dieser Verordnung sind vor allem Regelungen der zulässigen Datenkränze, der Datensicherung, des Akteneinsichtsrechts und der Aufbewahrungs- und Löschungsregelungen vorgesehen.

Es zeichnet sich ab, daß nach dem Vorbild von § 5 a Abs. 4 des Berliner Schulgesetzes den Schülern ein Auskunfts- und Akteneinsichtsrecht bereits vor Vollendung des 18. Lebensjahres eingeräumt wird (siehe auch 1.3).

Wichtig wäre zudem, über die Regelungen im Hamburgischen Datenschutzgesetz hinaus eine Verpflichtung zur Löschung von Daten auch dann vorzusehen, wenn diese Daten in Akten gespeichert sind. Zum Vergleich kann dazu auf die Anordnung über die Führung und Verwaltung der Personalakten vom 30. November 1971 verwiesen werden. Auch im Entwurf des Zweiten Gesetzes zur Änderung des Sozialgesetzbuches (siehe 6.2) ist vorgesehen, die Löschungsverpflichtung auf Daten in Akten zu erstrecken.

Mit einem Inkrafttreten der Schulgesetznovelle kann nach unseren Informationen erst nach Beginn des Schuljahres 1994/95 gerechnet werden. Diese erneute Verzögerung hängt allerdings nur mit solchen Neuregelungen zusammen, die keinen datenschutzrechtlichen Charakter haben. Sollte sich im Frühjahr 1994 zeigen, daß die Diskussion um diese Regelungen zu noch weiteren Verzögerungen führt, wäre es aus unserer Sicht unerläßlich, eine auf die datenschutzrechtlichen Regelungen beschränkte Novellierung des Schulgesetzes vorzuziehen.

9.2 Verfahren bei Einschulungen

Aus Anlaß einer Eingabe haben wir das einer Einschulung vorangehende Verfahren überprüft, und zwar beginnend mit den Übermittlungen aus dem Einwohnerzentralregister. Dabei ergaben sich verschiedene Verbesserungsmöglichkeiten.

9.2.1 Bisheriges Verfahren

Nach dem festgestellten Stand übermittelt die zentrale Meldestelle jährlich im Dezember nach Schulen geordnete Listen bezüglich der Kinder, die bis zum 30. Juni des übernächsten Kalenderjahres das 6. Lebensjahr vollendet haben. Diese Listen werden parallel an die Behörde für Schule, Jugend und Berufsbildung (BSJB) und an die bezirklichen schulärztlichen Dienste (SÄD) versandt; die BSJB leitet sie an die Schulen weiter. Grundlage dieser Übermittlungen ist § 12 der Verordnung über regelmäßige Datenübermittlungen aus dem Melderegister (HmbMeldeDÜV).

Die Listen dienen insgesamt drei verschiedenen Zwecken: Der SÄD schreibt die Eltern an, um die vorgezogene Schulanfängeruntersuchung durchführen zu können, die etwa ein Jahr vor der Einschulung erfolgen soll. Von den Schulen werden sie zunächst verwendet, um die Eltern auf die Möglichkeit des – freiwilligen – Vorschulbesuches hinzuweisen (die Vorschule beginnt ein Jahr vor der Einschulung). Ein Jahr später werden dieselben Listen von den Schulen verwendet, um die Eltern auf die Schulpflichtigkeit und die Notwendigkeit der Anmeldung hinzuweisen.

Neben diesen Standardlisten, in denen auch die jeweiligen ausländischen Schüler aufgeführt sind, gibt es noch zwei Formen von Sonderlisten. Zum einen werden den Schulen noch besondere Listen übermittelt, in denen nur ausländische Schüler aufgeführt sind. Zum anderen werden die Datensätze solcher Kinder, hinsichtlich derer im Einwohnerzentralregister eine Auskunftssperre eingetragen ist, auf einer gesonderten Liste aufgeführt, die einen ausdrücklichen Hinweis auf die Auskunftssperre enthält.

In der Diskussion mit der BSJB, der Behörde für Arbeit, Gesundheit und Soziales (BAGS), der Behörde für Inneres (BfI) und dem Amt für zentrale Meldeangelegenheiten haben wir die verschiedenen Fragen erörtert, die sich aus unseren Feststellungen ergaben.

9.2.2 Geburtsangaben

Die Geburtsdaten der gesetzlichen Vertreter und die Geburtsorte der Kinder werden bislang nicht übermittelt, obwohl die geltende HmbMeldeDÜV dies erlaubt. Damit wird deutlich, daß der Gesichtspunkt der eindeutigen Identifizierung, der üblicherweise das Geburtsdatum rechtfertigt, bei den gesetzlichen Vertretern nicht zum Tragen kommt. Beide Daten sollten daher konsequenterweise aus der HmbMeldeDÜV herausgenommen werden. Hinsichtlich der Geburtsorte der Kinder besteht insoweit bereits weitgehendes Einvernehmen.

9.2.3 Zeitpunkt der Übermittlungen

Die Übermittlungen erfolgen bislang früher als es die HmbMeldeDÜV erlaubt; diese sieht die Übermittlungen im ersten Halbjahr des Jahres vor, das der Vollendung des 6. Lebensjahres vorangeht. Die gegenwärtige Praxis beruht darauf, daß die Abarbeitung des umfangreichen Datenmaterials sowohl beim SÄD als auch in den Schulen mehrere Monate in Anspruch nimmt. Das führt zugleich dazu, daß die Daten während dieses langen Verwendungszeitraums zunehmend inaktuell werden. Daher sollen die Datensätze künftig durch regelmäßige Nachübermittlungen aktualisiert werden, um die Verwendung inaktueller Datensätze zu minimieren. Gegenüber den Schulen müßten sich zudem die Übermittlungen beschleunigen lassen, indem sie direkt an diese und nicht auf dem Umweg über die BSJB erfolgen. Im übrigen soll der Übermittlungszeitpunkt in der VO entsprechend den praktischen Erfordernissen geändert und präzisiert werden.

Da die Schulen die Daten nur einmal erhalten, obwohl sie sie zu zwei verschiedenen und zeitlich weit auseinanderliegenden Zeitpunkten benötigen, sind die Daten bereits weitgehend überholt, wenn sie für Einschulungszwecke verwendet werden. Daher sollen die Übermittlungen für Einschulungszwecke etwa ein Jahr später als bislang erfolgen.

9.2.4 Information über Vorschulklassen

Gegenwärtig ungeklärt ist die Frage der Sinnhaftigkeit regelmäßiger Übermittlungen zum Zwecke der Information über Vorschulklassen. Die Aufnahme von Kindern aus sozial schlechter gestellten Familien ist ein wesentlicher Zweck der Vorschulklassen. Die BSJB hält es daher für erforderlich, die Eltern aller in Betracht kommenden Kinder über das Angebot von Vorschulklassen zu unterrichten, um diesen die Chance zu geben, einen Platz in einer Vorschulklasse zu bekommen.

Wenn diese Argumentation der Praxis entspräche, wäre gegen die Übermittlungen datenschutzrechtlich nichts einzuwenden. Tatsächlich ist es aber nach unseren Informationen so, daß die verfügbaren Vorschulklassen meistens bereits durch Anmeldungen ausgebucht sind, die ohne vorheriges Anschreiben erfolgten. Namentlich adressierte Informationsschreiben ergeben daher eigentlich keinen Sinn. Im übrigen besteht für Zwecke der Planung zusätzlicher Vorschulklassen die Möglichkeit, zusammengefaßte Übermittlungen im Einzelfall aus dem Melderegister vorzunehmen.

9.2.5 Auskunftssperren

Klarer Vorgaben bedürfen die Schulen und die schulärztlichen Dienste für die Verwendung der Datensätze, für die eine Auskunftssperre besteht, worunter z. B. Fälle von Inkognito-Adoptionen fallen. In der Praxis gibt es nach unserem Eindruck keine ausreichenden Informationen darüber, wie mit solchen Datensätzen umgegangen werden soll. Daher besteht latent die Gefahr, daß die gesperrten Datensätze unzulässig verwendet werden. Sofern hier keine Klärung erreicht werden kann, sollte auf die Übermittlung dieser Datensätze verzichtet werden.

9.2.6 Vernichtung

Letztlich muß in den Grundschulen sichergestellt werden, daß die übermittelten Listen unverzüglich vernichtet werden, nachdem sie ihrem Zweck entsprechend verwendet worden sind. Eine darüber hinausgehende Aufbewahrung ist nicht zulässig (§ 31 Abs. 7 HmbMG).

Eine verbindliche Klärung dieser Fragen steht gegenwärtig noch aus. Zum Teil wird sie im Rahmen der anstehenden Novellierung der HmbMeldeDÜV erfolgen müssen.

9.3 Umfrage zu Noten- und Berichtszeugnissen

Nach § 31 Abs.1 Satz 2 des Schulgesetzes werden in den Klassen 3 und 4 der Grundschule entweder Noten- oder Berichtszeugnisse erteilt. Entscheidend ist insoweit die mehrheitliche Abstimmung der Erziehungsberechtigten, die einheitlich für die ganze Klasse gilt. Nach einer internen Regelung der Behörde für Schule, Jugend und Berufsbildung (BSJB) wird das Abstimmverhalten

namentlich erfaßt; die Stimmzettel sollen dann rund zwei Jahre aufbewahrt werden.

Eine Änderung dieses Verfahrens konnten wir gegenüber der BSJB nicht durchsetzen. Sie stellt u. a. darauf ab, daß es nach einer Abstimmung unter den Eltern eines Kindes zu Streit darüber kommen kann, ob das Stimmrecht einvernehmlich ausgeübt wurde. Die Schule müsse dann in der Lage sein, das Abstimmverhalten der Eltern nachzuvollziehen. Im übrigen vertrat die BSJB die Auffassung, daß es für die Eltern keine Geheimhaltungsgründe gebe und die Eltern zu ihrer Entscheidung stehen müßten. Datenschutzrechtliche Argumente seien in diesem Zusammenhang ungeeignet. Zudem soll die Kenntnis des Abstimmverhaltens eine – nicht näher konkretisierte – Bedeutung für den gemeinsamen Erziehungsprozeß von Eltern und Lehrern haben.

Wir haben die BSJB darauf hingewiesen, daß das Erforderlichkeitsprinzip, das aus dem Grundrechtscharakter des Datenschutzes und dem Eingriffscharakter der Datenverarbeitung folgt, durch allgemeine pädagogische Überlegungen nicht aufgehoben wird, sondern auch im schulischen Bereich zu beachten ist. Es kommt daher nicht darauf an, ob die Eltern Geheimhaltungsgründe für ihr Abstimmverhalten haben. Auch hat die Schule den Eltern nicht die Entscheidung darüber abzunehmen, ob sie zu einer Entscheidung „stehen" wollen.

Daher darf ein Zugriff auf die Abstimmzettel ausschließlich durch die Schulleitung (einschließlich der Schulsekretärin) und nur dann erfolgen, wenn das Abstimmergebnis von einem Betroffenen fristgerecht angefochten wurde. Unzulässig wäre es, wenn die Abstimmzettel aufgrund irgendwelcher allgemeinen pädagogischen Gründe herangezogen werden, um ein individuelles Abstimmverhalten nachzuvollziehen. Gemäß § 23 Abs. 2 1. Halbsatz HmbDSG haben wir der BSJB empfohlen, die Abstimmzettel so zu verwahren, daß sie dem allgemeinen Zugriff der Lehrer entzogen sind.

10. Steuerwesen

10.1 Abgabenordnung

10.1.1 Ursprüngliches Änderungskonzept

Mit Stand vom 11. Mai 1993 wurde der überarbeitete Entwurf eines Gesetzes zur Änderung der Abgabenordnung und anderer Rechtsvorschriften (AOÄG 1994) vorgelegt. Mit dem AOÄG-E 1994 wurden folgende Ziele angestrebt:

— die Reform des außergerichtlichen Rechtsbehelfsverfahrens nach der Abgabenordnung (AO) und des Verfahrens vor dem Bundesfinanzhof,

— die Ergänzung und Präzisierung bereichsspezifischer Datenschutzvorschriften in der AO sowie

— die Überarbeitung einer Reihe sonstiger steuerrechtlicher Regelungen, deren Notwendigkeit oder Zweckmäßigkeit sich seit der letzten umfassenden Änderung der AO durch das Steuerbereinigungsgesetz von 1986 ergeben hat.

Die bereits seit mehreren Jahren verfolgte Ergänzung und Präzisierung der bereichsspezifischen Datenschutzvorschriften in der AO sollte – darüber bestand bislang Einvernehmen mit den Finanzressorts des Bundes und der Länder – vor allem der neueren Datenschutzgesetzgebung Rechnung tragen und den Umgang mit Daten, die dem Steuergeheimnis unterliegen, klarer als bisher regeln.

Dieser Entwurf greift allerdings zum einen noch immer nicht alle Verbesserungsvorschläge auf, die wiederholt von den Datenschutzbeauftragten des Bundes und der Länder vorgetragen worden sind (11. TB, 10.1). Zum anderen enthält er gegenüber der bisherigen Fassung einige wesentliche Änderungen, die zusätzlich Anlaß zur Kritik aus datenschutzrechtlicher Sicht geben.

So sieht § 30 Abs. 6 Nr. 4 AOÄG-E 1994 vor, daß eine Offenbarung geschützter Daten dann zulässig sein soll, wenn diese zur Verfolgung von „Straftaten von erheblicher Bedeutung" erforderlich ist. Der Begründung ist zu entnehmen, daß der Begriff „Straftat von erheblicher Bedeutung" in der Strafprozeßordnung (StPO) abschließend definiert sei; damit trete eine klare Definition von Fällen, in denen eine Offenbarung zulässig sei, an die Stelle des unbestimmten Rechtsbegriffs „zwingendes öffentliches Interesse", soweit es um die Verfolgung von Straftaten gehe. Dies diene der Normenklarheit.

Es trifft jedoch nicht zu, daß der Begriff „Straftat von erheblicher Bedeutung" in der StPO abschließend definiert ist. Vielmehr werden in der StPO zu unterschiedlichen Verfolgungsmaßnahmen jeweils auch unterschiedliche Straftatenkataloge festgelegt. Wir halten deshalb eine gesetzliche Regelung mit Hilfe des unbestimmten Rechtsbegriffes „Straftat von erheblicher Bedeutung" nur dann für hinnehmbar, wenn in der AO – bezogen auf den jeweiligen Normzweck – eine enumerative Festlegung von Straftaten den Rahmen der Gesetzesanwendung eingrenzt.

Außerdem ist es nicht nachzuvollziehen, daß § 30 Abs. 6 Nr. 10 AOÄG-E 1994 ohne Einschränkung weiter an dem Begriff des „zwingenden öffentlichen Interesses" festhält. In der Begründung heißt es andererseits, daß nur noch zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung eine Durchbrechung des Steuergeheimnisses notwendig sei. Dies sollte dann aber auch im Gesetzestext konkret zum Ausdruck kommen.

Die in § 88 Abs. 3 AOÄG-E 1994 vorgesehene Zulässigkeit der Sammlung von geschützten Daten in Dateien oder Akten „für Zwecke zukünftiger Verfahren" und deren Offenbarung an andere Finanzbehörden widerspricht den Anforderungen, die an die Erforderlichkeit und Verhältnismäßigkeit der Verarbeitung personenbezogener Daten zu stellen sind. Insbesondere die bereits beabsich-

tigte Einrichtung einer automatisiert geführten bundesweiten Fahndungsdatei, die Zusammenführung aller Dateien der einzelnen Finanzämter für Steuerstrafsachen und Steuerfahndung in der Informationszentrale für den Steuerfahndungsdienst, der Verwendungszweck der dort gesammelten Daten, die zugelassenen Datenarten, der betroffene Personenkreis und die Datenempfänger bedürfen einer normenklaren gesetzlichen Festlegung. Eine so allgemein gehaltene Formulierung wie in § 88 Abs. 3 AOÄG-E 1994 reicht dafür keinesfalls aus.

Mit der Regelung in § 249 Abs. 2 AOÄG-E 1994 soll die Rechtsgrundlage dafür geschaffen werden, daß im Besteuerungsverfahren erlangte Kenntnisse auch im Vollstreckungsverfahren durch Finanzbehörden wegen außersteuerlicher Rückstände verwertet werden dürfen. Die pauschale Aufhebung des bislang geltenden Zweckbindungsgebotes von Steuerdaten an steuerrechtliche Verfahren halten wir aus datenschutzrechtlicher Sicht für bedenklich. Für den Fall, daß eine solche Regelung aus der Sicht des Steuergesetzgebers tatsächlich zwingend erforderlich ist, sollte sie ausdrücklich beschränkt werden auf die in der Begründung erwähnten Einzelfälle. Aus dem Gesetzestext selbst sollte dann auch eindeutig hervorgehen, daß nur bereits bekannte Daten verwertet werden dürfen und besondere Ermittlungen nach §§ 85 ff. AO für diese Fälle ausgeschlossen sind. Ein Hinweis in der Begründung erscheint in diesem Zusammenhang nicht weitreichend genug.

10.1.2 Aktueller Stand

Das insgesamt sachgerechte und in Einzelpunkten verbesserungsbedürftige Konzept des Entwurfs für ein AOÄG 1994 soll nun erstaunlicherweise nicht mehr weiterverfolgt werden. Die Änderungen datenschutzrechtlicher Bestimmungen in der Abgabenordnung und die Reform des außergerichtlichen Rechtsbehelfsverfahrens sollen außerhalb eines AOÄG 1994 jeweils gesondert weiterbehandelt werden. Alle übrigen Regelungen werden in den Entwurf eines Gesetzes zur Bekämpfung des Mißbrauchs und zur Bereinigung des Steuerrechts (Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetz) übernommen.

Eine solche Entscheidung würde alle bisherigen Bemühungen, die Vorschriften der AO zum Umgang mit personenbezogenen Daten an die Rechtsprechung und neuere Datenschutzgesetzgebung anzupassen, vorerst gegenstandslos machen.

Die Begründung für die oben genannte Absicht ist aus unserer Sicht nicht verständlich. Zum einen ist die Forderung nach Anpassung der AO in bezug auf die Systematik, den Aufbau und die Terminologie der Vorschriften nur ein Teil der insgesamt aus datenschutzrechtlicher Sicht erforderlichen Ergänzungen und Präzisierungen. Zum anderen lassen die Entscheidungen des Bundesverfassungsgerichtes, die zur Unterstützung der nunmehr angestrebten Vorgehensweise herangezogen werden, keineswegs den Schluß zu, es bestehe „für

eine Änderung der AO im Hinblick auf datenschutzrechtliche Vorschriften weder eine rechtliche noch eine praktische Notwendigkeit". Diese Urteile beziehen sich allein auf die jeweils zugrunde liegenden Tatbestände und erklären daher auch nur in diesen Fällen die Vorschriften der AO unter Berücksichtigung des Rechts auf informationelle Selbstbestimmung für im Grundsatz verfassungskonform. Inwieweit die betreffenden Regelungen in anderen Fällen mit den verfassungsrechtlichen Anforderungen an den Datenschutz übereinstimmen, war nicht Gegenstand dieser Entscheidungen.

Die Beschränkung der Änderungen der Abgabenordnung auf die – problematischen – Punkte des Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetzes ist aus unserer Sicht nicht vertretbar. Die von vielen Datenschutzbeauftragten der Länder und des Bundes zu dieser Vorgehensweise eingebrachte Kritik ist jedoch nicht berücksichtigt worden.

Der Bundesrat hat gemäß Beschluß vom 26. November 1993 zu dem vom Deutschen Bundestag am 11. November 1993 verarbschiedeten Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetz den Vermittlungsausschuß angerufen. Mit dem Beschluß soll u. a. auch die Aufnahme der beiden bereits oben kritisierten Änderungsvorschläge zur AO — hinsichtlich der Sammlung geschützter Daten für Zwecke zukünftiger Verfahren (jetzt § 88 a AO) und der Verwendung von Kenntnissen, die im Besteuerungsverfahren erlangt sind, für die Vollstreckung außersteuerlicher Rückstände (§ 249 Abs. 2 AO) – erreicht werden. Das Gesetzgebungsverfahren war bei Redaktionsschluß noch nicht beendet.

10.2 Zweitwohnungsteuer

Am 1. Januar 1993 ist in Hamburg das Gesetz zur Einführung der Zweitwohnungsteuer und Änderung melderechtlicher Vorschriften in Kraft getreten. Danach wird für das Innehaben einer Zweitwohnung in Hamburg zukünftig ein Betrag von 8 % der Jahres-Nettokaltmiete als Steuer erhoben. Das neue Gesetz regelt das Verfahren zur Erhebung, Festsetzung und Entrichtung dieser Zweitwohnungsteuer.

Daneben enthält das Gesetz mehrere für die Sicherstellung der Besteuerung notwendige Änderungen des Hamburgischen Meldegesetzes und der Verordnung über regelmäßige Datenübermittlungen aus dem Melderegister. Dazu gehört vor allem die Meldepflicht für Einwohner, die in Hamburg eine Nebenwohnung beziehen oder bereits bewohnen. Bislang waren diese nur hinsichtlich ihrer Hauptwohnung meldepflichtig.

Ende April 1993 begann das Finanzamt für Verkehrsteuern und Grundbesitz mit der Versendung der entsprechenden Erhebungsvordrucke. Angeschrieben wurden etwa 91.000 Bürger, bei denen eine Steuerpflicht vermutet wurde. Dazu wurden aufgrund von Art. 4 Abs. 3 des Zweitwohnungsteuergesetzes aus dem Melderegister alle Adressen derjenigen Einwohner übermittelt, die „zum Zeit-

punkt des Inkrafttretens dieses Gesetzes in der Freien und Hansestadt Hamburg bereits mit Nebenwohnung gemeldet" waren. Nur wenige Tage nach der Versendung der ersten Fragebögen häuften sich Anfragen und Eingaben, die alle auf Mängel im Meldedatenbestand zurückzuführen waren. So wurden Personen angeschrieben, die ihre Zweitwohnungen längst aufgegeben hatten, wegen Um- oder Wegzuges unter der von der Finanzbehörde verwendeten Adresse nicht mehr erreichbar waren oder sogar vor Jahren verstorben waren.

Bereits im 11. TB (13.2) hatten wir auf die wachsende Unzuverlässigkeit des Melderegisters aufmerksam gemacht. In diesem Fall war die zu einem hohen Anteil fehlerhafte Adressierung der Erhebungsvordrucke – nach Angaben der Finanzbehörde möglicherweise bis zu 45.000 unzutreffende Anschriften – jedoch nicht auf strukturelle Fehler im automatisierten Meldedatenbestand zurückzuführen. Sie beruhte vielmehr darauf, daß im Melderegister zwar in den zurückliegenden Jahren die Anmeldung einer Nebenwohnung eingetragen worden war (Wohnungsstatus „N"), diese Datensätze jedoch nur dann fortgeschrieben worden sind, wenn die Einwohnermeldeämter gezielte Änderungsmitteilungen erhalten haben. Diese wurden von den Betroffenen allerdings häufig unterlassen, da es bis zum Inkrafttreten des Zweitwohnungsteuergesetzes und der damit verbundenen Änderungen im Melderecht keine Meldepflicht für Nebenwohnungen in Hamburg gegeben hat. Regelmäßige Überprüfungen, wie sie sich im Zusammenhang mit einer Hauptwohnung ergeben (z. B. bei der Beantragung eines neuen Ausweises, einer Eheschließung oder der Versendung einer Wahlbenachrichtigungskarte), fanden bislang nicht statt.

Für zusätzliche Schwierigkeiten in bestimmten Einzelfällen sorgte zudem ein „bürgerfreundlicher Service" der Finanzbehörde. Der aus dem Melderegister übermittelte Datenbestand wurde per Programm auf „Ehegatten-Fälle" untersucht. Waren zwei Personen unterschiedlichen Geschlechts mit identischen Nachnamen und identischen Adressen gespeichert, bei denen jeweils das Alter größer 18 Jahre war und der Altersunterschied nicht mehr als 15 Jahre betrug, wurden diese Personen gemeinsam als Ehegatten zur Beantwortung des Fragebogens aufgefordert. Auf diese Weise kam es dazu, daß in einem Haus lebenden Geschwistern ein Eheverhältnis unterstellt wurde. Der Familienstand konnte auch nicht gegengeprüft werden, da er im Datenbestand nicht enthalten war.

Unser besonderes Augenmerk gilt der zügigen Berichtigung des Meldedatenbestandes. Ergibt sich aus den Ermittlungen des Finanzamts, daß eine mit Nebenwohnung gemeldete Person diese nicht mehr innehat, so sieht § 12 Satz 1 Zweitwohnungsteuergesetz eine entsprechende Mitteilung an die Meldebehörde vor.

Dieses Rückmeldeverfahren zur Aktualisierung des Melderegisters ist zwischen Steuerverwaltung, Senatsamt für Bezirksangelegenheiten und Bezirksamt Harburg, Amt für zentrale Meldeangelegenheiten bereits im Vorwege erörtert worden. Letzteres hat mit Rundschreiben vom 6. Mai 1993 die Einwohnerdienststellen über die vereinbarte Art und Weise der Durchführung informiert. Auch aus unserer Sicht kommt dabei allen Hinweisen, die beim Finanzamt über die Ursachen der Unzustellbarkeit von Erhebungsbögen (z. B. Wegzug, Namensänderungen, Sterbefälle) eingehen, besondere Bedeutung zu.

Aus den beim Hamburgischen Datenschutzbeauftragten eingegangenen Anfragen und Eingaben ergibt sich, daß das Finanzamt nicht nur Erhebungsbögen mit dem Zusatz „Post unzustellbar" zurückerhält, sondern auch – z. B. von den jetzigen Wohnungsinhabern, Verwandten oder Nachbarn – Erkenntnisse über den Grund der Unzustellbarkeit gewinnt. Jeder dieser zusätzlichen Hinweise würde den Meldedienststellen die Aufklärungsarbeit erleichtern. Deshalb wird die von der Steuerverwaltung zunächst beabsichtigte Verfahrensweise, nur die Tatsache der Unzustellbarkeit an die Meldebehörden mitzuteilen, dem Zweck der Übermittlungsvorschrift nicht gerecht.

Wir halten es für erforderlich und auch gemäß § 12 Satz 1 des Zweitwohnungsteuergesetzes rechtlich für zulässig, daß das Finanzamt für Verkehrsteuern und Grundbesitz den Einwohnerdienststellen alle vorhandenen, der Fortschreibung des Melderegisters dienenden Ermittlungsergebnisse mitteilt. Es sollte deshalb vom Finanzamt nicht nur automatisiert ein Formblatt ausgedruckt und versandt werden, aus dem lediglich entnommen werden kann, für welche Person die Post als unzustellbar zurückgekommen ist. Vielmehr sind die beim Finanzamt eingehenden Hinweise auf die Ursache der Unzustellbarkeit den Meldebehörden ebenfalls in geeigneter Weise zur Verfügung zu stellen.

Auch das Amt für zentrale Meldeangelegenheiten geht davon aus, daß die Einwohnerdienststellen vom Finanzamt alle dort aufgrund der Erhebungsbogenversendung bekanntgewordenen Informationen erhalten, die der Aktualisierung des Melderegisters dienen. Die Einwohnerdienststellen sind bereits in dem oben genannten Rundschreiben darauf hingewiesen worden, daß alle eingehenden Hinweise auf Wegzüge, Statusänderungen, Sterbefälle usw. zunächst im Einzelfall zu prüfen und erst dann in den Einwohnerdatenbestand zu übernehmen sind.

Es handelt sich bei der Übermittlung der melderechtlich relevanten Daten vom Finanzamt an die Meldestellen auch nicht um einen Bruch des Steuergeheimnisses, da sich die Offenbarungsbefugnis aus § 30 Abs. 4 Nr. 2 Abgabenordnung i. V. m. § 1 des Hamburgischen Abgabengesetzes ergibt.

Die Finanzbehörde hat zugesagt, unsere Vorschläge für die Umsetzung des Rückmeldeverfahrens aufzugreifen und zukünftig bei den Mitteilungen an die Meldebehörden zu berücksichtigen.

11. Wissenschaft, Forschung und Kultur

11.1 Datenverarbeitung durch die Hochschulen

11.1.1 Studentenoperationssystem

Im 11. TB (11.1.1) hatten wir von dem Entwurf einer Hochschuldatenverordnung berichtet. Die Hochschuldatenverordnung ist Ende 1992 in Kraft getreten. Dies haben wir zum Anlaß genommen, uns näher über das von der Universität Hamburg betriebene Studentenoperationssystem (SOS) zu informieren.

Das SOS wird als Verfahren der Universität auf Rechnern des Landesamtes für Informationstechnik betrieben. Im Hinblick auf den Datenkatalog und die Funktionalität des Systems haben in der Vergangenheit Abstimmungen mit anderen Hochschulen stattgefunden. Eine technische Verknüpfung zu Verfahren, die von anderen Hochschulen betrieben werden, existiert jedoch nicht.

Der verarbeitete Datenkatalog hält sich im wesentlichen an die Vorgaben der Hochschuldatenverordnung. Einige Detailfragen wie etwa die Erhebung des Vermieters bedürfen hingegen noch einer befriedigenden Lösung.

11.1.2. Datenübermittlung der Prüfungsämter an die Universität

Berlin hat im Gesetz über die Schaffung bereichsspezifischer Regelungen für die Verarbeitung personenbezogener Daten vom 26. Januar 1993 die Datenübermittlung der Prüfungsämter der Hochschulen und der staatlichen Prüfungsämter an die zuständigen Stellen der Hochschulen bereichsspezifisch geregelt. Danach übermitteln die Prüfungsämter zu Verwaltungszwecken die Namen von Personen, die an der Prüfung teilgenommen haben, sowie deren Anschriften und die Mitteilung über das Bestehen oder Nichtbestehen der Prüfung.

Unter Hinweis auf die neue Regelung in Berlin haben wir die Behörde für Wissenschaft und Forschung um Stellungnahme gebeten, ob aus ihrer Sicht auch in Hamburg die Datenübermittlung durch die Prüfungsämter bereichsspezifisch geregelt werden sollte. Die Behörde hat dies verneint.

Nach Erkenntnissen des Hamburgischen Datenschutzbeauftragten entspricht die Praxis in Hamburg im wesentlichen der neuen Berliner Regelung. Insbesondere werden auch in Hamburg keine Prüfungsnoten übermittelt. Die Daten werden unter anderem für Exmatrikulationszwecke benötigt. Gegen das Verfahren bestehen insoweit keine Bedenken.

Aus diesem Grund erscheint eine bereichsspezifische Regelung in Hamburg jedenfalls solange verzichtbar, wie in der Praxis keine datenschutzrechtlichen Probleme zu beobachten sind. Sollte etwa aufgrund von Eingaben aus datenschutzrechtlicher Sicht Handlungsbedarf entstehen, werden wir uns erneut mit der Forderung nach einer bereichsspezifischen Regelung an die zuständigen Stellen wenden.

11.2 Datenverarbeitung der Fachbereiche Wirtschaftswissenschaften und Psychologie der Universität Hamburg

Bei einer Prüfung der Datenverarbeitung in zwei Fachbereichen (Wirtschaftswissenschaften und Psychologie) der Universität Hamburg haben wir festgestellt, daß dort Daten von Studenten und von Lehrpersonal zu Verwaltungszwecken verarbeitet werden. So werden in verschiedenen Universitätsinstituten Daten für die Organisation von Lehrveranstaltungen und für die Abwicklung von Klausuren auf Personalcomputern gespeichert.

Von größerer Bedeutung sind UNIX-Verfahren, die im Rahmen eines Kooperationsabkommens zwischen einem Informatikunternehmen und der Universität Hamburg bzw. dem Fachbereich Wirtschaftswissenschaften zur Fachbereichsverwaltung und zur Unterstützung des dortigen Prüfungsamtes entwickelt werden. Anders als bei den auf stand-alone-PC geführten Institutssystemen können Benutzer von verschiedenen Endgeräten auf die gespeicherten Daten zugreifen. Problematisch erscheint hierbei, daß bereits in der Entwicklungsphase echte personenbezogene Daten verarbeitet werden, ohne daß die Systeme hinsichtlich ihrer Funktionalität – einschließlich der Datenschutzanforderungen – verbindlich abgenommen worden sind. Damit wird hier praktisch mit Echtdaten entwickelt und getestet. Außerdem werden verschiedene Regelungen nicht eingehalten, die durch das Hamburgische Datenschutzgesetz und durch Verwaltungsvorschriften vorgeschrieben sind.

Nach den Aussagen des Projektleiters aus dem Fachbereich Wirtschaftswissenschaften wird diesen Projekten eine Pilotfunktion mit denkbarer Übertragung auf andere Fachbereiche oder Universitäten zugedacht. Umso mehr wäre es erforderlich gewesen, den Datenschutzbelangen – einschließlich der frühzeitigen Beteiligung des Hamburgischen Datenschutzbeauftragten – ein angemessenes Gewicht einzuräumen.

Wir haben uns an die Universität Hamburg gewandt, um das weitere Verfahren abzustimmen. In diesem Zusammenhang haben wir ausdrücklich bedauert, daß wir – trotz wiederholter Rückfrage – erst durch diese Prüfung von der automatisierten Verarbeitung personenbezogener Daten in den Fachbereichen und insbesondere von dem Kooperationsabkommen und dem Automatisierungsprojekt erfahren haben.

Dieser Komplex bedarf in den Einzelheiten einer möglichst einvernehmlichen Klärung. Auf den Vorgang wird im nächsten TB zurückzukommen sein.

11.3 Vergabe von Wohnheimplätzen beim Studentenwerk

Im Berichtszeitraum hat das Studentenwerk den Aufnahmeantrag für Studentenwohnheimplätze neu gestaltet. Wir waren in das Verfahren einbezogen.

Auf unseren Vorschlag hin wird von den Bewerbern jetzt kein Lebenslauf mehr verlangt. Statt dessen enthält der Aufnahmeantrag gezielte Fragen insbeson-

dere zur finanziellen Situation der Betroffenen, um eine sachgerechte Vergabe der Plätze zu ermöglichen. Wir begrüßen ausdrücklich, daß auf die Erhebung von Daten Dritter verzichtet wurde. Vor allem werden die Bewerber nicht zur wirtschaftlichen Situation ihrer Eltern befragt. Eine Übermittlung der Daten an Dritte findet nicht statt.

11.4 Datenverarbeitung im Kulturbereich

Auf unsere Initiative fand im September 1993 in der Kulturbehörde erstmals ein Gespräch über grundlegende datenschutzrelevante Fragen statt. Bisher waren wir weder bei größeren IuK-Vorhaben einbezogen worden, noch hatten wir entsprechende Dateimeldungen erhalten. Die Vertreter der Kulturbehörde sagten insoweit Nachbesserung zu.

Folgende Bereiche wurden angesprochen:

— In der kulturellen Filmförderung werden Angaben zum Förderungsempfänger und zum Förderungsgegenstand automatisiert gespeichert. Diese Datei enthält z.B. auch sensible Daten über Darlehensrückzahlungen.

— Zur automatisierten Leser-Verwaltung der Hamburger Öffentlichen Bücherhallen wurde uns mitgeteilt, daß nach Rückgabe entliehener Bücher die personenbezogenen Daten des Entleihers gelöscht werden, ein langfristiges Leser-Profil also nicht erstellt werden könne.

— Zur Durchführung der mit Museumspädagogen abgeschlossenen Werkverträge wird derzeit ein IuK-Projekt vorbereitet, das dem Hamburgischen Datenschutzbeauftragten in Kürze vorgestellt werden soll.

— Bei der Kontrolle der zahlreichen Zuwendungsempfänger der Kulturbehörde werden – jedenfalls durch den behördeninternen Prüfdienst – ebenfalls personenbezogene Daten verarbeitet (vgl. 11. TB, 7.9). Der nach der Landeshaushaltsordnung erforderliche Sachbericht enthalte personenbezogene Daten jedoch nicht.

— Hinsichtlich der automatisierten Datenverarbeitung im Kartenvorverkauf und in der Abonnementverwaltung wurden wir auf die Theater und auf die Hamburgische Staatsoper als selbständige Unternehmen mit eigener Datenschutzverantwortung verwiesen.

Insgesamt verstärkte das Gespräch bei uns den Eindruck, daß auch im Kulturbereich durchaus eine Reihe datenschutzrelevanter Verfahren und Vorhaben bestehen, die der Beteiligung und Kontrolle des Hamburgischen Datenschutzbeauftragten bedürfen. Wir haben die Kulturbehörde insoweit auf die „Bringeschuld" nach dem Hamburgischen Datenschutzgesetz aufmerksam gemacht und werden die Einhaltung der gemachten Zusagen überprüfen.

12. Bauwesen und Stadtentwicklung

12.1 Hamburgisches Gesetz über das Vermessungswesen

Seit dem 30. Juni 1993 verfügt Hamburg als letztes Bundesland endlich über ein Vermessungsgesetz (HmbVermG), das die Aufgaben und Befugnisse des Vermessungswesens zusammenfassend und normenklar regelt. Damit ist eine langjährige Forderung des Hamburgischen Datenschutzbeauftragten (vgl. 4. TB, 4.5.3 und 9. TB, 4.8.1) erfüllt worden.

Im wesentlichen neu und auch in Kataster- und Vermessungsgesetzen anderer Bundesländer erst teilweise und in jüngster Zeit eingeführt sind die Vorschriften über die Nutzung des Liegenschaftskatasters als Basissystem für ein Flächenbezogenes Informationssystem (FIS) und die hierzu getroffenen datenschutzrechtlichen Regelungen in §§ 9 bis 15 HmbVermG. Besonders hervorzuheben ist hierbei, daß das HmbVermG – im Vergleich zu Vermessungsgesetzen anderer Bundesländer – eine abschließende Aufzählung der im FIS gespeicherten Daten enthält (§ 12 HmbVermG) und daß festgelegt ist, welche Behörden und sonstigen öffentlichen Stellen Daten erheben und übermitteln dürfen. Die Erhebung und Speicherung weiterer Daten im FIS ist nur möglich, wenn der Senat aufgrund der Verordnungsermächtigung des § 12 Abs. 3 HmbVermG dieses auch zuläßt.

Mit diesem Vermessungsgesetz wurden auch die rechtlichen Voraussetzungen dafür geschaffen, daß Hinweise auf flächenbezogene Datenverarbeitungsanlagen verschiedener Behörden (Fachinformationssysteme) mit dem Liegenschaftskataster zum FIS als einer einheitlichen Grundstücksdatenbank zusammengefaßt werden. Außerdem kann dieses Systems durch eine Reihe von hamburgischen Stellen im unmittelbaren lesenden und/oder schreibenden Zugriff (Online-Verfahren) genutzt werden.

Hinsichtlich des verändernden Zugriffs haben wir darauf gedrungen, daß die Verantwortung als speichernde Stelle gegenüber dem Betroffenen auch in einem solchem Fall die Stelle zu tragen hat, die für die Führung des FIS zuständig ist und daß die eingebenden Stellen feststellbar sein müssen (vgl. 11. TB, 12.1). Die in diesem Zusammenhang zu treffenden grundlegenden Bestimmungen für die Datenübermittlung aus dem FIS gegenüber den öffentlichen Stellen sind in § 14 HmbVermG enthalten:

— Absatz 1 regelt, unter welchen Voraussetzungen die für die Führung des FIS zuständigen Behörden Daten an Behörden oder sonstige öffentliche Stellen übermitteln dürfen.

— Gemäß Absatz 2 entfällt eine Prüfung der Voraussetzungen, ob Daten an andere öffentliche Stellen übermittelt werden dürfen, nur dann, wenn die für die Führung des FIS zuständigen Behörden von den unter den Nummern 1 bis 10 aufgeführten Behörden oder öffentlichen Stellen um Übermittlung im Rahmen der Erfüllung ihrer Aufgaben ersucht werden.

— Durch Absatz 3 wird sichergestellt, daß die jeweiligen Empfänger der Daten diese nur für den Zweck nutzen, zu dem sie übermittelt worden sind, und daß eine Weitergabe an Dritte nur zulässig ist, soweit eine andere Rechtsvorschrift dies gestattet.

— Absatz 4 stellt klar, daß es zur regelmäßigen Übermittlung an andere Behörden oder sonstige öffentlichen Stellen einer besonderen gesetzlichen Grundlage bedarf.

— Der Absatz 5 enthält eine Ermächtigungsgrundlage für den Senat, durch Rechtsverordnung gemäß § 11 Hamburgisches Datenschutzgesetz (HmbDSG) zu regeln, daß an die in Absatz 2 Nummern 1 bis 8 und 10 genannten öffentlichen Stellen sowie an Unternehmen der öffentlichen Energie- und Wasserversorgung oder der öffentlichen Abfallentsorgung bestimmte Daten im lesenden Zugriff durch einen automatisierten Abruf (Online-Verfahren) übermittelt werden dürfen. Weil diese Stellen regelmäßig und in einem erheblichen Umfang zur Erfüllung ihrer Aufgaben auf Daten aus dem FIS angewiesen sind, ist der Abruf der Daten im automatisierten Verfahren auch in Anbetracht der schutzwürdigen Interessen der Dateninhaber vertretbar ist.

— In Absatz 6 ist eine weitere Ermächtigungsgrundlage für den Senat enthalten. Er kann durch Rechtsverordnung regeln, daß die in diesem Absatz genannten Stellen bei bestimmten Datenarten Eintragungen, Veränderungen und Löschungen unmittelbar vornehmen können (schreibender Zugriff), wobei die eingebenden Stellen feststellbar sein müssen. Weiterhin wird bestimmt, daß die für die Führung des FIS zuständige Behörde auch in den Fällen des schreibenden Zugriffs durch andere Stellen nach außen, insbesondere in datenschutzrechtlicher Hinsicht, allein verantwortlich für die Richtigkeit und Vollständigkeit des FIS (z. B. auch als „speichernde Stelle" im Sinne von § 4 Abs. 3 HmbDSG) bleibt.

Außerdem haben wir festgestellt, daß in Absatz 5 auch eine Verordnungsermächtigung zur Online-Abfrage für die Polizei enthalten war, obwohl wir dieses bereits im 9. TB. (4.8.1) entschieden abgelehnt hatten. Die Verordnungsermächtigung wurde – wahrscheinlich aufgrund eines redaktionellen Versehens – erst kurz vor Einbringung in den Senat mit der Aufnahme der Landwirtschaftsbehörden in den Katalog der „priviligierten" Stellen erweitert. Wir haben unsere Bedenken gegen den automatisierten Abruf der Daten durch die Polizei aufrechterhalten, da die Notwendigkeit eines solchen Verfahrens für uns nicht erkennbar ist. Bei der Beratung über die Gesetzesvorlage im Bauausschuß der Bürgerschaft haben die Senatsvertreter daraufhin auf diese Ermächtigung verzichtet.

Mit den in § 14 HmbVermG getroffenen Regelungen ist auch unsere Forderung, die „Informationsbeziehungen" zwischen dem FIS und seinen Nutznießern normenklar zu regeln, erfüllt worden (vgl. 9. TB, 4.8.1).

Zwischenzeitlich wurde eine Lenkungsgruppe für die Einrichtung des Flächenbezogenen Informationssystems eingerichtet, an der wir beteiligt sind. Über die Aufgaben der Lenkungsgruppe und den Fortgang in diesem Projekt werden wir voraussichtlich im nächsten TB berichten.

12.2 Abgeschlossenheitsbescheinigungen nach dem Wohnungseigentumsgesetz (WEG)

Bei der Erteilung von Abgeschlossenheitsbescheinigungen im Rahmen der Umwandlung von Miet- in Eigentumswohnungen informierten die Bezirksämter die Mieter über ihre Rechte anhand eines von der Baubehörde erstellten Merkblattes, wobei die Verfahrensweise in den Bezirken unterschiedlich gehandhabt wurde.

Durch die Entscheidung des Gemeinsamen Senats der Obersten Bundesgerichte vom 30. Juni 1992 zum Begriff der Abgeschlossenheit nach § 3 Abs. 2 Satz 1 WEG war die Umwandlung von Miet- in Eigentumswohnungen wieder erleichtert worden, so daß Presseberichten zufolge mit einer enormen Umwandlungswelle zu rechnen war. Vor diesem Hintergrund wurde bereits im Vorfeld eine Diskussion ausgelöst, unter welchen Voraussetzungen und zu welchem Zeitpunkt betroffene Mieter im Zusammenhang mit der Erteilung von Abgeschlossenheitsbescheinigungen einheitlich und qualifiziert unterrichtet werden können.

Die Unterrichtung der Mieter über Anträge von Abgeschlossenheitsbescheinigungen nach dem WEG hat datenschutzrechtliche Relevanz, weil hierbei zumindest offenbart wird, daß der Eigentümer eine solche Bescheinigung beantragt hat. Dies läßt einen Rückschluß auf dessen persönliche oder sachliche Verhältnisse zu und ist somit ein personenbezogenes Datum im Sinne des § 4 Abs. 1 HmbDSG.

Der Vermieter kann eine Ortsbesichtigung der umzuwandelnden Wohnung verlangen, um durch die zuständige Behörde prüfen zu lassen, ob die Wohnung oder sonstige Räume gemäß § 3 Abs. 2 WEG in sich abgeschlossen sind und ob der jetzige Zustand den Angaben in den vorhandenen Bauakten entspricht. In diesem Fall kann der Vermieter aber nur unter Angabe von Gründen Einlaß in die Wohnung des Mieters begehren. Auf diese Weise wird dem Mieter zugleich die Information, daß ein „Umwandlungsfall" vorliegt, vom Vermieter selbst übermittelt. Die Aushändigung des Merkblattes durch den anwesenden Behördenbediensteten ist dann datenschutzrechtlich zulässig.

Die zuständige Behörde kann die Mieter im Rahmen der Antragsbearbeitung (nach der Beantragung) aber auch durch ein Anschreiben mit Merkblatt informieren und um Mitteilung relevanter Tatsachen bitten, die sich noch nicht aus den Bauakten ergeben. Da die Erteilung einer Abgeschlossenheitsbescheinigung weitreichende Auswirkungen sowohl für den Vermieter als auch für den Mieter haben kann, würde die Behörde auf diese Weise in die Lage versetzt,

die Bescheinigung rechtssicher erteilen zu können. Zugleich würden die Mieter damit in sachgerechter Form von den beabsichtigten Umwandlungsvorhaben informiert werden.

Zur Klärung der Frage, unter welchen Voraussetzungen die betroffenen Mieter von der Antragstellung bzw. der Erteilung von Abgeschlossenheitsbescheinigungen informiert werden können, haben wir diese Rechtsauffassung im vergangenen Jahr den zuständigen Behörden mitgeteilt und anheimgestellt, künftig entsprechend zu verfahren. Die Baubehörde hat daraufhin eine Verwaltungsvorschrift (Fachliche Weisung BOA 1/1993 „Abgeschlossenheitsbescheinigung nach dem Wohnungseigentumsgesetz (WEG)" vom 14. April 1993) erlassen, um die Erteilung von Abgeschlossenheitsbescheinigungen insgesamt für Hamburg einheitlich zu regeln. An der Abstimmung dieser Verwaltungsvorschrift waren wir beteiligt.

Nach dieser Fachlichen Weisung wird nunmehr in allen Bezirksämtern wie folgt verfahren:

— Bei bestehenden Gebäuden ist in der Regel durch Ortsbesichtigung zu überprüfen, ob die baulichen Voraussetzungen für die Abgeschlossenheit erfüllt sind und ob die Anlage dem Aufteilungsplan entspricht.

— Dem Antragsteller ist unverzüglich mit der Eingangsbestätigung mitzuteilen, daß eine Ortsbesichtigung beabsichtigt ist und daß hierüber auch die Mieter des Gebäudes informiert werden.

— Zugleich sind die Mieter des Gebäudes in jedem Fall schriftlich darüber zu informieren, daß aus Anlaß der Beantragung einer Abgeschlossenheitsbescheinigung eine Ortsbesichtigung beabsichtigt ist. Dem Schreiben sind die Merkblätter der Baubehörde – Amt für Wohnungswesen – über die Rechte und Pflichten von Mietern und Vermietern im Falle der Umwandlung von Wohnraum beizufügen.

— Namen und Anschrift der Mieter kann die Bauprüfdienststelle ggf. vom zuständigen Einwohneramt erfragen. Dies ist gemäß § 31 Abs. 1 Hamburgisches Meldegesetz (HmbMG) datenschutzrechtlich zulässig.

— In Einzelfällen kann von der Durchführung einer Ortsbesichtigung abgesehen werden, z. B. wenn bei Würdigung aller Umstände kein Anlaß zu Zweifeln besteht, daß der vorgelegte Aufteilungsplan die tatsächlichen Gegebenheiten zutreffend wiedergibt. Bei der Sachbearbeitung ist deshalb zunächst zu prüfen, ob eine Ortsbesichtigung im konkreten Fall entfallen kann.

— Der Zugang zu den Wohnungen kann von der Bauprüfdienststelle nicht hoheitlich erzwungen werden. Es ist Sache des Antragstellers, den Zugang zu ermöglichen.

— Ist eine Ortsbesichtigung erforderlich, ist deshalb der Antragsteller aufzufordern, einen Besichtigungstermin im Einvernehmen mit der Bauprüfdienststelle und den Mietern zu benennen.

Gegen diese Verfahrensweise haben wir keine Bedenken erhoben, weil auf diese Art die Mieter frühzeitig und in datenschutzrechtlich zulässiger Form informiert und die Vermieter in ihren Rechten nicht beeinträchtigt werden.

12.3 Hamburger Mietenspiegel

Wie bereits im 11. TB (12.3) berichtet, sollte – losgelöst von der Initiative auf Bundesebene – für die Mietenspiegelerhebung 1993 eine landesrechtliche Regelung auf der Grundlage des § 2 Hamburgisches Statistikgesetz (HmbStatG) getroffen werden.

Der Senat hat von der Ermächtigungsgrundlage des § 2 Abs. 3 HmbStatG Gebrauch gemacht und mit der Mietenspiegelbefragungsverordnung vom 6. April 1993 (Hamburgisches Gesetz- und Verordnungsblatt 1993, Seiten 76, 77) eine Rechtsverordnung – ohne Auskunftspflicht – für die Erstellung des Mietenspiegels 1993 geschaffen. Anstelle dieser Verordnung wäre auch eine Regelung durch ein entsprechendes Gesetz gemäß § 2 Abs. 1 HmbStatG möglich gewesen. Ausschlaggebend für den Weg über die Rechtsverordnung war der Zeitablauf, weil mit der Mietenspiegelbefragung bereits Anfang April begonnen werden sollte.

Da der Senat Landesstatistiken durch Rechtsverordnung gemäß § 2 Abs. 3 HmbStatG nur mit einer Geltungsdauer von 3 Jahren anordnen kann, wird für jede künftige Mietenspiegelerhebung eine neue Rechtsverordnung erforderlich. Wir schlagen daher vor, daß wegen der Periodizität der Mietenspiegelaufstellung mittelfristig eine dauerhafte Regelung für den Mietenspiegel entweder auf Bundesebene oder auf Landesebene realisiert werden sollte.

Nach der Mietenspiegelbefragungsverordnung 1993 erstreckt sich die Erhebung auf eine repräsentative Auswahl von bis zu 6.600 Wohnungen, wobei die Mieter oder Vermieter dieser Wohnungen zu gleichen Teilen befragt werden.

Zur Wahrung des Rechts auf informationelle Selbstbestimmung hatten wir im 10. TB (12.2) eine Ersatzbefragung beim Vermieter im Falle der Auskunftsverweigerung des Mieters abgelehnt. Wir hatten vorgeschlagen, daß zumindest die Mieter als Hauptbetroffene über die geplante Erhebung zu informieren sind und daß ihnen ein generelles Widerspruchsrecht einzuräumen ist. Wird hiervon Gebrauch gemacht, muß auf eine Ersatzbefragung beim Vermieter verzichtet werden.

Aufgrund unserer nachdrücklichen Forderungen ist die Baubehörde unserem Vorschlag gefolgt und hat dieses auch in dem Merkblatt zum Hamburger Mietenspiegel, das den zu befragenden Mietern vor der Erhebung zugesandt wird, zum Ausdruck gebracht. Weiterhin haben wir darauf gedrungen, daß die Mieter und Vermieter zu Beginn des Interviews ausdrücklich über die Freiwilligkeit der Auskünfte und die Folgen im Falle einer Auskunftsverweigerung durch den Interviewer zu informieren sind, und daß entsprechende Anleitungen für den Interviewer im Interviewerhandbuch wiedergegeben werden.

Folgende Textpassagen wurden daraufhin für die Interviewanleitung in das Interviewerhandbuch aufgenommen:

— Die Teilnahme an der Erhebung ist freiwillig; bei Verweigerung entstehen keine Nachteile. Darüber muß die zu befragende Person zu Beginn des Interviews ausdrücklich belehrt werden. Dieser Hinweis und das Einverständnis zum Interview sind im Fragebogen festzuhalten (noch vor Frage 1). Ohne diese Bestätigung kann der Fragebogen nicht abgenommen werden.

— Im Falle einer Auskunftsverweigerung wird zwischen einer allgemeinen Ablehnung der Befragung und einer Ablehnung aus datenschutzrechtlichen Gründen unterschieden. Ist letzteres der Fall, dürfen die Daten nicht bei anderen Stellen, z.B. beim Vermieter, erhoben werden.

— Lehnt der Gesprächspartner eine Auskunft im Ganzen ab, ist er zu fragen, aus welchem Grund er die Auskunft verweigert.

— Falls der Mieter/Vermieter aus Datenschutzgründen ablehnt, ist er darauf hinzuweisen, daß die Daten beim Vertragspartner erhoben werden. Er ist dann zu fragen, ob er diese Verfahrensweise aus Datenschutzgründen ablehnt.

— Sollte ein Mieter die Datenerhebung beim Vertragspartner aus Datenschutzgründen ablehnen, muß eine dem äußeren Anschein nach gleiche Wohnung (gleiche Größe, gleiche Ausstattung usw.), die nach Möglichkeit direkt über oder direkt unter der ursprünglich zu erhebenden Wohnung liegt, vom Interviewer notiert werden. Bei diesem Mieter ist kein Interview durchzuführen.

— Bei Verweigerung von Mietern mit Hinweis auf den Datenschutz ist dies mitzuteilen und eine Ersatzwohnung zu melden.

— Sollte ein Vermieter auch eine Datenerhebung beim Vertragspartner aus Datenschutzgründen ablehnen, muß über die Verweigerung hinaus auch die weiterführende Ablehnung mitgeteilt werden.

Die Auswertungen der Mietenspiegelbefragung haben gezeigt, daß die durchschnittlichen Verweigerungsquoten sowohl aus allgemeinen Gründen (ca. 13 %) als auch aus datenschutzrechtlichen Gründen (0,5 %) im Vergleich zur Mietenspiegelerhebung 1991 nahezu konstant geblieben sind. Wir gehen daher davon aus, daß sich die vereinbarte Regelung hinsichtlich der frühzeitigen und umfassenden Information der betroffenen Mieter/Vermieter auch bei künftigen Mietenspiegelerhebungen gut bewähren wird. Von der befürchteten Beeinträchtigung oder sogar Verhinderung einer repräsentativen Mietenspiegelerhebung bei dieser datenschutzgerechten Verfahrensweise kann jedenfalls keine Rede sein.

12.4 Wohnraumdatei

Die Wohnraumkartei soll eine automatisierte Wohnraumdatei werden, damit die zweckbestimmte Nutzung von öffentlich geförderten Wohnungen nach dem

Wohnungsbindungsgesetz (WoBindG) bei den Bezirksämtern sichergestellt werden kann. Die Entwürfe der IuK-Verfahrensdokumentation und der Dienstvorschrift, die die Erteilung und Veränderung der Zugangsberechtigung zum IuK-Verfahren „Unterstützung der Aufgabenerledigung zur Sicherstellung der zweckbestimmten Nutzung der Sozialwohnungen" regeln, wurden uns zugesandt.

Dabei haben wir festgestellt, daß im Informations-Struktur-Diagramm wiederum ein Datenfeld für die Speicherung der Staatsangehörigkeit vorgesehen ist, obwohl die Baubehörde früher bereits erklärt hatte, künftig keine umstrittenen Mieterdaten in die neue Wohnraumdatei aufzunehmen (vgl. 5. TB, 5.5.3 und 7. TB, 4.8.1). Wir haben daraufhin die Baubehörde um Klarstellung gebeten, da für uns keine rechtliche Grundlage für die Erhebung dieser Information erkennbar war. Die Baubehörde hat uns mitgeteilt, daß das Datenfeld „Staatsangehörigkeit" in der neuen Wohnraumdatei entfällt.

12.5 Prüfung der Vergabe von Sozialwohnungen

Im Berichtszeitraum haben wir im Bezirksamt Eimsbüttel und in der Baubehörde – Amt für Wohnungswesen – die Verarbeitung personenbezogener Daten bei der Vergabe von Sozialwohnungen geprüft. Es handelt sich um ein nicht-automatisiertes Verfahren unter Verwendung von Akten, das eine Reihe datenschutzrechtlicher Mängel aufweist. Wir mußten Defizite in den Rechtsvorschriften, die dem Verfahren zugrunde liegen, und Organisationsmängel feststellen.

12.5.1 Rechtsvorschriften

Das Verfahren stützt sich im wesentlichen auf § 5a Wohnungsbindungsgesetz (WoBindG), worin die Landesregierungen vom Bundesgesetzgeber ermächtigt worden sind, Rechtsverordnungen für Gebiete mit erhöhtem Wohnungsbedarf zu erlassen. Daneben werden einige wenige Verfahrensregelungen für die Benennung von Wohnungsuchenden beim Verfügungsberechtigten getroffen, ohne daß die Erhebung und weitere Verarbeitung personenbezogener Daten näher bestimmt wird.

Der Senat hat von der Verordnungsermächtigung des § 5a WoBindG am 28. Juli 1970 nur begrenzt Gebrauch gemacht. Die darin getroffenen Festlegungen enthalten keine präzisen und und bereichsspezifischen Datenschutzregelungen. Deshalb sollte der Senat unverzüglich die Verordnung den verfassungs- und datenschutzrechtlichen Erfordernissen anpassen.

Im übrigen haben wir empfohlen, gemeinsam mit den anderen Bundesländern die Erfolgsaussichten zu klären, möglichst im Wohnungsbindungsgesetz die wesentlichen datenschutzrechtlichen Regelungen zu treffen. Damit würde zugleich die Rechtssicherheit erhöht, daß das Gesetz eine ausreichende Ermächtigungsgrundlage für die Rechtsverordnung darstellt. Die Baubehörde will diesen Weg weiterverfolgen.

Die zu § 5a WoBindG erlassene Fachliche Weisung W 3/83 enthält zwar grundrechtsbeschränkende Aussagen zur Datenverarbeitung, ist aber keine Rechtsnorm und scheidet damit als bereichsspezifische Regelung aus. Überdies mußten wir feststellen, daß diese Fachliche Weisung bereits nach § 5 Abs. 2 Bezirksverwaltungsgesetz mit Ablauf des 31. Dezember 1988 außer Kraft getreten und nicht durch eine Neufassung ersetzt worden ist.

12.5.2 Organisationsmängel

Von den Organisationsmängeln sollen an dieser Stelle nur die besonders schwerwiegenden erwähnt werden:

— Im Bezirksamt Eimsbüttel werden die Antragsunterlagen ungeheftet in sog. „Akten-Taschen" aufbewahrt. Dabei fanden wir neben dem Antragsformular teilweise hochsensible Belege wie z. B. ärztliche Bescheinigungen über psychische Erkrankungen, Entlassungsschein aus dem Gefängnis mit Bewährungshelferbericht, Therapieteilnahmebescheinigung eines Alkoholikers, Arztbriefe mit detaillierten Angaben über die Befunde und die Behandlungen sowie Krankenhausaufnahmebögen.

  Zum einen ist kein Erfordernis erkennbar, daß solche Unterlagen überhaupt für Zwecke der Vergabe einer Sozialwohnung zur Akte genommen werden müssen. Zum anderen ist die Sammlung dieser Unterlagen in Form loser Blätter völlig unzulänglich, weil dadurch die Vollständigkeit und die Richtigkeit des Vorgangs nicht nachvollzogen werden kann. Deshalb muß über jeden Antragsvorgang zumindest eine Akte angelegt werden, wie es in der sonstigen Leistungsverwaltung üblich ist.

— Die Sachgebiete „Anerkennung als Wohnungsnotfall" und „Wohnraumvermittlung" müssen im Bezirksamt organisatorisch und faktisch getrennt werden. An die Wohnraumvermittlungsstelle dürfen nicht weiterhin alle Informationen, die zur Anerkennung als Wohnungsnotfall geführt haben, weitergegeben werden. Vielmehr muß sich dieser Datenfluß auf die für die Wohnraumvermittlung erforderlichen Daten beschränken.

— Die Baubehörde – Amt für Wohnungswesen – ist dafür zuständig, behinderten Personen bei der Suche nach einer für sie geeigneten Wohnung behilflich zu sein. Fristen für eine Mindestaufbewahrung oder für eine Löschung der Unterlagen sind nicht festgelegt. Deshalb war es nicht verwunderlich, daß wir in einem der Aktenordner auf Fälle stießen, die vor mehr als 10 Jahren erledigt worden waren.

  Die Baubehörde vertritt hierzu die Auffassung, daß die Aufbewahrung der Unterlagen über einen längeren Zeitraum erforderlich sei, um im Falle einer Zweitvermittlung darauf zurückgreifen zu können. Wir halten es dagegen nicht für vertretbar, daß ein 10 Jahre alter Vorgang routinemäßig an einen neu eingehenden Antrag geheftet wird. Vielmehr ist vorher zu klären, welche von den seinerzeit erhobenen und gespeicherten Daten für eine Zweitvermittlung erforderlich sind.

  Zur Vermeidung eines unverhältnismäßigen Verwaltungsaufwands, der mit einer Durchsicht von 1.600 bis 1.700 Altakten nach Erforderlichkeitskriterien verbunden wäre, haben wir vorgeschlagen, diesen Aktenbestand zu sperren und in einer für die Sachbearbeitung nicht mehr zugänglichen Weise aufzubewahren. Der Zugriff auf die gesperrten Daten wäre dann nur noch in gesetzlich festgelegten Ausnahmen möglich, beispielsweise zu wissenschaftlichen Zwecken, zur Behebung einer Beweisnot oder zu Revisionszwecken. Bis zur Löschung der Akten nach einer noch zu bestimmenden Frist müßte für eine Aufbewahrung unter sicherem Verschluß Sorge getragen werden.

Unsere Gespräche mit den betroffenen Behörden über das Prüfungsergebnis waren bei Redaktionsschluß noch nicht beendet. Über das Ergebnis werden wir weiter berichten.

12.6 Repräsentativerhebung zur Vorbereitung einer sozialen Erhaltensverordnung

Der Senat hat im letzten Jahr soziale Erhaltensverordnungen für mehrere innenstadtnahe Wohngebiete beschlossen, um die dort lebenden Mieter vor drohenden Spekulationen mit Wohnraum zu schützen. Durch die Einführung eines Genehmigungsvorbehaltes bei Anträgen auf Abbruch, bauliche Veränderung oder Nutzungsänderung soll die bisherige Mieterstruktur erhalten bleiben.

Um die sozialen Erhaltensverordnungen räumlich eingrenzen und gezielt umsetzen zu können, mußten vorab detaillierte Informationen über die Wohnsituation in den betroffenen Wohngebieten erhoben werden. Hierzu wurde von der Stadtentwicklungsbehörde eine Repräsentativerhebung beim Statistischen Landesamt in Auftrag gegeben. Das Statistische Landesamt vergab die Durchführung der Erhebung wiederum an ein privates Institut. Die Repräsentativerhebung basierte auf einem standardisierten Interview, das mit speziell ausgewählten Haushalten auf freiwilliger Basis geführt werden sollte.

Das datenschutzrechtliche Problem bestand zunächst darin, daß neben statistischen Hilfsmerkmalen wie Adresse und Telefonnummer zahlreiche personenbezogene Informationen über Gebäude, Wohnungen und Haushalte, insbesondere deren Sozialstruktur, erhoben werden sollten. So war ursprünglich vorgesehen, daß der an der Wohnungstür Befragte umfangreiche Auskünfte über sämtliche im Haushalt lebenden Personen geben sollte, ohne daß deren ausdrückliches Einverständnis vorliegt. Problematisch ist diese Vorgehensweise vor allem bei Wohngemeinschaften.

Wir haben daher gefordert, lediglich Geschlecht, Geburtsjahr und Staatsangehörigkeit der im Haushalt lebenden Personen sowie deren verwandtschaftliche Stellung zum Befragten einzeln zu erheben. Weitaus sensiblere Daten wie z. B. die Höhe und Zusammensetzung des monatlichen Einkommens, der Bezug von Wohngeld, der Schulabschluß und die Stellung im Beruf sollen dagegen

nur aggregiert, d.h. je Haushalt zusammengefaßt ohne konkreten Personenbezug erfragt werden. Dieser Vorschlag wurde von der Stadtentwicklungsbehörde aufgegriffen und im Interviewer-Leitfaden entsprechend berücksichtigt.

12.7 Parlamentarischer Untersuchungsausschuß Städtische Wohnungen

Mit einem Zwischenbericht an die Bürgerschaft vom 10. Juni 1993 hat der Parlamentarische Untersuchungsausschuß zur „Klärung von politischen Verantwortlichkeiten und Untersuchungen der Geschäftstätigkeit städtischer Unternehmen im Zusammenhang mit der Verwaltung und Vermietung von Wohnungen im Eigentum der Freien und Hansestadt Hamburg oder städtischer Unternehmen" seine Arbeit beendet. Ausschlaggebend für diese Entscheidung war die vom Hamburgischen Verfassungsgericht festgestellte Ungültigkeit der Bürgerschaftswahl 1991, die die Auflösung und Neuwahl des Landesparlamentes zur Folge hatte.

Wie im 11. TB (12.5) beschrieben, hatte ich am 26. November 1992 dem Untersuchungsausschuß für die Vorlage der Akten, die die Vermietung und Unterhaltung stadteigener Wohnungen und Häuser betrafen, eine abgestufte Verfahrensweise dargelegt. Sie berücksichtigt sowohl das in der Hamburgischen Verfassung festgelegte Beweiserhebungsrecht des Ausschusses als auch die datenschutzrechtlichen Belange der betroffenen Mieter. Am 14. Januar 1993 beschloß der Parlamentarische Untersuchungsausschuß, entsprechend vorzugehen. Daraufhin wurden ihm vom Senat – mit Ausnahme der die Werkdienstwohnungen betreffenden Vorgänge – ausschließlich anonymisierte Akten vorgelegt. Dazu wurden die persönlichen Daten der Mieter geschwärzt oder durch Entnahme bestimmter Aktenbestandteile (z. B. Fotos von Häusern) unkenntlich gemacht, soweit diese Rückschlüsse auf personenbezogene Daten zuließen. Die Akten über Werkdienstwohnungen wurden dem Untersuchungsausschuß erst nach Zusicherung der ausschließlichen Behandlung in nicht-öffentlicher Sitzung übergeben.

Auch von den städtischen Wohnungsunternehmen erhielt der Untersuchungsausschuß keine Akten mit personenbezogenen Daten der Mieter. Zu zwei Beschlagnahmeanträgen des Ausschusses hatte das Amtsgericht Hamburg in einer Zwischenverfügung erhebliche verfassungsrechtliche Zweifel geäußert, weil es die Begründung nicht für ausreichend hielt. Da zur Erfüllung des Untersuchungsauftrags allenfalls die Beantwortung eines Teils der darin genannten Fragen eine namentliche Benennung bestimmter Mieter bzw. Käufer erfordere, wäre die komplette Beschlagnahme aller Akten und ihre nicht anonymisierte Herausgabe unverhältnismäßig gegenüber den vom Untersuchungsauftrag gar nicht erfaßten Personen. Zu dieser Verfügung des Gerichts, in denen die Antragsteller zu einem ergänzenden Vortrag aufgefordert worden sind, haben sie innerhalb der vorgegebenen Frist nicht mehr Stellung genommen.

Es bleibt festzuhalten, daß das verfassungsrechtlich geschützte Interesse der von dem Untersuchungsauftrag betroffenen Mieter an der Verwendung ihrer

personenbezogenen Daten in diesem Fall vorerst angemessen berücksichtigt worden ist. Die auch in der Öffentlichkeit geführte Diskussion über die Abwägung zwischen den Rechten des Parlaments und dem informationellen Selbstbestimmungsrecht der Betroffenen zeigt jedoch deutlich, daß eine verbindliche gesetzliche Regelung für Aktenvorlagen an Untersuchungsausschüsse dringend erforderlich ist (siehe 1.5.2).

13. Meldewesen

13.1 Mängelbeseitigung im Melderegister

Unsere Darstellung der wachsenden Unzuverlässigkeit des Melderegisters in Hamburg im 11. TB (13) hatte zunächst erhebliche öffentliche Aufmerksamkeit auch bei den kritisierten Behörden hervorgerufen. Zur Klärung des weiteren Vorgehens wurden mit den Beteiligten beim Senatsamt für Bezirksangelegenheiten (SfB), dem Amt für zentrale Meldeangelegenheiten im Bezirksamt Harburg (Leitstelle), der Behörde für Inneres und dem Organisationsamt die Probleme und Lösungsmöglichkeiten im Detail erörtert. Dabei wurde herausgearbeitet, welche gegenwärtigen Mängel noch im derzeitigen automatisierten Verfahren behoben werden können und welche nur mit einem neuprogrammierten Melderegister zu bereinigen sind.

13.1.1 Behebbare Mängel

Die Programmierung des Rückmeldeverfahrens, die erforderlich war, um Mitteilungen über Meldevorgänge außerhalb Hamburgs zu verarbeiten, ist abgeschlossen. Bis Ende 1993 sollen die Voraussetzungen zur Speicherung von Nachweisen über Anträge auf Reisepässe und Personalausweise abgeschlossen werden.

§ 10 Abs. 3 des Hamburgischen Meldegesetzes (HmbMG) schreibt vor, daß Daten fünf Jahre nach dem Wegzug oder dem Tod eines Einwohners, die nicht ohnehin gelöscht werden müssen, gesondert aufzubewahren und durch technische und organisatorische Maßnahmen zu sichern sind. Dies geschieht bisher nicht. Im bestehenden Verfahren sollen daher die weiterzuspeichernden Datensätze, die älter als fünf Jahre sind, mit einer Zugriffssperre versehen werden. Die Vertreter der Leitstelle und des SfB haben zugesagt, entsprechende Vorkehrungen zu treffen.

Die Leitstelle hat ferner eine detaillierte Handlungsanweisung für die Meldedienststellen über die Identifizierung von Einwohnern bei Auskunftsersuchen herausgegeben, um Verwechslungsfälle (11. TB, 13.1) zu vermeiden. Wenn gleichwohl Verwechslungen vorkommen, wird eine Auskunftssperre eingetragen, die Auskünfte an Privatpersonen verhindert und auch bei Übermittlungen an Behörden zu besonderer Achtsamkeit anhält.

13.1.2 Zur Zeit nicht behebbare Mängel

Die aus datenschutzrechtlicher Sicht wesentlichen Mängel, die im bestehenden automatisierten Melderegister nicht behoben werden können, betreffen folgende Punkte:

— Nachweisdaten

Unverzichtbare Nachweisdaten, für deren Speicherung kein Ermessensspielraum besteht, sind nach gemeinsamer Auffassung diejenigen Hinweise auf andere Verwaltungsvorgänge, die zu Änderungen von Meldedaten führen. Aus dem Bereich des Personenstandswesens sind dies z.B. Geburt, Tod, Eheschließung, Namensänderung. Hinzu kommen: gerichtliche Aktenzeichen bei Ehescheidung, Hinweise auf Einbürgerungen usw.. Derzeit werden die erforderlichen Nachweise zwar in Papierform vorgehalten, jedoch nicht im automatisierten Register gespeichert.

Nach Einschätzung des SfB wird in einem neuen Verfahren die Nacherfassung der personenstandsrechtlichen Nachweise aus Hamburg durch Übernahme der Daten aus dem EDV-Verfahren der Standesämter automatisiert sichergestellt werden können, so daß in diesem Bereich nicht mit unverhältnismäßigem Nacherfassungsaufwand zu rechnen ist. Manuell nachzuerfassen wären jedoch die personenstandsrechtlichen Nachweise von außerhalb Hamburgs und die sonstigen erforderlichen Nachweise (z.B. Ehescheidungen, Einbürgerungen).

— Mehrere Datensätze zu einem Einwohner

Wenn zu einer Person im Melderegister mehrere Datensätze gespeichert sind, was im bestehenden Verfahren in einer nicht erkennbaren Zahl von Fällen vorkommt, kann dies in der Praxis zu Fehlinterpretationen führen. Das Problem verschärft sich noch dadurch, daß sich die Fälle bei zunehmendem „Alter" des automatisierten Registers vermehren, wobei das neue Namensrecht mit einer wachsenden Zahl von Namensänderungen hinzukommt. Es wäre zur Zeit zwecklos, die Anzahl der Fälle, in denen zu einem Einwohner mehrere Datensätze gespeichert sind, im bestehenden Verfahren zu ermitteln, weil das Verfahren keine Möglichkeit vorsieht, inaktuelle Daten im aktuellen Datensatz nachzutragen und somit die verschiedenen Datensätze zusammenzuführen. Eine manuelle Bereinigung scheidet daher derzeit aus. Es wurde auch keine Möglichkeit gesehen, einen besonderen Hinweis auf einen weiteren Datensatz zur selben Person anzubringen, da dies sehr fehleranfällig wäre und zu erneuten Fehlinterpretationen führen würde.

Nach Auffassung der Beteiligten wird dieser Bereich bei der Einführung eines neuen EDV-Verfahrens erhebliche Probleme aufwerfen, da vermieden werden muß, daß der derzeitige Mangel sich bei der Datenübernahme auf das neue Register überträgt.

— Ordens- und Künstlernamen

Diese Angaben können nicht gespeichert werden, obwohl das Melderecht des Bundes und Hamburgs dies vorschreibt. Aus Sicht des SfB als programmierender Stelle ist eine Erweiterung des bestehenden Verfahrens um die entsprechenden Datenfelder nicht leistbar, da die technischen Folgeänderungen z.B. bei regelmäßigen Übermittlungen nicht übersehbar seien.

Als vorläufiger Ausweg wurde eine Hilfsdatei für diese Fälle erörtert. Von den beteiligten Behörden wurde dieser Weg als nicht praktikabel verworfen; es sei nicht zu erwarten, daß im Alltagsbetrieb der Meldedienststellen in allen Fällen ein Abgleich mit dieser Datei erfolge, wenn die Fälle insgesamt verhältnismäßig selten sind. Die rechtlich gebotene Speicherung der Ordens- und Künstlernamen kann demnach erst im neuen Verfahren vorgenommen werden.

13.1.3 Stand der Verfahrensneuentwicklung

SfB und Leitstelle haben mit den vorbereitenden Arbeiten begonnen. Die Informationsstrukturanalyse für das neue Verfahren ist im Entwurf fertiggestellt.

Das SfB teilte mit, daß die Neuentwicklung des Verfahrens mit hoher Priorität verfolgt werde. Seit Anfang 1993 stehen für die vorbereitenden Arbeiten dauerhaft 2,5 Kräfte zur Verfügung, die durch IuK-Trainees und Regierungsräte zur Anstellung ergänzt werden. Mit einem Schreiben an die Amtsleiter des SfB, des Organisationsamtes und der Behörde für Inneres habe ich um Unterstützung dieser Bereitschaft zur Behebung der bestehenden Mängel durch entsprechende personelle und materielle Absicherung des Projekts gebeten. Ich habe für die Entscheidungen zum Stellen- und IuK-Plan 1994 darauf hingewiesen, daß die gesetzlichen Vorgaben des Melderechts nicht disponibel sind und entsprechende Anträge der zuständigen Behörden Priorität genießen müssen. Das SfB hat mitgeteilt, daß das Vorhaben für ein neues automatisiertes Melderegister für den IuK-Plan 1995–97 angemeldet worden ist. In der Zwischenzeit sollen die erforderlichen Vorarbeiten erfolgen, so daß man damit rechnet, das neue Verfahren bis 1997 einführen zu können.

13.2. Novellierung des Hamburgischen Meldegesetzes (HmbMG)

13.2.1 Noch kein neuer Sachstand

Da die Neuentwicklung des automatisierten Melderegisters insbesondere auch abhängig ist von den Vorgaben des Hamburgischen Meldegesetzes, sollte seitens der Behörde für Inneres (BfI) bis zu den Entscheidungen von Senat und Bürgerschaft über die Mittel für die Verfahrensneuentwicklung eine Klärung zur Novellierung des Melderechts erfolgen. Hierzu ist es aus mehreren Gründen nicht gekommen.

Zum einen ist das Hamburgische Meldegesetz abhängig vom Melderechtsrahmengesetz (MRRG). Der Entwurf des Bundes zur Änderung des Rahmenrechts ist jedoch seit dem Entwurf von 1992, der im Vergleich zum Entwurf von 1990 (9. TB, 4.9.1) im wesentlichen unverändert geblieben ist, nicht vorangekommen.

Die für Hamburg im Entwurf der Bfl zusätzlich vorgesehene grundlegende Veränderung der Aufgabenverteilung der Meldebehörden (überörtliche Zuständigkeiten der örtlichen Meldebehörden; 9. TB, 4.9.2., 10. TB, 13.1.1) war zwar nicht abhängig vom Melderechtsrahmengesetz, stand jedoch im engen Zusammenhang mit den Überlegungen zur Verwaltungsreform. Eine Richtungsentscheidung des Senats, die sich für die Konzeption der Bfl zur überörtlichen Zuständigkeit der Einwohnerämter in den Bezirken aussprach, konnte wegen der vorzeitig beendeten Legislaturperiode der Bürgerschaft nicht mehr umgesetzt werden. Über das Stadium des Entwurfs der Bfl vom Januar 1993 ist die Novellierung daher nicht hinausgelangt.

13.2.2 Übermittlung von Meldedaten an Parteien

Wie notwendig eine Gesetzesänderung gewesen wäre, hat sich allerdings vor den Wahlen vom 19. September 1993 gezeigt.

Das Hamburgische Meldegesetz sieht in § 35 vor, daß Parteien zum Zwecke der Wahlwerbung Adressen rechtmäßigerweise übermittelt bekommen können. Für die Zusammensetzung der entsprechenden Listen ist das Lebensalter der betroffenen Wahlberechtigten entscheidend (z. B. Erst- und Jungwähler; Wahlberechtigte über 60 usw.). Die Geburtstage der Wahlberechtigten dürfen dabei nicht mitgeteilt werden. Die Daten dürfen nur zum Zwecke der Werbung zur anstehenden Wahl gebraucht werden, nicht jedoch zur wahlunabhängigen Interessentenwerbung oder gar zum Adressenhandel.

Aus datenschutzrechtlicher Sicht ist die derzeitige gesetzliche Regelung zu kritisieren. Die Datenschutzbeauftragten des Bundes und der Länder setzen sich seit langem dafür ein, daß den Bürgern zumindest ein Widerspruchsrecht eingeräumt wird (10. TB, 13.1.3). Dann würden die Anschriften von Wahlberechtigten, die im Vorwege widersprochen haben, nicht an Parteien herausgegeben werden. In acht Bundesländern gibt es bereits ein derartiges Widerspruchsrecht. Auch im Entwurf für eine Änderung des Hamburgischen Meldegesetzes war ein solches Widerspruchsrecht vorgesehen. Weil er nicht verabschiedet wurde, hatten die Wahlberechtigten keine gesetzlich abgesicherte Möglichkeit, der Herausgabe ihrer Anschriften an Parteien zu widersprechen.

Von dem Recht nach § 35 des Hamburgischen Meldegesetzes haben anläßlich der Wahl vom 19. September 1993 mehrere Parteien Gebrauch gemacht. Sofern die formellen Voraussetzungen erfüllt waren, war die Meldebehörde gesetzlich und insbesondere nach dem Grundsatz der Gleichbehandlung verpflichtet, Anschriften über Wahlberechtigte an alle zur Wahl antretenden Parteien unabhängig von deren politischer Ausrichtung antragsgemäß herauszugeben.

Zu diesem Thema wurden in den Wochen vor der Wahl mehr Beschwerden von Bürgern an uns gerichtet, als zu irgend einem anderen Datenschutzproblem seit der Volkszählung von 1987. Die Betroffenen äußerten ihr Befremden darüber, daß trotz des Datenschutzes die Herausgabe von detaillierten Adressenlisten aus dem Melderegister gleichsam als Selbstverständlichkeit angesehen wird. Wir konnten sie lediglich auf die geltende Rechtslage und die Erwartung, daß das Widerspruchsrecht hoffentlich in Zukunft eingeführt wird, hinweisen.

Die Erfahrungen anläßlich der letzten Wahl haben deutlich gemacht, daß das im Meldegesetz verankerte Vorrecht der Parteien grundsätzlich überdacht werden sollte. Die bisher erwogene Widerspruchsmöglichkeit stellt aus Sicht des Datenschutzes lediglich die zweitbeste Lösung dar. Die Widerspruchslösung verhindert die Weitergabe der Meldedaten nur, wenn die Bürger von sich aus aktiv werden, um den Widerspruch eintragen zu lassen.

Für die Weitergabe der Daten bedürfte es jedoch eigentlich in allen Fällen einer selbständigen Rechtfertigung, die mehr besagt, als daß die Betroffenen nicht widersprochen haben. Zu berücksichtigen ist, daß bereits die Meldepflicht einen Eingriff in das Grundrecht auf Datenschutz darstellt, der nur im überwiegenden Allgemeininteresse gerechtfertigt ist. Die Weitergabe von Meldedaten ist ein weiterer Grundrechtseingriff, der ebenfalls einer Begründung durch das überwiegende Interesse der Allgemeinheit bedarf.

Das Parteieninteresse an Wahlwerbung kann für sich betrachtet den Grundrechtseingriff nur rechtfertigen, wenn alle Parteien, die Adressenlisten anfordern und verwenden, hierbei zugleich im überwiegenden Allgemeininteresse handeln.

Ob dies immer der Fall ist, muß allerdings angesichts der Praxis einer Partei bei der letzten Bürgerschaftswahl kritisch hinterfragt werden:

Der Antrag der DVU bezog sich gezielt auf die Jungwähler (18–25 Jahre) einer Reihe von Ortsteilen. Ortsteile in Hamburg sind überschaubare, durch wenige Straßenzüge abgegrenzte Einheiten. Die betroffenen Ortsteile waren offenbar nach dem Kriterium ausgewählt, ob es sich um sog. soziale Brennpunkte handelte: z. B. in großen Wohnsiedlungen mit erhöhter Arbeitslosigkeit, teilweise hohem Ausländeranteil und auch überdurchschnittlichen Stimmenanteilen für rechtsradikale Parteien bei vergangenen Wahlen.

Mit dem – melderechtlich vorgeschriebenen – zusätzlichen Kriterium der Altersstruktur erhielt die Partei damit eine Auswertung aus dem Melderregister, die dem Ergebnis einer Rasterfahndung nahekommt. Welches Potential eine derartige Auswertung in sich birgt, kann man sich vorstellen, wenn man die erschreckende Zunahme fremdenfeindlicher Tendenzen gerade unter jungen Menschen aus sogenannten sozialen Brennpunkten berücksichtigt.

Ursprünglich hatte die Partei sogar nur die Adressen von männlichen Wahlberechtigten verlangt, was nach dem Meldegesetz nicht zulässig war und daher abgelehnt wurde. Nachdem auf dieses Kriterium verzichtet wurde, gab es keine Handhabe mehr gegen die Auslieferung der Adressen.

Die präzise Auswertbarkeit wäre nur dann vermeidbar gewesen, wenn die Meldebehörde mehr Adressen geliefert hätte, als verlangt waren (z.B. sämtliche Jungwähler von ganzen Bezirken). Dies wäre nicht nur mangels entsprechendem Antrag unzulässig, sondern sicherlich auch nicht im Interesse der Betroffenen gewesen. Die Adressen wurden antragsgemäß in Form von Adreßaufklebern nach München an den Sitz des Vorsitzenden der Partei geliefert. Adressaten von Werbeschreiben der Partei teilten uns jedoch mit, daß die Schreiben, die sie erhielten, in Freiburg oder der Umgebung von Freiburg abgestempelt waren.

Angesichts dieser Erfahrungen sollte der Gesetzgeber im Rahmen der anstehenden Novellierung des Hamburgischen Meldegesetzes sorgsam abwägen, ob er nach wie vor überwiegende Interessen der Allgemeinheit bejaht, wenn es um die Frage geht, ob Parteien Adressen aus dem Melderegister erhalten können. Die Alternative wäre, wegen überwiegender Interessen der betroffenen Bürger die bisherige Regelung in § 35 HmbMG ganz zu streichen. Eine grundgesetzliche Pflicht für den Gesetzgeber, den Parteien den Zugang zu Meldedaten einzuräumen, gibt es nicht. Vielmehr muß der Gesetzgeber beachten, daß Beschränkungen des Rechts auf informationelle Selbstbestimmung laut Bundesverfassungsgericht nur vertretbar sind, soweit sie zum Schutz öffentlicher Interessen unerläßlich sind.

Wir haben der Behörde für Inneres diese Bedenken aufgrund der Erfahrungen bei der letzten Bürgerschaftswahl mitgeteilt. Sie hat daraufhin die für Melderegisterauskünfte zuständigen Bezirksämter aufgefordert, bis zur Klärung dieser Frage im neuen Hamburgischen Meldegesetz keine Adressen an Parteien zum Zwecke der Wahlwerbung mehr herauszugeben. Dies hat das Oberverwaltungsgericht Münster in einem Beschluß vom 23. Mai 1989 für zulässig erklärt, wenn der Grundsatz der Gleichbehandlung eingehalten wird und damit alle Anträge von Parteien auf Melderegisterauskünfte abgelehnt werden. Nach diesem Beschluß kann das Recht auf informationelle Selbstbestimmung der betroffenen Bürger die Ermessensentscheidung der Meldebehörde rechtfertigen, gar keine Adressen an die Parteien herauszugeben. Die Regelung der Behörde für Inneres ist angesichts der im Jahr 1994 anstehenden Wahlen zum Europaparlament und zum Deutschen Bundestag sehr zu begrüßen.

Den Parteien verbleibt auch nach Wegfall der Melderegisterauskünfte immer noch die Möglichkeit zur unadressierten Wahlwerbung, mit der grundsätzlich alle Bürger ohne eine derart gezielte Auswahl erreicht werden können. Wer auch unadressierte Werbung nicht erhalten will, kann dies durch Annahmeverweigerung verhindern (siehe 22.1).

14. Standesamt

14.1 Auskunft aus Personenstandsbüchern zu wissenschaftlichen Zwecken

Häufig beschweren sich Bürger auch bei uns darüber, daß ihnen vom Standesamt verwehrt wird, Auskunft aus Personenstandsbüchern (Geburtenbuch, Familienbuch, Sterbebuch) über Familienangehörige zu erhalten, die bereits vor Jahrzehnten verstorben sind. Die Daten sollen zur privaten Ahnenforschung, also z.B. zur Erstellung eines Familienstammbaums, verwendet werden. Die Rechtslage in diesen Fällen ist eindeutig:

Das Personenstandsgesetz (PStG) regelt Art und Umfang der Anlegung und Führung der Personenstandsbücher durch die Standesbeamten. Nach § 61 Abs. 1 Satz 1 PStG kann Einsicht oder Auskunft in die Personenstandsbücher nur von Behörden im Rahmen ihrer Zuständigkeit und von Personen verlangt werden, auf die sich der Eintrag bezieht, sowie von deren Ehegatten, Vorfahren und Abkömmlingen. Dies bedeutet, daß kein entsprechender Anspruch geltend gemacht werden kann, wenn es sich nicht um direkte Vorfahren handelt.

Nach § 61 Abs. 1 Satz 3 PStG haben andere Personen – also z.B. Verwandte außerhalb der geraden Linie – nur dann ein Recht auf Einsicht bzw. Auskunft, wenn sie ein rechtliches Interesse glaubhaft machen. Ein rechtliches Interesse liegt dann vor, wenn die Kenntnis der Eintragungen in Personenstandsbüchern zur Verfolgung von Rechten oder zur Abwehr von Ansprüchen erforderlich ist, z.B. in Erbschaftsangelegenheiten. Die ständige Rechtsprechung der hiermit befaßten Gerichte zählt das Interesse an der Familienforschung nicht zu den rechtlichen Interessen.

Dabei läßt sich nicht übersehen, daß die Gefahr der Beeinträchtigung von Persönlichkeitsrechten dann als sehr gering zu veranschlagen ist, wenn die verzeichneten Personen bereits vor Jahrzehnten verstorben sind. Der Schutz dieser Personen ist jedoch nicht der einzige Zweck der Regelung. Vielmehr nimmt sie eine Abgrenzung vor zwischen den Pflichten der Standesbeamten und den Rechten der Bürger, Personenstandbücher zu nutzen. Im Vordergrund stehen dabei die Rechte der unmittelbar Betroffenen, ihrer direkten Verwandten und von Personen, deren Rechte von Personenstandsbüchern abhängen. Diese Rechte muß der Standesbeamte unverzüglich erfüllen; er würde pflichtwidrig handeln, wenn er andere Anliegen berücksichtigen würde, die nicht rechtlich begründet sind.

Insofern dient § 61 PStG auch dem Datenschutz. Es geht bei datenschutzrechtlichen Vorschriften nicht allein darum, personenbezogene Angaben möglichst weitgehend von fremder Kenntnisnahme abzuschotten. Sehr häufig ist es vielmehr Zweck von datenschutzrechtlichen Regelungen, den Berechtigten den Zugang zu „ihren" Daten zu verschaffen, was in der Praxis oft nur möglich ist, wenn andere von diesem Zugang ausgeschlossen werden. Bei dieser Unter-

scheidung zwischen berechtigten und anderen Auskunftsersuchen muß auch berücksichtigt werden, daß Standesbeamte ständig eine Vielzahl von Geburten, Eheschließungen und Sterbefällen beurkunden und die entsprechenden Auskünfte usw. erteilen müssen. Sie sind hierbei in jedem Fall für die Genauigkeit und Richtigkeit der einzelnen Vorgänge verantwortlich.

Die Unterscheidung zwischen berechtigten und anderen Auskunftsverlangen kann selbstverständlich nicht nach Gutdünken vorgenommen werden. Vielmehr ist der Gesetzgeber berufen, die Grenzen zu ziehen. Nach geltendem Recht ist daher die Ablehnung von Auskunftsersuchen zum Zwecke der Familienforschung ohne ein rechtliches Interesse nach § 61 PStG unvermeidlich.

Nach einem Vorentwurf des Bundesminster des Innern zur Änderung des Personenstandsgesetzes aus dem Jahr 1989 war vorgesehen, ein Recht auf Auskunft über Eintragungen zu Personen einzuräumen, die vor mindestens dreißig Jahren gestorben oder vor 120 Jahren geboren sind, wenn ein berechtigtes Interesse glaubhaft gemacht wird. Zu den berechtigten Interessen kann im Unterschied zum rechtlichen Interesse durchaus auch die Familienforschung gehören. Ob und wann diese Regelung des Entwurfs tatsächlich vom Bundesgesetzgeber verabschiedet wird, läßt sich nicht absehen.

Während bei der Frage der privaten Familienforschung lediglich das private Interesse in Frage steht, kann es bei anderen Forschungsvorhaben durchaus auch um öffentliche Interessen gehen, die sich nach geltendem Personenstandsgesetz nicht befriedigend beantworten lassen. So wurde uns folgender Sachverhalt geschildert:

Ein Hamburger Bürger beabsichtigte, eine Biographie seiner früheren Lehrerin zu schreiben, die 1941 aus Hamburg deportiert und 1942 in einem Vernichtungslager ermordet worden war. Diese Biographie sollte einen Beitrag zur öffentlichen Ehrung der Lehrerin in ihrer früheren Schule leisten. Von besonderem Interesse für die Biografie waren insbesondere Angaben zur Religionszugehörigkeit und zur Eheschließung der Lehrerin. Der Antrag auf entsprechende Auskunft aus den Personenstandsbüchern wurde abgelehnt, weil der Autor der Biografie weder in gerader Linie mit der Lehrerin verwandt war, noch zivilrechtliche Interessen geltend machte.

Wir haben demgegenüber darauf hingewiesen, daß die in Art. 5 Abs. 3 Satz 1 Grundgesetz verbürgte Forschungsfreiheit ein Recht ist, das Ansprüche begründen kann. Auch wenn das Grundrecht nicht den unmittelbaren Zugang zu amtlichen Unterlagen gewährleistet, ist dennoch abzuwägen, ob die von § 61 Personenstandsgesetz geschützten Rechte tatsächlich Vorrang vor dem Forschungsinteresse haben. Wir haben keine Bedenken dagegen vorgebracht, die Auskunft gestützt auf die grundgesetzlich gewährleistete Forschungsfreiheit als einem rechtlichen Interesse im Sinne des Personenstandsgesetzes zu erteilen.

Die für die Aufsicht über die Standesämter zuständige Behörde für Inneres verwies dagegen auf eine Entscheidung des Landgerichts Frankenthal von 1985. Das Gericht hatte einer Universität die Einsichtnahme in Personenstandsbücher für ein konkretes Forschungsprojekt verwehrt, da § 61 PStG nur die Durchsetzung oder Abwehr von zivilrechtlichen Ansprüchen als rechtliche Interessen anerkenne. Ob diese Auffassung der Bedeutung der Forschungsfreiheit entspricht, mag dahinstehen. Jedenfalls ist dem Gericht zuzustimmen, daß die Frage, inwieweit wissenschaftliche Forschung die Benutzung von Personenstandsbüchern rechtfertigt, dringend vom Gesetzgeber beantwortet werden muß. Dies ist in dem genannten Vorentwurf von 1989 in einem neuen § 61b PStG vorgesehen. Beließe man es bei der derzeitigen Regelung, die für wissenschaftliche Vorhaben sehr restriktiv ist, bestünde die Gefahr, daß der Datenschutz der in Personenstandsbüchern Verzeichneten zu einem rein formalen, inhaltlich aber nicht mehr begründbaren Argument zur Verweigerung von Auskünften degeneriert. Hiermit wäre weder den Betroffenen noch dem Datenschutz selbst gedient.

15. Ausländerangelegenheiten

15.1 Automation der Ausländerverwaltung

Das Projekt „Automation des Ausländer- und Asylwesens" (PAULA) konnte entgegen der ursprünglichen Planung 1993 nicht zum Abschluß gebracht werden. Die Einführung des Verfahrens in den neuen Gebäuden der Ausländerbehörde ist nunmehr bis Mitte 1994 vorgesehen.

Ein zentrales Problem bei der Einführung ist die Bereitstellung eines Grunddatenbestandes aller im Zuständigkeitsgebiet der Behörde lebenden Ausländer. Um eine zeitaufwendige manuelle Datenerfassung zu vermeiden, ist geplant, diesen Grunddatenbestand durch einen Abgleich zwischen dem Melderegister und dem Ausländerzentralregister zu erstellen. Allerdings muß nach den Erfahrungen der Berliner Ausländerbehörde, die diesen Weg bereits beschritten hat, mit einer beträchtlichen Fehlerquote von ca. 30 bis 40 % bei diesem Abgleich gerechnet werden. Dies wären ca. 75.000 bis 100.000 Datensätze von Ausländern, die in Hamburg mit erstem Wohnsitz gemeldet sind.

Um von verläßlichen Prognosen ausgehen zu können, ist deshalb ein Test durchgeführt worden. Grundsätzlich dürfen Tests nur mit besonderen, nicht auf Personen beziehbaren Testdatenbeständen durchgeführt werden. Wir haben in diesem Fall jedoch anerkannt, daß es sich um eine Ausnahme handelt, und der Durchführung dieses Tests mit Echtdaten zugestimmt. Verfremdete Testdaten könnten keine Antwort auf die Frage liefern, ob die beiden Datenbestände aus dem Melderegister und dem Ausländerzentralregister tatsächlich zueinander passen.

Wir haben allerdings Wert darauf gelegt, daß bei dem Test und der Auswertung der Erfahrungen aus Berlin insbesondere auch geklärt wird, in welchen Berei-

chen die Fehler auftreten. Das Projekt geht bisher davon aus, daß einzelne Datensätze gar nicht oder nicht vollständig eingegeben werden (z. B. Person A ist zutreffend erfaßt, es fehlen aber Daten zum Aufenthaltsstatus).

Dies würde einen erheblichen Nacherfassungsaufwand bei der Ausländerbehörde auslösen. Dadurch würden – zumindest in der Anfangsphase – die mit dem Projekt verbundenen Erwartungen in Frage gestellt, daß das automatisierte Verfahren tatsächlich zu einer wesentlichen Arbeitserleichterung führt.

Gravierende datenschutzrechtliche Probleme würden sich jedoch zusätzlich dann ergeben, wenn sich im Rahmen des Tests herausstellt, daß durch den Abgleich zwischen Melderegister und Ausländerzentralregister Datensätze falsch zugeordnet werden (z. B. Person A mit dem aufenthaltsrechtlichen Status der Person B). Wenn dies in einer relevanten Anzahl der Fälle das Ergebnis des Abgleichs wäre und diese Fälle nur mit erheblichem Aufwand zu bereinigen wären, müßte aus datenschutzrechtlicher Sicht der Übernahme der Datenbestände durch einen Abgleich, der zu Falschspeicherungen führt, widersprochen werden.

15.2 Übermittlungen von Sozialdienststellen an die Ausländerbehörde

15.2.1 Rechtliche Ausgangssituation

Im 9. TB (4.10.1) war die Problematik der Übermittlungspflichten anderer Stellen an die Ausländerbehörde geschildert worden, die durch das Ausländergesetz von 1990 (AuslG) eingeführt worden waren. § 76 Abs. 2 AuslG schreibt vor, daß öffentliche Stellen die Ausländerbehörde unverzüglich zu unterrichten haben, wenn sie Kenntnis von einem Ausweisungsgrund erhalten. Ein Ausweisungsgrund kann nach § 46 Nr. 6 AuslG auch der Bezug von Sozialhilfe sein. In § 71 Abs. 2 SGB-X wird die Durchbrechung des Sozialgeheimnisses zur Erfüllung dieser Mitteilungspflichten an die Ausländerbehörde zugelassen.

Zur Eingrenzung dieser äußerst weitgehenden Übermittlungspflichten sahen die von der zuständigen Behörde für Inneres 1991 herausgegebenen Anwendungshinweise vor, daß es einer Mitteilung über Sozialhilfebezug dann nicht bedarf, wenn die Sozialhilfe nur als Vorschuß für einen anderen Leistungsträger (z. B. die Bundesanstalt für Arbeit) erbracht wird. Sozialhilfeleistungen, die zur Behebung einer vorübergehenden Notlage für nicht länger als 6 Monate erbracht werden, werden nur dann mitgeteilt, wenn sich die Betroffenen mit einem Besuchervisum hier aufhalten. Über den Bezug zur Hilfe in besonderen Lebenslagen ist die Ausländerbehörde nur dann zu unterrichten, wenn es sich um Dauerleistungen handelt oder die Summe der Hilfen 10.000 DM übersteigt. Eine Unterrichtung der Ausländerbehörde unterbleibt, wenn gegenüber dem Sozialamt nachgewiesen wird, daß der Betroffene im Besitz einer Aufenthaltsberechtigung oder einer unbefristeten Aufenthaltserlaubnis oder einer EG-Aufenthaltserlaubnis ist. Dies gilt auch für minderjährige Ausländer, wenn ihre Eltern über den verfestigten Aufenthaltsstatus verfügen (10. TB, 14.2).

Diese Regelungen wurden auch in einen Entwurf für eine Fachliche Weisung der Behörde für Arbeit, Gesundheit und Soziales zum Sozialdatenschutz aufgenommen, die allerdings noch nicht in Kraft gesetzt worden ist.

15.2.2 Prüfungsergebnisse

Wir haben uns durch eine Prüfung der Mitteilungspraxis einen Eindruck von dem Informationsfluß zwischen Sozialamt und Ausländerbehörde verschafft.

Zunächst haben wir beim Sozialamt Hamburg Mitte insgesamt 31 Akten von ausländischen Sozialhilfebeziehern eingesehen. In keinem der Fälle war eine besondere Zuständigkeit für Asylbewerber beim Sozialamt begründet. Anschließend haben wir eine Gegenkontrolle in der Ausländerbehörde vorgenommen. Hierbei wurden allerdings zu acht Personen, über die Sozialhilfeakten eingesehen worden waren, keine Akten aufgefunden. Andererseits erstreckte sich die Einsicht teilweise auch auf Ausländerakten von Angehörigen der Anspruchsinhaber beim Sozialamt, über die dort nur eine gemeinsame Akte geführt wird.

Lediglich in fünf Fällen ließ sich aufgrund der Sozialhilfeakten feststellen, daß Übermittlungen erfolgt sind. In den überprüften Akten bei der Ausländerbehörde fanden sich darüber hinaus keine weiteren Hinweise über entsprechende Mitteilungen.

In einem Fall war ein sog. de-facto-Flüchtling betroffen, der wegen Sozialhilfebezugs nicht ausgewiesen werden kann. Eine Mitteilung über den Sozialhilfebezug war somit nicht zulässig. Vom Sozialamt wurde dieser Fall mit Unsicherheiten beim Vollzug der Übermittlungsregelungen erklärt. Ein anderer Fall betraf eine EG-Angehörige. Er ließ sich nicht zweifelsfrei aufklären, weil die Akte nach unserer Prüfung beim Sozialamt nicht mehr auffindbar war.

Bis auf diese Fälle bestanden nach Maßgabe der Vorschriften des AuslG und der hierzu ergangenen Anwendungshinweise keine gundsätzlichen Bedenken gegen die Übermittlung der Tatsache des Sozialhilfebezugs. Es handelte sich um die Gewährung von laufender Hilfe zum Lebensunterhalt an Personen ohne verfestigten Aufenthaltsstatus (höchstens befristete Aufenthaltsgenehmigung).

Soweit Akten bei der Ausländerbehörde vorgefunden wurden, fiel allerdings auf, daß die nach den Vorschriften zulässigen Mitteilungen durch das Sozialamt für die ausländerrechtlichen Entscheidungen ohne Bedeutung waren. Die Aufenthaltsgenehmigungen wurden auch nach den Mitteilungen verlängert.

Zweifel an der sachlichen Erforderlichkeit der Mitteilungen kommen auch auf, wenn man den Ablauf der Mitteilungen, so wie er sich aus den Akten ergab, nachvollzieht:

Üblicherweise wird die Mitteilung vom Sozialamt an die Ausländerbehörde dadurch dokumentiert, daß in der Sozialhilfeakte ein vorgedruckter Aufkleber angebracht wird, auf dem mit Datumsangabe vermerkt ist, daß eine „Mitteilung

nach §§ 46, 76 Ausländergesetz" an das Einwohner-Zentralamt abgesandt wurde. In den entsprechenden Akten selbst fand sich keine Durchschrift von einer derartigen Mitteilung, so daß auch nicht nachvollziehbar ist, was im einzelnen mitgeteilt wurde.

Der von den Sozialämtern für die Mitteilungen entwickelte Vordruck wurde von uns lediglich in einer Ausländerakte wiedergefunden. Er war allerdings weder datiert, noch unterschrieben. Auch weiterer Schriftwechsel zwischen Sozialamt und Ausländerbehörde, der aus den Sozialamtsakten ersichtlich war, ließ sich in den entsprechenden Akten der Ausländerbehörde nicht nachvollziehen.

Andererseits wurden diverse handschriftliche Vermerke teilweise in zeitlichem Zusammenhang mit der Versendung von Mitteilungen durch das Sozialamt in den Ausländerakten aufgefunden. Somit war unklar, ob aus Sicht der Ausländerbehörden die Mitteilungen über den Sozialhilfebezug zur eigenen Aufgabenerfüllung erforderlich waren oder nicht. Wenn sie nicht als erforderlich angesehen wurden, stellt sich die Frage nach dem Sinn der handschriftlichen Vermerke. Wenn sie für erforderlich gehalten wurden, wäre auch die Dokumentation der Originalmitteilungen notwendig gewesen.

Das Sozialamt Mitte teilte aufgrund der Prüfung mit, daß Übermittlungen in Zukunft nur noch auf ausdrückliche Ersuchen der Ausländerbehörde erfolgen sollten. Der Vordruck werde daher nicht mehr benutzt. In diesem Sinne war auch die Stellungnahme der Ausländerbehörde zu verstehen, die ebenfalls nur auf Ersuchensfälle einging. Die Behörde für Arbeit, Gesundheit und Soziales (BAGS) teilte daraufhin jedoch mit, daß es eine Vorgabe, die sogenannten Spontanmitteilungen nach § 76 Abs. 2 AuslG einzustellen, nicht gebe. Das Bezirksamt Hamburg Mitte habe die Spontanmitteilungen offenbar eingestellt, da Aufenthaltsentscheidungen der Behörde für Inneres (Bfl) häufig ohne Berücksichtigung der Mitteilungen der Sozialhilfedienststellen erfolgten. Hierzu hat die Bfl der BAGS inzwischen mitgeteilt, daß die Defizite im Verwaltungsvollzug durch Einführung des Automationsvorhabens PAULA vermieden werden könnten.

Ob sich diese Erwartung bestätigt, bleibt abzuwarten. Jedenfalls hat sich unsere Einschätzung im 9. TB (4.10.1) bestätigt, daß die gesetzlich vorgeschriebenen Mitteilungen von der Ausländerbehörde kaum verarbeitet werden könnten.

Auch nach der Einführung des Automationsvorhabens in der Ausländerbehörde sollte daher die Übermittlung auf Ersuchen der Ausländerbehörde die Regel sein. Spontanmitteilungen sollten nur dann erfolgen, wenn aus Sicht der Sozialämter Mißbrauchsfälle offensichtlich sind.

16. Straßenverkehr

16.1 Führerscheineignung und Drogenkonsum

Aufgrund einer Eingabe haben wir folgenden Sachverhalt mit der Behörde für Inneres erörtert:

Der Petent hatte 1993 bei einem Polizeirevier Strafanzeige wegen einer Sachbeschädigung an seinem Fahrzeug gestellt. Einige Zeit später erhielt er Post von der Landesverkehrsverwaltung.

Die Führerscheinstelle forderte ihn auf, ein amtsärztliches Gutachten über seine Eignung zum Führen eines Kraftfahrzeugs beizubringen. Zur Begründung wurde in dem Bescheid ausgeführt, daß der Landesverkehrsverwaltung ein Bericht des Polizeireviers, bei dem der Petent die Anzeige erstattet hatte, vorliege. Daraus gehe hervor, daß er überprüft worden sei. Der Bericht des Polizeireviers über den Petenten, der noch am selben Tag unmittelbar nach der Anzeigeerstattung abgefaßt wurde, enthielt die Feststellung, daß der Petent als Konsument von Drogen bekannt sei, eine Verkehrsstrafanzeige jedoch nicht gefertigt worden sei. Die Führerscheinstelle teilte weiter mit, ihre eigenen Ermittlungen hätten ergeben, daß er mit Urteil aus dem Jahr 1986 wegen unerlaubten Besitzes von Haschisch verurteilt worden sei. Das Urteil lautete auf eine Geldstrafe von 10 Tagessätzen. Bei einer Vernehmung im Jahr 1985 habe er angegeben, seit ca. 1975 Haschisch konsumiert zu haben. Weiterhin habe er zugegeben, daß er bereits als Lehrling – ca. 1975 – mit Drogen zu tun gehabt hätte.

1. Hierbei stellte sich zunächst die Frage, ob die Verurteilung von 1985 und die dem Urteil zugrundeliegenden Angaben aus Vernehmungen dem Petenten zulässigerweise entgegengehalten werden durften. Nach § 46 Bundeszentralregistergesetz (BZRG) war die Eintragung im Bundeszentralregister nach Ablauf von 5 Jahren – also bereits 1991 – zu tilgen. § 52 Abs. 2 BZRG läßt die Verwertung von zu tilgenden Eintragungen in einem Verfahren zur Erteilung der Fahrerlaubnis nur dann zu, wenn zugleich eine Eintragung im Verkehrszentralregister erfolgt ist. Dies war nicht der Fall; die Verurteilung durfte also nicht mehr verwertet werden.

Die unklare Formulierung aus dem Polizeibericht, der Petent sei als Drogenkonsument bekannt, bedeutete tatsächlich, daß er im polizeilichen Auskunftssystem POLAS mit der sog. kriminologischen Kurzbezeichnung „BTM" gespeichert war. Der zuständige Polizeibeamte hatte also nach Entgegennahme der Anzeige zunächst einmal eine POLAS-Abfrage über den Anzeigenerstatter vorgenommen und das Ergebnis der Landesverkehrsverwaltung mitgeteilt.

In der Stellungnahme zur Eingabe wurde uns mitgeteilt, der Petent habe bei Erstattung seiner Anzeige den Eindruck gemacht, unter Drogen zu stehen. Nähere Feststellungen, ob dies tatsächlich der Fall war, wurden bei Entgegennahme der Anzeige nicht getroffen; der Landesverkehrsverwaltung wurde hierüber nichts mitgeteilt.

Die Kurzbezeichnung „BTM" in POLAS beruhte auf einem geringfügigen Vergehen (Verurteilung zu 10 Tagessätzen). Sie wäre also ebenfalls nach 5 Jahren zu löschen gewesen (vergleiche 10. TB, 16.3.1). Erst aufgrund der Eingabe wurde die Speicherung überprüft und mangels Erforderlichkeit zur polizeilichen Aufgabenerfüllung insgesamt gelöscht.

Selbst wenn man von einer zehnjährigen Frist ausgehen würde, bliebe die Frage, ob die Speicherung in POLAS der Landesverkehrsverwaltung mitgeteilt werden durfte. Speicherungen in POLAS über frühere Ermittlungsverfahren und insbesondere kriminologische Kurzbezeichnungen dienen nach § 16 Abs. 2 Satz 3 des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) der Vorsorge für künftige Strafverfolgung. Die Mitteilung an die Landesverkehrsverwaltung diente dagegen deren Aufgabe zur Überprüfung der Eignung, ein Kraftfahrzeug zu führen, was mit Strafverfolgung nichts zu tun hat. Eine entsprechende Zweckdurchbrechung von POLAS-Erkenntnissen ist nicht vorgesehen; daher war auch die polizeiliche Mitteilung, der Petent sei als Drogenkonsument bekannt, unzulässig. Die genannten Verwertungsbeschränkungen für polizeiliche Erkenntnisse sind auch deshalb erforderlich, um zu verhindern, daß ein Bürger, der als Geschädigter eine Strafanzeige stellt, damit rechnen muß, zunächst einmal dateimäßig überprüft zu werden und hieraus empfindliche Nachteile durch Maßnahmen anderer Behörden zu erleiden.

Somit gab es schon an den Quellen der polizeilichen Erkenntnisse und Ermittlungen der Landesverkehrsverwaltung eine Menge auszusetzen. Darüber hinaus stellte sich jedoch die Frage, ob die Tatsachen, wenn sie denn zulässigerweise verwertbar gewesen wären, ausgereicht hätten, um die Führerscheineignung des Petenten in Zweifel zu ziehen und ihn zur Beibringung eines Gutachtens aufzufordern.

Seit langem wird in der Praxis der Führerscheinbehörden diskutiert, ob und in welchen Fällen der Konsum illegaler Drogen Zweifel an der Eignung, ein Kraftfahrzeug zu führen, begründen kann.

1986 hatte uns die Behörde für Inneres noch mitgeteilt, daß die Unterrichtung der Führerscheinstelle dann erforderlich ist, wenn wegen des Konsums von Rausch- und Betäubungsmitteln – insbesondere von sog. harten Drogen – vermutet werden muß, daß die betroffene Person wegen des Drogenkonsums infolge Entzugserscheinungen zum Führen von Kraftfahrzeugen nicht nur vorübergehend ungeeignet sein könnte. In solchen Fällen würde außer den Personalien des Betroffenen nur das Aktenzeichen des staatsanwaltschaftlichen Ermittlungsverfahrens mitgeteilt. Ein Verfahren wegen des Konsums einer Haschisch-Zigarette würde jedoch nicht zu einer Mitteilung an die Führerscheinstelle führen.

Diese Differenzierung war aus unserer Sicht zutreffend. Eine polizeiliche Mitteilung an die Führerscheinstelle ist dann zulässig, wenn es hinreichende Anhaltspunkte dafür gibt, daß die Führerscheinstelle selbst die Fahrerlaubnis entzieht oder Maßnahmen zur Klärung von Zweifeln an der Führerscheineignung ergreift. Ein Führerscheinentzug ist nach § 15 b Abs. 1 Straßenverkehrszulassungsordnung (StVZO) vorgeschrieben, wenn jemand unter erheblicher Wirkung geistiger Getränke oder anderer berauschender Mittel am Verkehr teilgenommen oder sonst gegen verkehrsrechtliche Vorschriften oder Strafgesetze erheblich verstoßen hat. Unstrittig ist danach, daß Fahrten oder gar die Verursachung eines Verkehrsunfalls unter erheblichem Drogeneinfluß zu polizeilichen Mitteilungen an die Führerscheinstelle und zum Führerscheinentzug führen können. Notwendig ist dann auch, daß die Polizei diese Fälle unverzüglich im Laufe der Ermittlungen meldet. Eine Mitteilung erst aufgrund einer Eintragung in polizeiliche Dateien durch einen Beamten, der nicht für die Ermittlungen zuständig ist, wäre dagegen sachwidrig.

Liegen die zum Führerscheinentzug zwingenden Voraussetzungen nicht vor, sondern bestehen lediglich Zweifel an der Eignung, kann die Führerscheinbehörde die Beibringung eines amts- oder fachärztlichen Gutachtens, eines Gutachtens einer medizinisch-psychologischen Untersuchungsstelle oder eines Sachverständigen oder Prüfers für den Kraftfahrzeugverkehr anfordern. Das Problem in diesen Fällen ist, wann Feststellungen über Drogenkonsum zu Zweifeln und dementsprechend Mitteilungen an die Führerscheinstelle und Gutachtenanforderungen gegenüber dem Führerscheininhaber führen.

Verschiedene gerichtliche Entscheidungen der letzten Jahre gingen hierbei sehr weit: Nach einer vom Bundesverwaltungsgericht bestätigten Entscheidung des Verwaltungsgerichtshofs Mannheim (NJW 1989, Seite 2637) reichte schon das Auffinden von Marihuana bei einem Reisenden in einem Zugabteil, also ohne jeden Bezug zum Straßenverkehr, für Zweifel an der Führerscheineignung aus. Dies hat in einigen Bundesländern zu einer ausufernden Mitteilungspraxis der Polizei an die Führerscheinbehörden geführt; denn wenn jede polizeiliche Feststellung zum Besitz jeglicher Art illegaler Drogen aus Sicht der Führerscheinbehörden Zweifel begründen kann, darf alles mitgeteilt werden. Die Folge war dann eine Fülle von amtsärztlichen und medizinisch-psychologischen Untersuchungen.

Dem hat das Bundesverfassungsgericht in einer vielbeachteten Entscheidung vom 24. Juni 1993 (NJW 1993 Seite 2365ff.) einen Riegel vorgeschoben. Das Gericht führt aus, daß insbesondere die sehr eingehende medizinisch-psychologische Untersuchung einen Eingriff in das allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG darstelle. Der Eingriff sei nur dann gerechtfertigt, wenn die Anforderung eines Gutachtens sich auf solche Mängel bezieht, die bei vernünftiger, lebensnaher Einschätzung die Besorgnis begründen, daß der Betroffene sich als Führer eines Kraftfahrzeugs nicht verkehrsgerecht und umsichtig verhalten wird. Außerdem ist nicht bereits jeder Umstand, der auf die entfernt liegende Möglichkeit eines Eignungsmangels hindeutet, ein hinreichender Grund für die Anforderung eines medizinisch-psychologischen Gutachtens. Vielmehr müssen der Entscheidung über die Anforderung tatsächliche Feststellungen zugrundegelegt werden, die einen Eignungsmangel als naheliegend erscheinen lassen. Schließlich ist bei der Entscheidung über die Art des anzufordernden Gutachtens dem allgemeinen Persönlichkeitsrecht des Betroffenen Rechnung zu tragen.

Dies bedeutet für die Praxis der Führerscheinstelle, daß Zweifel an der Eignung, ein Kraftfahrzeug führen zu können, nur dann anzunehmen sind, wenn

die tatsächlichen Feststellungen einen ausreichenden Bezug zum Straßenverkehr haben. Ebensowenig wie die Führerscheineignung eines Bahnreisenden, der eine Flasche Alkohol im Gepäck hat und sie vielleicht auch austrinkt, in Zweifel gezogen werden kann, gilt dies für den Besitz oder auch Konsum von sogenannten weichen illegalen Drogen ohne Bezug zum Straßenverkehr. Erst dann, wenn Anhaltspunkte für gewohnheitsmäßigen Konsum oder Drogenabhängigkeit vorliegen, sind auch Zweifel an der Führerscheineignung angebracht. Diese Zweifel sind primär durch fachärztliche medizinische Gutachten zu bestätigen oder auszuräumen. Die besonders tief in das Persönlichkeitsrecht eingreifende medizinisch-psychologische Untersuchung, die im Volksmund „Idiotentest" genannt wird, kommt erst als letztes Mittel in Betracht.

Die Behörde für Inneres teilt zwar die Auffassung, daß der vom Bundesverfassungsgericht betonte Verhältnismäßigkeitsgrundsatz bei der Wahl des Mittels zur Feststellung der Führerscheineignung zu berücksichtigen ist. Noch keine Übereinstimmung besteht jedoch insoweit, als sie nach wie vor davon ausgeht, daß entsprechende Untersuchungen bei bloßem Haschischkonsum auch ohne Bezug zum Straßenverkehr erfolgen können. Die geltenden polizeiinternen Regelungen sehen Mitteilungen an die Landesverkehrsverwaltung auch bei Feststellungen über bloßen Drogenkonsum (außer Alkohol) ohne Bezug zum Straßenverkehr vor.

Wir haben dagegen geltend gemacht, daß sich an den vom Bundesverfassungsgericht formulierten Maßstäben auch polizeiliche Mitteilungen an die Führerscheinstelle orientieren müssen. Sie können nur erfolgen, wenn die Feststellungen der Polizei zum Drogenkonsum entweder in direktem Zusammenhang mit dem Straßenverkehr stehen oder es hinreichend konkrete Anhaltspunkte für Dauerkonsum oder Abhängigkeit gibt. Diese tatsächlichen Voraussetzungen können nur im Laufe von einschlägigen Ermittlungen festgestellt werden, nicht jedoch allein aufgrund von Dateieintragungen im polizeilichen Auskunftssystem.

17. Polizei

17.1 Polizeiliche Automationsvorhaben

17.1.1 Projekt Computerunterstützte Vorgangsbearbeitung bei der Polizei (COMVOR)

Die Planung des Projekts COMVOR ist gegenüber dem im 11. TB (17.1.1) geschilderten Sachstand unverändert geblieben. Das Projekt hat uns an den einzelnen datenschutzrechtlich relevanten Details auch weiterhin intensiv beteiligt. Im Frühjahr sind die ersten Teilleistungen zur Vergabe an einen privaten Anbieter ausgeschrieben worden. In Abstimmung mit uns sind in den Ausschreibungsunterlagen folgende Anforderungen zur Gewährleistung einer ausreichenden Datensicherheit aufgenommen worden:

— Authentifizierung der Anwender durch Chipkarte am Arbeitsplatz-Rechner sowie zusätzliche Benutzerauthentifikation jeweils bei Nutzung relevanter Funktionalitäten oder bei Bereitstellung besonders sensibler Daten

— verschlüsselte Speicherung des Paßwortes ausschließlich auf der Chipkarte

— Ende-zu-Ende-Verschlüsselung für den Transport von Inhaltsdaten über das Datennetz an der Schnittstelle des lokalen – polizeiinternen – Netzes (LAN) zum behördenübergreifenden Netz (WAN)

— kein Betriebssystemzugriff auf dem Arbeitsplatz-Rechner

— Bildschirmverdunkelung auf dem Arbeitsplatzrechner bei Arbeitsunterbrechung durch den Benutzer, Weiterarbeiten erst nach erneuter Authentifizierung

— Protokollierung unberechtigter Zugriffe und bestimmter Funktionalitäten der Systemadministration und der Anwender

— Gehäuseschloß oder Verplomben sämtlicher Geräte, Sicherung der Schnittstellen an der Arbeitsplatz-Hardware gegen unbefugte Nutzung, keine Diskettenlaufwerke am Arbeitsplatz oder gleichwertige Sicherung.

Bis zum Redaktionsschluß konnte von uns noch nicht geprüft werden, ob diese Vorgaben eingehalten sind.

17.1.2 Projekt „Verbrechensbekämpfung"

Zu Beginn des Jahres wurden nicht allein wir von einem Senatsbeschluß überrascht, mit dem die Bürgerschaft um Bewilligung von ca. 18 Millionen DM zur Verbesserung der Verbrechensbekämpfung in Hamburg ersucht wurde (Bürgerschaftsdrucksache 14/3623). Ein beträchtlicher Teil dieser Mittel sollte auf den Einsatz von IuK-Technik bei der Polizei entfallen.

Hierauf wurde ein neues Projekt „Verbrechensbekämpfung" der Polizei gegründet. Anfangs war unklar, wie der programmatische Titel dieses Projekts tatsächlich mit Inhalt gefüllt werden sollte.

Als Ziel des Projekts wurde genannt, angesichts wachsender Kriminalität schnelle und für den Polizeivollzug und die Bürgerinnen und Bürger sichtbare Unterstützung vor allem bei der Verbrechensbekämpfung im örtlichen Bereich zu leisten. Hierbei sollten besonders belastete Schwerpunktbereiche der polizeilichen Tätigkeit vorrangig durch moderne Standards und Möglichkeiten der Informations- und Kommunikationstechnik unterstützt werden.

Im Frühsommer wurde dann deutlicher, worum es im einzelnen ging: Bis zum Januar 1994 sollen Dienststellen an etwa 50 Standorten mit insgesamt 240 zunächst unvernetzten Arbeitsplatz-Rechnern und Büro-Standard-Software ausgestattet werden. Um eine Voraussetzung für den Aufbau eines wirksamen Datennetzes für die Polizei Hamburg zu schaffen, sollen möglichst viele Dienst-

stellen der Polizei verkabelt werden. Danach sollen schrittweise die Verknüpfung von eingerichteten Arbeitsplatz-Rechnern in den Schwerpunktbereichen zu lokalen Netzen, die Verknüpfung von lokalen Netzen untereinander sowie der Zugang von Arbeitsplatz-Rechnern zum Groß-Rechner erfolgen.

Die anzuschaffende Hardware und die Maßnahmen zur Datensicherung entsprechen den Vorgaben von COMVOR (siehe oben 17.1.1). Die Standard-Software umfaßt das Textverarbeitungsprogramm „Winword" und die Tabellenkalkulation „Excel". Ferner soll auch die erste Teilleistung von COMVOR, die bestimmte Masken für Standardformulare des Polizeivollzugs zur Verfügung stellt, auf den Arbeitsplatzrechnern vorgehalten werden (siehe 11. TB, 17.1.1).

Eingehend wurde zwischen der Polizei und uns die Frage diskutiert, ob – im Unterschied zu den Vorgaben von COMVOR – Texte, die mit dem eigenständigen Textverarbeitungsprogramm erstellt werden, auf Dauer im PC gespeichert bleiben können. Wir haben gefordert, daß nach bestimmten fachlich festzulegenden Fristen (z.B. einer Woche) eine automatische Löschung der im PC gespeicherten und ausgedruckten Texte erfolgt.

Maßgeblich hierfür war die Überlegung, daß alle auf dem PC erstellten Texte des Polizeivollzugs Bestandteil der jeweiligen Akten werden. Das Auseinanderlaufen von Aktenvorgängen und Speicherungen im PC soll vermieden werden. Datenschutzrechtlich unzulässige gesonderte Ablagen von Texten würden dadurch unterbleiben.

Wenn z.B. mit der automatisierten Textverarbeitung eine Stellungnahme verfaßt wird, die die Mitteilung enthält, daß bestimmte Daten in einer polizeilichen Datei gelöscht wurden, wäre es inakzeptabel, diesen Text auf Dauer im PC vorzuhalten, da dann die zu löschenden Informationen elektronisch gespeichert blieben (9. TB, 4.12.8; 10. TB, 16.8). Ein anderer Fall wäre die dauerhafte Speicherung von Texten über sog. Anhaltemeldungen, die nur drei Monate lang erfaßt werden dürfen (10. TB, 16.2.2). Die Vernichtung der Papierunterlagen über Anhaltemeldungen und die Löschung in der Tagebuchdatei würden unterlaufen, wenn der Text im PC erhalten bliebe. Antworten auf Ermittlungsersuchen bei Ordnungswidrigkeiten könnten auch dann noch sensible Informationen über die Betroffenen vermitteln, wenn die Daten über das Verfahren bei der Bußgeldstelle längst gelöscht wären (9. TB, 4.11.4). Mitteilungen für Meldedienste, die in der ermittelnden Dienststelle mit Hilfe der Textverarbeitung erstellt würden, wären auch dann noch vorhanden, wenn die für die Erfassung in der kriminalpolizeilichen Sammlung zuständige Dienststelle entscheidet, daß der Fall zur dauerhaften Speicherung nicht geeignet ist oder der Verdacht im weiteren Ermittlungsverfahren ausgeräumt wird (10. TB, 16.3; 11. TB, 17.4). Die Beispiele ließen sich fortsetzen.

Andererseits war zu berücksichtigen, daß es durchaus Notwendigkeiten gibt, Texte auf Dauer im PC zur Verfügung zu stellen. Dies betrifft z.B. Textbausteine oder verwaltungsinterne Vorgänge. Wir haben daher vorgeschlagen, diese dauerhaft erforderlichen Texte in einem besonderen zugriffsgeschützten Bereich zu speichern, der von der routinemäßigen Löschung nicht erfaßt wird. Dies würde jedoch voraussetzen, daß es an allen Standorten der PC besonders berechtigte Mitarbeiter gibt, die die Texte im Einzelfall in den nicht der Löschung unterworfenen Bereich übertragen.

Dieser Vorschlag war nicht zu realisieren, da es derartige Mitarbeiter, die begrenzte Aufgaben der Systemverwaltung an den PC-Standorten wahrnehmen, nicht geben wird. Vielmehr werden die PC den Dienststellen zunächst ohne nähere funktionelle Differenzierungen mit den Standardprogrammen zur Verfügung gestellt. Erst beim weiteren Ausbau infolge der Vernetzung und der Integration von COMVOR wird es Abstufungen geben.

Daher blieb zunächst nur die Lösung, zwei Bereiche einzurichten, von denen einer der routinemäßigen Löschung unterliegt; hierfür wurde eine Frist von vierzehn Tagen bis zur Löschung vorgesehen. Im anderen Bereich bleiben die Texte dagegen solange gespeichert, bis die Löschung im Einzelfall erfolgt. Die Mitarbeiter können ohne technische Vorgaben zwischen diesen beiden Möglichkeiten wählen. Es hängt somit von der Verantwortlichkeit der einzelnen Sachbearbeiter ab, ob Texte, für die besondere Löschverpflichtungen bestehen, auch tatsächlich nur in dem Bereich erstellt werden, in dem die automatisierte Löschung erfolgt. Wird dagegen im Bereich mit dauerhafter Speicherung gearbeitet, muß im Einzelfall nach bestimmten Fristen geprüft werden, ob der Text zulässigerweise gespeichert bleiben darf.

Den hiermit verbundenen Kontroll- und Überwachungsaufwand hätten wir gern vermieden. Es bleibt den weiteren Erfahrungen vorbehalten, ob sich die Praxis akzeptabel gestaltet oder die oben beispielhaft beschriebenen unzulässigen Wirkungen eintreten.

17.1.3 Neukonzeption des bundesweiten Informationssystems der Polizei (INPOL)

Die technische Ausgestaltung des bundesweiten Informationssystems der Polizei (INPOL-Bund) beruht auf einer Konzeption aus den siebziger Jahren. Seitdem ist es ständig erweitert worden (siehe 11. TB, 17.2.1). Inzwischen hat sich gezeigt, daß die bestehende Struktur des Informationssystems aus Sicht der polizeilichen Anwender erneuerungsbedürftig ist.

Eine beim Bundeskriminalamt eingerichtete Projektgruppe hat daher den Auftrag bekommen, eine Neukonzeption zu erarbeiten, von der bisher der Abschlußbericht für ein grobes Fachkonzept vorliegt. Die Kernaussage dieses Abschlußberichts läßt sich wie folgt zusammenfassen: Die INPOL-Struktur soll nicht mehr durch mehrere nahezu selbständige Anwendungen gekennzeichnet sein, sondern durch einen sog. gemeinsamen, anwendungsunabhängigen Datenpool.

Nicht mehr die Frage, in welcher Datei die Daten gespeichert sind, soll darüber entscheiden, welche Informationen der Anwender erhält, sondern welche Zugriffsbefugnisse er besitzt. Die Informationen aus INPOL sollen nicht mehr isoliert neben der täglichen Vorgangsbearbeitung stehen, sondern im Rahmen der automatisierten Vorgangsbearbeitung unmittelbar Bestandteil des polizeilichen Vorgangs werden können. Umgekehrt soll der einzelne polizeiliche Vorgang, der in automatisierten Vorgangsbearbeitungssystemen erstellt worden ist, ohne Bruch im Speichermedium zur Quelle von INPOL-Speicherungen werden.

Damit wird deutlich, daß die INPOL-Neukonzeption nicht allein ein Problem des Bundes ist, sondern die polizeiliche Datenverarbeitung in den Ländern unmittelbar strukturieren wird. Konsequenterweise stellt die INPOL-Neukonzeption daher das Bundeskriminalamt nicht mehr in den Mittelpunkt der INPOL-Struktur, sondern betrachtet es als einen Teilnehmer wie die Länderpolizeien auch.

Wir sind von der Behörde für Inneres frühzeitig über die Neukonzeption unterrichtet worden. Gemeinsam mit anderen Datenschutzbeauftragten des Bundes und der Länder haben wir uns durch die Projektgruppe beim BKA die Vorstellungen erläutern lassen und eine erste datenschutzrechtliche Bewertung vorgenommen.

Bei Redaktionsschluß zeichnete sich jedoch ab, daß in absehbarer Zeit nicht mit der Umsetzung der Pläne zu rechnen ist. Unsere datenschutzrechtliche Bewertung soll daher erst in späteren Tätigkeitsberichten wieder aufgegriffen werden, wenn das Thema aktuell wird.

17.2 Europäische Zusammenarbeit der Polizei (Europol)

Im Juni 1991 hatte die deutsche Delegation dem Europäischen Rat der Staats- und Regierungschefs der Mitgliedstaaten der EG Vorschläge zur Schaffung eines zentralen Europäischen Kriminalamtes unterbreitet. Auf der Tagung des Rats in Maastricht vom Dezember 1991 einigte man sich darauf, daß diese Vorschläge weiterverfolgt werden sollten. Ziel ist der Aufbau einer europäischen Polizeibehörde, die eigenständige Ermittlungsbefugnisse insbesondere auf dem Gebiet des Drogenhandels und der internationalen organisierten Kriminalität erhalten soll.

Als erster Baustein für diese Polizeieinheit ist die Einrichtung einer zentralen Organisation zur Erleichterung des Austauschs und der Koordinierung kriminalpolizeilicher Informationen vorgesehen. Mit einer gemeinsamen Datenbank (Europäisches Informationssystem EIS) soll die Weitergabe von polizeilichen Erkenntnissen über grenzüberschreitende kriminelle Aktivitäten unterstützt werden.

Im September 1992 hat daraufhin unter deutscher Federführung ein Projektteam als Aufbaustab in Straßburg seine Arbeit aufgenommen. Zwischen allen Beteiligten besteht Übereinstimmung darüber, daß es für die Errichtung von

Europol als internationaler zwischenstaatlicher Organisation mit eigenen Befugnissen eines völkerrechtlich bindenden Vertrags bedarf. Zum Abschluß einer Konvention ist es jedoch bisher nicht gekommen. Das Europäische Parlament hat in einer Entschließung vom 22. Januar 1993 (Bundestagsdrucksache 12/4378) Anforderungen an die Ausgestaltung der Konvention formuliert, die insbesondere auch den Schutz personenbezogener Daten betreffen.

Das Parlament fordert, daß jede Initiative zum Aufbau von Europol und des Europäischen Informationssystems davon abhängig gemacht wird, daß angemessene Rechtsvorschriften zum Schutz des Privatlebens in das nationale Recht der Mitgliedstaaten aufgenommen werden. Es vertritt die Meinung, daß im Zusammenhang mit der Informationsverarbeitung von Europol sowohl die Definition von „Information" als auch das anzuwendende Verfahren genau eingegrenzt werden müssen, um die unkontrollierte Übermittlung von Daten zu verhindern. Neben dem Schutz der Privatsphäre müsse gleichzeitig ein Rechtsschutz der Betroffenen vorgesehen sein. Zumindest müsse das Recht auf Information, Einsichtnahme und Rechtshilfe sowie eine Regelung über die Folgen bei unrechtmäßigem oder unsachgemäßem Vorgehen für alle Bürger, die sich rechtmäßig in der Gemeinschaft aufhalten, eingeführt werden.

Die an den Planungen zu Europol beteiligten Regierungen wollen jedoch nicht auf die Schaffung der rechtlichen Grundlagen warten, sondern bereits im Vorgriff hierauf Fakten schaffen.

Im April 1993 wurde eine Ministervereinbarung über die Einrichtung der Europol-Drogenzentralstelle (EDU) getroffen. Die Vereinbarung sieht vor, daß die zuständigen Ministerien der Mitgliedstaaten ab dem 1. Juli 1993 Verbindungsbeamte entsenden. Diese Verbindungsbeamten bilden die EDU als Zentralstelle für den Austausch und die Analyse von Informationen und Erkenntnissen über den illegalen Drogenhandel, darin verwickelte kriminelle Vereinigungen und damit verbundene Geldwaschaktivitäten, die zwei oder mehr Mitgliedstaaten betreffen.

Der Austausch personenbezogener Informationen ist folgendermaßen vorgesehen: Jeder Austausch von Informationen zwischen einem ersuchenden und einem auskunftserteilenden Staat erfolgt über die Verbindungsbeamten. Sie greifen hierzu auf ihre jeweiligen nationalen polizeilichen Informationssysteme zu, die deutschen Verbindungsbeamten also auf INPOL. Sollte der auskunftserteilende Staat über Informationen im Zusammenhang mit einer drogenbezogenen Straftat verfügen, die für einen anderen Staat relevant sind, können diese Informationen von den Verbindungsbeamten entsprechend den nationalen Gesetzen weitergegeben werden. Automatisierte Dateien oder sonstige Datensammlungen mit personenbezogenen Daten werden nach der Ministervereinbarung nicht geführt.

Wir haben gegenüber der Behörde für Inneres zu diesem in der Ministervereinbarung vorgesehenen Verfahren folgende Grundsätze deutlich gemacht:

Eine Vereinbarung zwischen den jeweiligen Fachministern hat nicht die Qualität eines materiellen Gesetzes, sondern allenfalls einer Verwaltungsvorschrift. Die Vereinbarung stellt daher keine eigenständige Rechtsgrundlage für die Übermittlungen dar und genügt somit nicht den Anforderungen des Gesetzesvorbehalts für Eingriffe in das Recht aus informationelle Selbstbestimmung. Dementsprechend verweist der Vereinbarungstext hinsichtlich der Zulässigkeit der Datenübermittlung im Rahmen der EDU auf die jeweiligen nationalen Rechtsvorschriften.

Die Verantwortung für den zulässigen Umgang mit Daten, die im INPOL-System gespeichert sind, trägt die Stelle, die für die materielle polizeiliche Aufgabe, in der Regel das zugrunde liegende polizeiliche Ermittlungsverfahren, zuständig ist. Wenn die Polizei Hamburg eine Person in INPOL aufgrund ihrer Zuständigkeit zur Strafverfolgung oder Gefahrenabwehr gespeichert hat, bleibt sie auch für weitere Übermittlungen der Daten aus dem INPOL-System verantwortlich.

Zugriffe auf INPOL-Datenbestände durch die Verbindungsbeamten zum Zweck der Übermittlung an Verbindungsbeamte anderer Staaten stellen somit für den von der Polizei Hamburg eingegebenen Datenbestand Übermittlungen an ausländische Polizeibehörden dar, die nach Maßgabe von § 20 Abs. 3 des hamburgischen Gesetzes über die Datenverarbeitung der Polizei (PolDVG) zu beurteilen sind.

Die Übermittlung ist danach nur möglich, wenn im Einzelfall einer der gesetzlichen Gründe vorliegt: Erforderlichkeit zur Erfüllung eigener polizeilicher Aufgaben; Verpflichtung oder Berechtigung aufgrund internationaler Vereinbarungen über Datenübermittlungen zwischen Polizeidienststellen; Erforderlichkeit zur Abwehr einer erheblichen Gefahr durch den Empfänger. Die Verbindungsbeamten können allenfalls die Prüfung nach der letzten Voraussetzung selbst vornehmen, wenn sie beurteilen können, ob der Datenempfänger die Informationen zur Abwehr einer erheblichen Gefahr benötigt. Da es sich hierbei um eine konkrete Gefahr handeln muß, also der Gesichtspunkt der vorbeugenden Bekämpfung von Straftaten nicht ausreicht, dürfte dieser Fall die seltene Ausnahme sein.

Demnach bedeutet der in der Ministervereinbarung enthaltene Verweis auf die Vorschriften zur Datenübermittlung nach dem nationalen Recht in aller Regel, daß nur die Erfüllung eigener polizeilicher Aufgaben in Betracht kommt. Zwischen den zuständigen Ministerien des Bundes und der Länder besteht Übereinstimmung darüber, daß der Zugriff des deutschen Verbindungsbeamten auf INPOL-Dateien nur dazu genutzt werden darf, die Anfrage gezielt an die ermittelnde Polizeidienststelle des Bundes oder der Länder weiterzuleiten. Er darf die Dateierkenntnisse jedoch nicht unmittelbar an die anfragende ausländische Polizeidienststelle übermitteln.

Die Ministervereinbarung begrenzt die Aufgabenstellung der Europol-Drogenzentralstelle auf Delikte im Zusammenhang mit dem Drogenhandel. Bei dieser

eingeschränkten Aufgabenstellung der Verbindungsbeamten kann – nach den oben genannten Kriterien – nur ein Zugriff auf die für Drogendelikte bestimmten INPOL-Anwendungen in Betracht kommen. Dies ist nach Mitteilung der Behörden für Inneres gewährleistet.

17.3 Organisierte Kriminalität

17.3.1 Prüfung der Arbeitsdatei PIOS „Organisierte Kriminalität"

Der Begriff „organisierte Kriminalität" –OK– beherrscht die öffentliche Diskussion über die innere Sicherheit. Wenig schlagzeilenträchtig ist dagegen die bundesweit als Verbundsystem betriebene Arbeitsdatei PIOS „Organisierte Kriminalität" (APOK). Im Berichtszeitraum haben wir erstmals Speicherungen der Polizei Hamburg in dieser Datei querschnittsmäßig überprüft.

APOK soll der Aufklärung und/oder vorbeugenden Bekämpfung von Straftaten der organisierten Kriminalität dienen, insbesondere in bestimmten Kriminalitätsbereichen wie z.B. Falschgeldherstellung, Waffenhandel, Kfz-Diebstahl, Schutzgelderpressung, Zuhälterei. Der Drogenhandel wird von APOK dann abgedeckt, wenn auch andere Bereiche der organisierten Kriminalität betroffen sind; andernfalls existiert für Drogendelikte die eigene Arbeitsdatei PIOS „Rauschgift" (APR).

Insgesamt sind in APOK mehrere zehntausend Personendatensätze bundesweit gespeichert. Diese Zahl ist erstaunlich hoch, wenn man berücksichtigt, daß im Jahr 1992 nach Angaben des Bundeskriminalamtes 641 strafrechtliche Ermittlungsverfahren im Bereich der organisierten Kriminalität anhängig gewesen sind. Der Anteil Hamburgs an Speicherungen in APOK ist von fast einem Drittel im Jahr 1987 auf ca. 9 % der Datensätze im Sommer 1993 gesunken. Gleichwohl ist er immer noch überproportional hoch und entspricht in etwa dem Anteil Niedersachsens. Nordrhein-Westfalen hat dagegen nicht einmal halb so viele Daten gespeichert. Diese unterschiedliche Verteilung ist vor allem darauf zurückzuführen, daß Hamburg das erste Land mit einer speziell für organisierte Kriminalität zuständigen Dienststelle war, die seit Bestehen der Verbunddatei gezielt Speicherungen vorgenommen hat. Inzwischen hat jedoch Hessen mit weitem Abstand die meisten Daten gespeichert. Länder, in denen die polizeilichen Zuständigkeiten für OK-Delikte nicht vergleichbar konzentriert sind, weisen dagegen nur einen verhältnismäßig geringen Anteil aus.

Die Entscheidung, ob ein Sachverhalt und die dazugehörenden personenbezogenen Daten in APOK gespeichert werden, wird bei Eingang des Vorgangs in der zuständigen Dienststelle des Landeskriminalamtes getroffen. Maßgeblich ist, ob der Sachverhalt einen Bezug zur organisierten Kriminalität (sog. OK-Relevanz) aufweist. Das Problem hierbei ist, daß es keinen eindeutigen Maßstab für die Feststellung organisierter Kriminalität gibt. § 1 Abs. 7 des hamburgischen Gesetzes über die Datenverarbeitung der Polizei (PolDVG) definiert organisierte Kriminalität als „die von Gewinn- oder Machtstreben bestimmte plan-

mäßige Begehung von Straftaten nach Abs. 4, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig 1. unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen, 2. unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder 3. unter Einflußnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken." Diese Definition folgt den von den Justiz- und Innenministern bzw. -senatoren 1991 beschlossenen Richtlinien über die Zusammenarbeit von Staatsanwaltschaft und Polizei bei der Verfolgung der organisierten Kriminalität.

In der polizeilichen Praxis werden zur Konkretisierung dieser Definition Indikatoren herangezogen, um die OK-Relevanz beurteilen zu können. Hierzu gehören z. B. präzise, marktgerechte Tatplanung und -vorbereitung, professionelle, arbeitsteilige Tatdurchführung durch Spezialisten, profitorientierte Beuteverwertung mit „Geldwäsche", Abschottung, hierarchischer Gruppenaufbau, Unterstützung von Gruppenmitgliedern, Korruption, Monopolisierungsbestrebungen, Öffentlichkeitsarbeit.

Sachverhalte, deren OK-Relevanz sich noch nicht mit hinreichender Sicherheit bejahen läßt und die sich daher noch nicht für APOK eignen, werden als sogenannte Prüffälle behandelt. Zur Verarbeitung des Informationsaufkommens aus diesen Prüffällen wäre aus Sicht der Dienststelle eine selbständige automatisierte Datei erforderlich, die jedoch aus Kapazitätsgründen bisher nicht realisiert werden konnte. Derzeit stehen die Prüffälle ohne weitere Informationsaufbearbeitung lediglich in Papierform zur Verfügung.

Unsere Überprüfung bezog sich auf folgende Bereiche:

— Kriminelle Vereinigungen

  Die Problematik des Tatbestands der kriminellen Vereinigung nach § 129 StGB als möglicher Auffangtatbestand ist im 9. TB (4.12.1) aufgezeigt worden. Bei der Überprüfung dieser Fälle sollte der Frage nachgegangen werden, ob Speicherungen allein mit der Begründung „kriminelle Vereinigung" vorlagen.

  Dies war nicht der Fall. Alle unter diesem Gesichtspunkt erfaßten Fälle aus dem Jahr 1993 betrafen Sachverhalte, die sich auch und insbesondere auf andere Delikte (Waffen-, Betäubungsmittel-, Menschenhandel usw.) bezogen. Die OK-Relevanz dieser Fälle war auch ohne den Gesichtspunkt „kriminelle Vereinigung" nachvollziehbar.

— Speicherungen von Personen

  Zur Prüfung der innerhalb einer Woche vorgenommenen Personenspeicherungen und der Speicherungen von sog. anderen Personen mit einem bestimmten Anfangsbuchstaben der Namen wurden Ausdrucke der Kurz- und Langinformationen in der Datei sowie die dazugehörenden Aktenvorgänge herangezogen.

Die OK-Relevanz sämtlicher Eintragungen war anhand der gespeicherten Sachverhaltsschilderung und der vorliegenden Unterlagen nachvollziehbar. Diskrepanzen zwischen der Sachverhaltsschilderung in der Datei und den Unterlagen wurden nicht festgestellt.

Zu allen Speicherungen lagen zwar aktenmäßige Unterlagen vor. Diese waren jedoch nicht mit vollständigen polizeilichen Ermittlungsakten vergleichbar, die einen Ermittlungsvorgang chronologisch dokumentieren. Das Aktenmaterial beschränkte sich z. B. auf Fernschreiben anderer Dienststellen, die Wiedergabe von Erkenntnissen ausländischer Polizeibehörden oder zusammenfassende Vermerke. Dies ist in erster Linie darauf zurückzuführen, daß die Speicherungen häufig vor der Einleitung eines strafprozessualen Verfahrens erfolgen.

Für die datenschutzrechtliche Prüfung bedeutete dies allerdings, daß ein eingehender Vergleich der in der Datei gespeicherten Bewertung mit der in den Akten enthaltenen Sachverhaltsdarstellung, der z. B. der Überprüfung von APIS-Speicherungen in den letzten Jahren zugrundelag (vergleiche 9. TB, 4.12.5.2; 10. TB, 16.9), nicht möglich war.

Als verbesserungsbedürftig stellte sich die Einordnung von Personen in die Kategorien Beschuldigte, Verdächtige und sog. andere Personen dar. Gegen Beschuldigte ist bereits ein strafrechtliches Ermittlungsverfahren eingeleitet. Bei Verdächtigen liegen zwar Anhaltspunkte für die Begehung einer Straftat vor, sie reichen jedoch (noch) nicht zur Einleitung eines förmlichen Ermittlungsverfahrens aus. Während in anderen Dateien die Beschuldigten den weitaus größten Anteil von Gespeicherten ausmachen und die Verdächtigen kaum eine Rolle spielen, sind drei Viertel der in APOK von Hamburg erfaßten Personen als Verdächtige gespeichert. In einigen der überprüften Fälle war aus unserer Sicht die Einordnung von Personen als Verdächtige zweifelhaft. Inzwischen sind die Datensätze gelöscht worden.

Nach den Hintergrundschilderungen war zwar festzustellen, daß die Betroffenen Kontakt zu anderen hatten, die ohne Zweifel als Personen der organisierten Kriminalität anzusehen waren. Sie waren daher zur Gruppe der sog. Kontaktpersonen zu rechnen. Für die Annahme von Verdachtsmomenten fehlten jedoch hinreichende Gründe.

Die „Hochstufung" zur verdächtigen Person hat Auswirkungen auf die Dauer der Speicherung. Für Verdächtige gilt eine Prüffrist von fünf Jahren, für Kontaktpersonen dagegen eine Löschfrist von höchstens drei Jahren. Nach Maßgabe von § 16 Abs. 3 Sätze 2 und 3 PolDVG sind während der dreijährigen Regellöschfrist die Voraussetzungen für die Speicherung nach jeweils einem Jahr zu prüfen.

Ferner sind auch die rechtlichen Voraussetzungen für die Speicherung von Kontaktpersonen höher: Nach § 16 Abs. 3 Satz 1 PolDVG muß die Speicherung von Kontaktpersonen unerläßlich zur vorbeugenden Bekämpfung von

Straftaten von erheblicher Bedeutung sein. Es reicht daher nicht aus, einen Kontakt zu einer bekannten Person festzustellen, um jemanden als Kontaktperson zu speichern. Die Speicherung muß vielmehr zwingend sein, um den Sachverhalt aufklären zu können oder Ansatzpunkte zur vorbeugenden Bekämpfung von Straftaten zu erhalten.

— Finanzermittlungsfälle

Eine Reihe von Speicherungen betraf Geldtransaktionen, bei denen aufgrund näherer Umstände die Annahme von OK-Relevanz nachvollziehbar war. Die Speicherung der an den Transaktionen Beteiligten als Verdächtige haben wir auch dann für gerechtfertigt gehalten, wenn zwar ein konkreter Tatverdacht im Sinne der Strafprozeßordnung nicht bejaht werden konnte, jedoch hinreichende OK-Indikatoren vorlagen.

Sofern jedoch Informationen über eine bestimmte Geldtransaktion ohne nähere Anhaltspunkte für die Annahme einer OK-Relevanz eingehen, würde dies allein die Speicherung nicht rechtfertigen. Vielmehr müssen auch bei Meldungen mit dem Ziel der Gewinnaufspürung immer zusätzliche Indikatoren vorliegen, um die Fälle in APOK speichern zu können. Eine routinemäßige Speicherung aller eingehenden Meldungen wäre dagegen weder durch die Errichtungsanordnung APOK noch durch das PolDVG und insbesondere auch nicht durch das 1993 verabschiedete Geldwäschegesetz (GwG) gerechtfertigt. Die Behörde für Inneres hat mitgeteilt, daß Informationen über finanzielle Transaktionen nach dem Geldwäschegesetz vor Speicherung in APOK auf ihre Relevanz hin überprüft werden.

17.3.2 Postamt und Geldwäsche

Erhebliche öffentliche Aufmerksamkeit lösten im Sommer 1993 Berichte aus, wonach in einem kleinen Hamburger Postamt Bargeldeinzahlungen in beträchtlicher Höhe zur Überweisung ins Ausland vorgenommen wurden. Nach polizeilichen Feststellungen war davon auszugehen, daß es hierbei um Gewinne aus dem Straßendrogenhandel ging, die „gewaschen" werden sollten.

Auch nachdem der Postbank die konkreten Verdachtsmomente geschildert worden waren, sah sie sich zunächst außerstande, die Praxis zu unterbinden. Sie hielt sich nach dem Postgesetz für verpflichtet, die Überweisungen vorzunehmen. Ob dies tatsächlich zutraf, ist keine datenschutzrechtliche Frage. Von datenschutzrechtlichem Interesse war jedoch die weitere Auffassung der Postbank, daß sie aufgrund des Postgeheimnisses gehindert sei, die Polizei über derartige Einzahlungen zu informieren.

Wir haben die Behörde für Inneres und die Justizbehörde darauf hingewiesen, daß diese Auffassung nicht haltbar ist. Vielmehr erlaubt § 5 Abs. 3 Satz 1 des Postgesetzes eine Durchbrechung des Postgeheimnisses, wenn dies zur Verfolgung einer im Zusammenhang mit dem Postdienst begangenen Straftat erforderlich ist. Die Meinung, Geld zu überweisen sei nicht strafbar, trifft

dann nicht zu, wenn es um Drogengewinne geht. Überweisungen können in Fällen wie dem hier geschilderten Vorgehen den Tatbestand der Geldwäsche gemäß § 261 Abs. 1 StGB erfüllen.

Dies galt bereits vor Inkrafttreten des sog. Geldwäschegesetzes (GwG), das die Kreditinstitute zur Identifizierung von Einzahlern und zur Meldung verpflichtet und im Sommer 1993 noch nicht verabschiedet war. Die Neuerung dieses Gesetzes besteht in der Begründung einer Identifizierungpflicht bei Einzahlungen ab 20.000 DM und einer Meldepflicht durch Kreditinstitute bei verdächtigen Einzahlungen. Eine Meldeberechtigung bei konkretem Tatverdacht bestand jedoch schon vorher.

Auch der für die Post als Stelle des Bundes zuständige Bundesbeauftragte für den Datenschutz teilte unsere Auffassung. Die Postbank hat inzwischen ihre Haltung geändert.

17.4 Datensammlungen zur Rauschgiftbekämpfung

Seit September 1991 arbeitet im Gebiet des Hauptbahnhofs in St. Georg eine polizeiliche Koordinationsstelle zur Bekämpfung der offenen Rauschgiftszene (KORA). Sie hat den Auftrag, durch verstärkte Polizeistreifen im Gebiet die Verfestigung einer offenen Rauschgiftszene vor allem präventiv zu bekämpfen. Hierzu werden Personalien festgestellt und gegenüber Angehörigen der Rauschgiftszene Platzverweise ausgesprochen. Bei Zuwiderhandlungen gegen die Platzverweise können Personen auch in Gewahrsam genommen werden. Bereits in den ersten vier Monaten wurden über 10.000 Personalien festgestellt, mehr als 6.500 Platzverweise ausgesprochen und über 1.100 Ingewahrsamnahmen durchgeführt. Bis Mitte 1993 wurden über 85.000 Personen überprüft; hieraus resultierten etwa 3.000 Strafanzeigen wegen Drogendelikten.

Anfang 1992 erfuhren wir durch Zufall davon, daß im zuständigen Polizeirevier eine Kartei über diese Maßnahmen geführt wird. Eine vom Leiter der Polizei verfügte Errichtungsanordnung für diese Datei lag uns nicht vor, obwohl dies nach § 26 des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) Voraussetzung für deren Einführung gewesen wäre.

Aufgrund einer Prüfung der bestehenden Datei haben wir uns hiermit auseinandergesetzt. In der Datei wurden ursprünglich Personalien, Ort, Uhrzeit und Datum des Antreffens aller derjenigen erfaßt, deren Personalien festgestellt worden waren. Bei Platzverweisen und Ingewahrsamnahmen wurden Art und Geltungsbereich der Maßnahme erfaßt. Wenn Strafanzeigen gefertigt wurden, gab es Verweise auf die Aktenzeichen. In Einzelfällen kamen Lichtbilder aufgrund erkennungsdienstlicher Maßnahmen hinzu. Zum Zeitpunkt der Prüfung umfaßte die Kartei schätzungsweise mehr als 1.000 Karten, obgleich nur Karteikarten vorlagen, deren Eintragungen nicht älter waren als zwei Monate.

Der nachgeholte Entwurf einer Errichtungsanordnung sah nur noch die Erfassung von Platzverweisen, nicht mehr die bloße Personalienfeststellung vor.

Auch nach dieser Einschränkung haben wir erhebliche Bedenken gegen die Führung der Datei geltend gemacht. Diese Bedenken richteten sich nicht gegen die Erfassung von Personen, die wegen Drogenhandels festgestellt worden waren. Der Personenkreis der Dealer machte im Vergleich zu den überwiegend erfaßten Personen, die dem Kreis der Konsumenten zugerechnet wurden, ohnehin nur einen geringen Anteil aus.

Vielmehr haben wir uns dagegen gewandt, daß im Unterschied zu sog. kriminalpolizeilichen Sammlungen (KpS) nicht der Verdacht auf Straftaten zur Erfassung führen sollte, sondern polizeirechtliche Maßnahmen wie Platzverweise und Ingewahrsamnahmen. Während strafrechtliche Ermittlungsverfahren in allen Fällen der Staatsanwaltschaft zur Entscheidung vorzulegen sind, findet bei massenweise ausgesprochenen polizeirechtlichen Maßnahmen in aller Regel keine weitere Überprüfung statt.

Auch der Zweck der Speicherung ist ein anderer. Unterlagen über eingeleitete Ermittlungsverfahren können personen- und sachbezogene Erkenntnisse zur Aufklärung von Straftaten liefern, deren Täter noch nicht bekannt sind, oder Ansätze für die Aufklärung weiterer Straftaten der Betroffenen bieten. Polizeiliche Maßnahmen zur Gefahrenabwehr hängen jedoch immer von der ganz konkreten Situation am Ort der Maßnahme ab. Entweder ist aus Sicht der handelnden Beamten der Platzverweis oder die Ingewahrsamnahme wegen des Verhaltens des Betroffen möglich; dann ist eine Dateiauskunft überflüssig. Wenn die Maßnahme dagegen nicht verhaltensbedingt gerechtfertigt werden kann, vermag auch eine Dateispeicherung sie nicht zu begründen.

Die Polizei verwies dagegen zunächst darauf, daß die Dateispeicherungen Informationen zur Gefahrenbeurteilung und zum Zwecke eines abgestuften Vorgehens vermitteln können. Hiergegen sprach jedoch, daß oftmals Platzverweise gar nicht personenbezogen ausgesprochen werden, sondern die Betroffenen durch starke Polizeipräsenz verdrängt werden und somit die Erfassung in der Datei von Zufälligkeiten abhing.

Gegen die Datei sprach auch der mit der dauernden Neuerfassung und Löschung von Karteikarten verbundene Aufwand und die Unübersichtlichkeit der Kartei. Wir hatten in unserer Stellungnahme das Fazit gezogen, die Kartei führe im damaligen Zustand dazu, daß die eigentlich relevante Gruppe der Dealer sich in der großen Masse der Daten über Drogenkonsumenten „verstecken" könne.

Die Frage, ob die Kartei tatsächlich geführt werden sollte, wurde auch innerhalb der Behörde für Inneres längere Zeit kontrovers diskutiert. Schließlich erhielten wir die Mitteilung, daß die Kartei im April 1993 aufgelöst und vernichtet worden ist.

Seitdem werden die Daten aufgrund von Personalienfeststellungen nur noch listenmäßig zur Dokumentation polizeilichen Handelns erfaßt. Die Listen werden drei Monate aufbewahrt. Ein personenbezogen ausgesprochener Platzverweis führt zu einem entsprechenden Kurzbericht, der ebenfalls zur Dokumention drei Monate aufbewahrt wird.

Unberührt von den inzwischen überholten Plänen für eine Platzverweiskartei bleibt dagegen die dateimäßige Erfassung von Tatverdächtigen, die am aktiven Straßendrogenhandel beteiligt sind. Gegen entsprechende Dateien, die spezifisch für erkannte Schwerpunkte des Straßendrogenhandels geführt werden, bestehen die oben genannten Bedenken nicht (siehe 10. TB, 16.6).

17.5 Zuhälter- und Milieukartei

17.5.1 Verbesserungen bei der Kartei

Im 11. TB (17.5) war bereits die grundsätzliche Problematik einer Datei zur Verfolgung und vorbeugenden Bekämpfung von Straftaten im sogenannten Rotlichtmilieu angesprochen worden. Sie läßt sich mit folgender Frage zusammenfassen: Wie kann sichergestellt werden, daß der Polizei einerseits erforderliche Informationen über diesen durch Abschottung und Ausbeutungsdruck gekennzeichneten Kriminalitätsbereich zur Verfügung stehen, andererseits jedoch die Erfassung von Prostituierten nur aufgrund ihrer Tätigkeit unterbleibt?

Das Verwaltungsgericht Stuttgart hat hierzu in einem Urteil vom 14. November 1990 festgestellt, daß Prostituierte nicht allein deshalb gespeichert werden können, weil allgemein das Umfeld der Prostitution nach polizeilichen Erkenntnissen erheblichen kriminellen Einflüssen ausgesetzt ist. Eine Speicherung von Prostituierten könne allenfalls dann erfolgen, wenn im Einzelfall Besonderheiten hinzutreten, welche geeignet wären, das Grundrecht auf informationelle Selbstbestimmung hinter das öffentliche Interesse an der vorbeugenden Verbrechensbekämpfung gerade im Umfeld der Prostitution zurücktreten zu lassen.

Diesen Grundlinien folgt die im letzten Jahr verfügte Errichtungsanordnung der Polizei für die sogenannte Zuhälter- und Milieukartei. Sie sieht vor, milieubedingte Delikte zu erfassen. Hierzu gehören u.a. die Tatbestände: kriminelle Vereinigung, Vergewaltigung, sexuelle Nötigung, Menschenhandel, bandenmäßige gefährliche Körperverletzung, also Tatbestände, die Straftaten von erheblicher Bedeutung im Sinne des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) sind. Daneben ist die Erfassung von Delikten wie Förderung der Prostitution, Zuhälterei, Nötigung und Erpressung vorgesehen, die ebenfalls als milieutypisch gelten. Diese beiden Tatbestandsgruppen betreffen ausschließlich oder ganz überwiegend Zuhälter.

Dagegen betreffen die ebenfalls vorgesehenen Delikte Diebstahl und Betrug auf sexueller Basis in erster Linie Prostituierte. Die Speicherung dieser Fälle ist nur dann vorgesehen, wenn sich aus den Umständen der Begehung Hinweise über kriminelle Verbindungen ergeben. Diese Begrenzung folgt aus der kriminalpolizeilichen Erfahrung, daß eine Häufung von Diebstählen und Betrugsfäl-

len durch Prostituierte oftmals auf besonderen Ausbeutungsdruck der Zuhälter zurückzuführen ist.

Die Errichtungsanordnung sieht allerdings nicht nur die Erfassung von Beschuldigten und Verdächtigen vor, sondern auch von Zeugen in laufenden Ermittlungsverfahren, gefährdeten Personen und sog. Kontakt- und Begleitpersonen. Neben konkreten Gefährdungssituationen, in denen Prostituierte oftmals selbst die Polizei um Schutz bitten, kann insbesondere die Rolle als Kontakt- und Begleitperson zur Erfassung von Prostituierten ohne Vorwurf strafbaren Verhaltens führen. Allerdings muß hierbei stets beachtet werden, daß die Speicherung nur dann zulässig ist, soweit dies zur vorbeugenden Bekämpfung von Straftaten anderer Personen von erheblicher Bedeutung unerläßlich ist.

Wir haben im Ergebnis keine Einwendungen gegen die Errichtungsanordnung vorgebracht, da das Erfordernis der intensiven Strafverfolgung und vorbeugenden Straftatenbekämpfung im sogenannten Rotlichtmilieu unverkennbar ist. Die Umsetzung der Errichtungsanordnung wird zudem zu einer ganz erheblichen Reduzierung der Speicherung von Prostituierten führen.

Diese Einschätzung beruht auf einer Prüfung, die wir 1992 vor der Neuregelung vorgenommen hatten. Zu diesem Zeitpunkt war eine Reihe von gravierenden datenschutzrechtlichen Unzulänglichkeiten festzustellen. Dies betraf unter anderem die Speicherung von Lichtbildern von Geschädigten und Zeugen und die Erfassung von Prostituierten aufgrund von Anhaltemeldungen ohne Strafvorwurf.

Nachdem die neue Errichtungsanordnung einige Monate galt, haben wir 1993 eine erneute Prüfung vorgenommen. Hierbei ergab sich, daß ca. ein Drittel des früheren Bestandes ausgesondert war und auch bei der Zuordnung der erfaßten Personen zu den vorgesehenen Kategorien erhebliche Verbesserungen erfolgt waren. Gleichwohl gab es immer noch Probleme:

Bei den Erörterungen im Rahmen der Prüfung bestand zwischen den zuständigen Mitarbeitern der Polizei und uns Übereinstimmung darüber, daß die Einhaltung der differenzierten Vorgaben der Errichtungsanordnung insbesondere bei den unterschiedlichen Fristen angesichts der manuellen Karteiorganisation besondere Schwierigkeiten bereitet.

Diese bereits bei der Prüfung von 1992 geäußerte Erwartung hat sich bestätigt. Im Unterschied zu früher ist zwar jetzt erkennbar, mit welcher Rolle eine Person zuletzt erfaßt wurde und welche der unterschiedlichen Fristen für Beschuldigte einerseits, für Anzeigende, Verdächtige, Geschädigte und Gefährdete andererseits und schließlich für die sogenannten Kontakt- und Begleitpersonen gilt. Bei letzteren sieht das PolDVG eine Überprüfungsfrist von einem Jahr vor. Eine effektive Kontrolle der Fristen ermöglicht die Kartei jedoch nicht, da die für jede Karteikarte geltende Frist nur individuell festgestellt werden kann. Eine Kennzeichnung nach Jahrgängen wäre zwar denkbar, dürfte in der Praxis jedoch

kaum zu leisten sein. Die Alternative hierzu wäre die – mindestens jährliche – Durchsicht der gesamten Kartei. Angesichts der laufenden Neuzugänge und Veränderungen erscheint auch dies kaum realistisch.

Auch die Erfassung der sog. Kontakt- und Begleitpersonen und von Zeugen führte bei der manuellen Karteiführung zu Schwierigkeiten. Bei mehreren Personen, die als Kontaktpersonen erfaßt waren, handelte es sich tatsächlich um Zeugen in laufenden Ermittlungsverfahren. Die Speicherung als Kontaktperson ist nur dann möglich, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß die „Zielperson" Straftaten von erheblicher Bedeutung im Sinne von § 1 Abs. 4 PolDVG und der Errichtungsanordnung begehen wird.

Derartige tatsächliche Anhaltspunkte waren nicht immer zweifelsfrei gegeben. Die Ermittlungsverfahren wurden vornehmlich wegen des Vorwurfs der Zuhälterei oder vergleichbarer Tatbestände geführt, die keine Straftaten von erheblicher Bedeutung sind. Die zur Annahme von erheblichen Straftaten erforderliche Prognose würde über die Tatbestandshandlungen dieser Delikte hinausgehende tatsächliche Anhaltspunkte erfordern.

Zum anderen muß die Erhebung und Speicherung von Daten über die Kontaktperson erforderlich sein für die vorbeugende Bekämpfung der Straftaten der „Hintermänner". Dies kann z. B. dann der Fall sein, wenn der „Hintermann" unbekannt oder unerreichbar ist. Ist die eigentlich gesuchte Person jedoch bekannt, reduziert sich der Informationswert der Kontaktpersonen auf die Zeugenrolle.

Aus diesen Gründen haben wir mehr Zurückhaltung bei der Einordnung in die Kategorie Kontakt- und Begleitperson und eine direktere Zuordnung von Zeugen zu einzelnen Ermittlungsverfahren gefordert. Letzteres ist bei der derzeitigen manuellen Dateiführung nur schwer zu gewährleisten. Vielmehr besteht dann immer die Gefahr, daß sich einzelne Speicherungen gleichsam verselbständigen und nur noch mit größerem Aufwand aus den Ermittlungsvorgängen zu rekonstruieren ist, welcher Gesichtspunkt tatsächlich zur Erfassung geführt hat. Die Behörde für Inneres hat dem zugestimmt.

Insgesamt sind wir gemeinsam mit der Behörde für Inneres und der dateiführenden Stelle zur Auffassung gelangt, daß die Datei nur dann hinsichtlich der Speicherfristen und der unterschiedlichen Personenrollen in voller Übereinstimmung mit der Errichtungsanordnung ausgestaltet werden kann, wenn sie als automatisierte Datenbank eingerichtet wird. Das – auf den ersten Blick erstaunliche – Ergebnis, wonach Gründe des Datenschutzes für die Automation von Dateien sprechen können, beruht darauf, daß mit automatisierten Verfahren eine individuelle Überprüfung von differenzierten Speicherfristen ohne Weiteres zu gewährleisten ist. Eine automatisierte Datenbank kann auch so strukturiert werden, daß der jeweilige Kontext, der die Erfassung rechtfertigte, im einzelnen Datensatz erkennbar bleibt. So ließen sich die oben beschriebenen Zuordnungsprobleme bei Kontaktpersonen und Zeugen verringern.

Die Behörde für Inneres erarbeitet zur Zeit ein fachliches Feinkonzept für eine automatisierte Dateistruktur. Zur schnellen technischen Umsetzung des Konzepts soll die Programmierung durch einen privaten Anbieter voraussichtlich im ersten Quartal 1994 erfolgen.

17.5.2 Informationsaustausch zur „Prostitutionsüberwachung"

Bei den Prüfungen der Zuhälter- und Milieukartei haben wir auch Eintragungen festgestellt, die sich auf Aktenzeichen auswärtiger Polizeidienststellen bezogen. Anlaß waren Anfragen, ob Erkenntnisse über die Person vorlägen, was von der Polizei Hamburg verneint wurde. Derartige Erkenntnisanfragen reichen als Speicherungsanlaß nach der Errichtungsanordnung nicht aus. Die Daten wurden daher gelöscht.

Aus anderen Vorgängen ließ sich ersehen, daß formularmäßige Erkenntnisanfragen zur „Prostitutionsüberwachung" von auswärtigen Dienststellen ohne weitere Angaben zum Verwendungszweck eingehen.

Hierzu haben wir festgestellt: § 19 des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) erlaubt die Übermittlung personenbezogener Daten an andere Polizeidienststellen zur Erfüllung polizeilicher Aufgaben. Die sog. „Prostitutionsüberwachung" ist nicht schlechthin eine polizeiliche Aufgabe. Vielmehr müßte ein konkreter Bezug zur polizeilichen Aufgabenstellung nach § 1 Abs. 1 PolDVG oder zur Strafverfolgung bestehen. Auch wenn bei Übermittlungen an andere Polizeidienststellen eine eingeschränkte Begründungspflicht des Ersuchenden gilt, reicht die Angabe „zur Prostitutionsüberwachung" nicht aus. Erforderlich wären vielmehr konkretere Angaben zu laufenden Ermittlungsverfahren, zur Abwehr bevorstehender Gefahren oder zur Verhütung von Straftaten, um der ersuchten Stelle die Prüfung zu ermöglichen, ob es sich tatsächlich um eine polizeiliche Aufgabe handelt.

Sollen bei derartigen Erkenntnisanfragen auch Speicherungen in Dateien (Milieukartei, POLAS oder irgendeine andere) genutzt werden, ist ferner – und vor allem – § 14 Abs. 1 Satz 3 PolDVG zu beachten. Nach dieser Vorschrift ist die Nutzung von in Dateien gespeicherten Daten grundsätzlich nur entsprechend der Zweckbestimmung in der jeweiligen Errichtungsanordnung zulässig. Ausnahmen sind nur zur Verhinderung oder Beseitigung von erheblichen Nachteilen für das Gemeinwohl oder schwerwiegender Beeinträchtigungen von gewichtigen Rechtspositionen einzelner möglich. Dies schließt beispielsweise die Nutzung der Milieukartei zum Zweck der Übermittlung in einem Ordnungswidrigkeitenverfahren aus. Die Angaben in den Ersuchen anderer Polizeidienststellen müssen daher auch die Prüfung ermöglichen, ob die Voraussetzungen von § 14 PolDVG erfüllt sind. Die Behörde für Inneres hat mitgeteilt, daß sie unsere Auffassung teilt und die Dienststelle angewiesen wurde, Anfragen nur nach Überprüfung der entsprechenden Voraussetzungen zu beantworten.

17.6 Datenverarbeitung bei fremdenfeindlichen Straftaten

Die Häufung fremdenfeindlicher Straftaten hat zur Erweiterung bestehender und zur Planung neuer Anwendungen für die Datenverarbeitung bei der Polizei geführt.

17.6.1 Beschluß der Innenministerkonferenz

Die Innenministerkonferenz hat am 14. Mai 1993 folgende Maßnahmen beschlossen:

- Alle fremdenfeindlichen Straftaten werden im bundesweiten INPOL-Kriminalaktennachweis (KAN) erfaßt.
- Für den Kriminalaktennachweis und die INPOL-Dateien Personenfahndung und Erkennungsdienst wird ein neuer personenbezogener Hinweis „fremdenfeindlich" eingeführt.
- Der kriminalpolizeiliche Meldedienst in Staatsschutzsachen (KPMD-S) wird auf fremdenfeindliche Straftaten erweitert.
- In der Arbeitsdatei PIOS Innere Sicherheit (APIS) wird ein neuer Katalogwert „fremdenfeindlich" eingeführt.

Der diesen Erweiterungen zugrunde liegende Begriff der fremdenfeindlichen Straftaten wird wie folgt definiert:

„Straftaten, die in der Zielrichtung gegen Personen begangen werden, denen Täter (aus intoleranter Haltung heraus) aufgrund ihrer tatsächlichen oder vermeintlichen Nationalität, Volkszugehörigkeit, Rasse, Hautfarbe, Religion, Weltanschauung, Herkunft oder aufgrund ihres äußeren Erscheinungsbildes ein Bleibe- oder Aufenthaltsrecht in der Wohnumgebung oder in der gesamten Bundesrepublik bestreiten. Oder Straftaten, die gegen sonstige Personen/Institutionen/Objekte/Sachen begangen werden, bei denen der Täter aus fremdenfeindlichen Motiven heraus handelt."

17.6.2 Datenschutzrechtliche Bewertung

Von der Behörde für Inneres wurden wir vor der Beschlußfassung lediglich über die Einführung des neuen personenbezogenen Hinweises (PHW) informiert. Der PHW soll für Maßnahmen zur Gefahrenabwehr insbesondere beim Schutz gefährdeter Objekte genutzt werden. An derartigen gefährdeten Orten (z. B. Asylbewerberunterkunft) können nach dem Gesetz über die Datenverarbeitung der Polizei Personalienfeststellungen stattfinden. Durch Abfragen in den Dateien, in denen der PHW gespeichert ist, kann dann festgestellt werden, ob es sich um einen potentiellen Störer handelt.

Diese Nutzung des Hinweises leuchtet ein. Wir haben daher keine Bedenken gegen seine Einführung vorgebracht. Maßgeblich müssen bei der Speicherung des Hinweises jedoch immer hinreichend konkrete Anhaltspunkte dafür sein,

daß die Person tatsächlich eine Straftat mit fremdenfeindlicher Motivation begangen hat. Eine Vergabe des PHW z. B. für einen Ladendieb, der der „Skin-Head-Szene" zugerechnet wird, dem aber keine einschlägigen Straftaten vorgeworfen werden, kann dagegen nicht in Betracht kommen.

Neu war für uns der Beschluß der Innenministerkonferenz, alle fremdenfeindlichen Straftaten bundesweit im INPOL-Kriminalaktennachweis zu speichern. Bisher war der Kriminalaktennachweis nur für solche Delikte vorgesehen, die sich wegen ihrer Schwere und überregionalen Bedeutung für eine bundesweite Speicherung eignen. Dies ist sicherlich bei einer Beleidigung auch dann nicht der Fall, wenn sie mit fremdenfeindlicher Motivation erfolgt ist. Das unbestreitbare Erfordernis, fremdenfeindlichen Straftaten wirksam zu begegnen, kann die Prüfung, ob entsprechende Dateispeicherungen hierzu geeignet und erforderlich sind, nicht überflüssig machen. Hinzu kommt, daß der Informationswert der bundesweiten Speicherung fremdenfeindlicher Delikte dann entwertet würde, wenn sie in allen möglichen Bagatellsachen erfolgt.

Die neue besondere Erwähnung der fremdenfeindlichen Motivation bei den Kriterien des kriminalpolizeilichen Meldedienstes in Staatsschutzsachen (KPMD-S) und entsprechend für die Datei APIS ist wenig verständlich. Bisher war es Zweck des Meldedienstes und der Datei APIS, durch Sammlung und Auswertung von Nachrichten und Unterlagen Hinweise für die Verhütung und Aufklärung von Straftaten zu gewinnen, die gegen die freiheitliche demokratische Grundordnung gerichtet sind. Hierzu war u. a. die Erfassung von Straftaten, die den demokratischen Rechtsstaat gefährden (etwa das Verbreiten von Propagandamitteln verfassungswidriger Organisationen oder das Verwenden von deren Kennzeichen, z. B. Hakenkreuz), vorgesehen, aber auch von sonstigen Straftaten, wenn sie mit entsprechender Motivation begangen wurden.

Ein Erfordernis zur besonderen Erwähnung der fremdenfeindlichen Motivation hätte nur dann bestanden, wenn es eine relevante Zahl von Fällen gegeben hätte, in denen man zwar eine fremdenfeindliche Motivation annehmen konnte, eine verfassungsfeindliche Motivation jedoch ausschließen konnte. In der Praxis hat dies jedoch nach unserer Kenntnis nicht die entscheidende Rolle gespielt. Für die Datei APIS war dementsprechend schon immer ein Datenfeld „ausländerfeindlich" vorgesehen, das jetzt durch den Begriff „fremdenfeindlich" neu bezeichnet wird. Das Ministerium eines Landes hat daher in der Innenministerkonferenz zum Ausdruck gebracht, daß die Erfassung fremdenfeindlicher Straftaten im notwendigen Umfang in APIS auch nach der bisherigen Regelung möglich war und praktiziert werde.

Unumstritten zwischen der Polizei und uns war bei allen Prüfungen der Datei in den letzten Jahren, daß jedenfalls Gewaltanwendungen gegen Personen oder erhebliche Sachbeschädigungen dann einen Rückschluß auf verfassungsfeindliche Motivation zulassen, wenn sie zur Verfolgung politischer Ziele begangen werden. Dagegen war aus unserer Sicht immer wieder problematisch, daß die verfassungsfeindliche Motivation oftmals bereits dann angenommen wurde, wenn es um politische Themen bei verhältnismäßig unbedeutenden Straftaten ging (10. TB, 16.9; vergl. auch unten 17.7).

Die besondere Erwähnung der fremdenfeindlichen Motivation neben der verfassungsfeindlichen wird nur dann erklärlich, wenn man sie so versteht, daß nunmehr sämtliche fremdenfeindliche Delikte – ungeachtet ihrer Schwere und überregionalen Bedeutung und auch ohne extremistische Motivation – ebenfalls in APIS erfaßt werden sollen. In diesem Sinne legt die Staatsschutzabteilung des Landeskriminalamtes die Neuregelung aus.

Wir haben dagegen geltend gemacht, daß die Zweckbestimmung der Datei und ihre Ausgestaltung als bundesweites Verbundsystem immer auch die Prüfung des Relevanzkriteriums erfordert. Dies wird dadurch bestätigt, daß bereits 1988 von der Kommission Staatsschutz der AG Kripo – also einem polizeilichen Gremium – zu Recht darauf hingewiesen wurde, daß es sich bei Hakenkreuzschmierereien, die nach der Errichtungsanordnung regelmäßig zu erfassen sind, oftmals um reine Tabuverletzungen oder Provokationen Jugendlicher handelt. Dementsprechend bestand Übereinstimung darüber, daß in derartigen Fällen geprüft werden müsse, ob die Speicherung in APIS wirklich erforderlich ist.

Wenn nunmehr gleichwohl im INPOL-Kriminalaktennachweis wie in der Verbunddatei APIS sämtliche fremdenfeindlichen Straftaten erfaßt werden sollen, stellt sich nicht nur die Frage, ob der damit verbundene Erfassungsaufwand, der bei verschiedenen Orginsationseinheiten der Polizei zu leisten ist, sich noch mit dem Grundsatz der Erforderlichkeit vereinbaren läßt. Die im Zusammenhang mit der INPOL-Neukonzeption (17.1.3) seitens der Polizei aufgezeigten Schwachstellen bei der Mehrfacherfassung in verschiedenen Speichersystemen werden durch diese Verfahrensweise noch verstärkt. Aus datenschutzrechtlicher Sicht ist darüber hinaus problematisch, daß bei der vorgesehenen Doppelspeicherung in unterschiedlichen Dateien auch erforderliche Berichtigungen nach dem Verfahrensausgang und insbesondere Löschungen unübersichtlich und damit fehleranfällig sind.

17.7 Arbeitsdatei PIOS „Innere Sicherheit" (APIS)

Im 10. TB (16.9) hatten wir vorgeschlagen, daß auch die Hamburger Polizei die in Schleswig-Holstein praktizierte Regelung übernimmt, wonach in APIS nur solche Straftaten erfaßt werden, die nach ihrer Schwere und der Gefahr für die freiheitliche demokratische Grundordnung mit den eigentlichen Staatsschutzdelikten vergleichbar sind. Indizien für die Schwere sind aktive Gewaltanwendung gegen Personen, deren Androhung oder gewaltverursachte Sachschäden über 1.000 DM.

Aufgrund der Beratungen des 10. TB (16.9) hatte die Bürgerschaft den Senat ersucht, „zu prüfen, welche Auswirkungen eine ergänzende Regelung der Arbeitsdatei PIOS Innere Sicherheit (APIS) entsprechend den einschränken-

den Kriterien des Landes Schleswig-Holstein hätte, und dies durch ein Versuchsprogramm zu dokumentieren" (Mitteilung der Bürgerschaft an den Senat vom 27./28. Januar 1993; Drucksache 14/2845).

Wir haben der Polizei vorgeschlagen, bei dem im Ersuchen angesprochenen Versuchsprogramm wie folgt zu verfahren:

Bei Fällen, die nach Auffassung der zuständigen Polizeidienststelle speicherungswürdig sind, aber nach den in Schleswig-Holstein geltenden Zusatzregelungen nicht gespeichert werden können, werden die Aktenzeichen mit kurzer Angabe über die entgegenstehende konkrete Regelung in einer Liste erfaßt.

Nach einem aus polizeilicher Sicht geeigneten Zeitraum sollte eine Auswertung dieser Liste stattfinden, ob tatsächlich die Erforderlichkeit zur Erfassung dieser Fälle bejaht werden kann. Das Ergebnis dieser Auswertung könnte uns zur Kenntnis gegeben werden, damit Einvernehmen über etwaige notwendige Änderungen oder Ergänzungen der Zusatzregelung, deren Fortbestand oder auch deren völlige Aufgabe erzielt werden kann.

Dem ist die Polizei nicht gefolgt. Sie erfaßt vielmehr nach wie vor auch die Fälle in der Datei, die nach ihrer Auffassung die Kriterien für APIS erfüllen, aber bei Anwendung der Regelung aus Schleswig-Holstein nicht gespeichert werden können. Allerdings werden diese Fälle mit einem Merker versehen und können mithilfe des Merkers ausgewertet werden. Die Behörde für Inneres beabsichtigt, erst 1995 nach Abschluß des Versuchsprogramms hierüber zu berichten.

Um diesen Zeitraum nicht ungenutzt verstreichen zu lassen, werden wir in geeigneten Abständen Auswertungen der mit Merker versehenen APIS-Datenbestände vornehmen und die Fälle mit der Polizei erörtern. Die Laufzeit des Versuchsprogramms bis zum Redaktionsschluß dieses TB war jedoch noch zu kurz für eine derartige Zwischenbilanz.

17.8 Probleme der Videoüberwachung

17.8.1 Video- und Fotoaufnahmen bei Versammlungen

Im 11. TB (17.8) war zunächst in allgemeiner Form die datenschutzrechtliche Problematik von Videoaufnahmen bei Demonstrationen nach dem Versammlungsrecht angesprochen worden. Im Berichtszeitraum haben wir aus Anlaß einer Versammlung, bei der die Polizei Videoaufnahmen und Fotos angefertigt hatte, deren Zulässigkeit anhand der polizeilichen Unterlagen überprüft, die über den Versammlungsablauf vorliegen.

Die Demonstration hatte als unangemeldete Spontanversammlung gegen den geplanten Abriß von leerstehenden Häusern stattgefunden, nachdem es einige Stunden zuvor aus demselben Anlaß zu gewalttätigen Ausschreitungen gekommen war. Die Teilnehmer hatten sich zunächst auf der Straße versammelt und waren hierbei und noch ca. 5 Minuten nach dem Abmarsch des Demonstrationszugs mit Videokameras aufgenommen worden. Ferner waren Einzelpersonen fotografiert worden, wenn die beim Einsatz befindlichen Polizeibeamten den Verdacht hatten, daß Straftaten begangen wurden. Gegen eine Reihe von Teilnehmern waren Strafermittlungsverfahren wegen Nötigung von Verkehrsteilnehmern und gegen zwei Personen wegen Sachbeschädigung eingeleitet worden.

Aus unserer Sicht waren die Videoaufnahmen der Polizei zu Beginn der Versammlung nach § 19a, § 12a des Versammlungsgesetzes gerechtfertigt. Die gewalttätigen Ereignisse einige Stunden zuvor begründeten die Prognose, daß von der Demonstration aus gleichem Anlaß am Nachmittag ebenfalls erhebliche Störungen ausgehen würden.

Übereinstimmung mit der Polizei besteht auch insoweit, daß Aufnahmen über Einzelpersonen gemacht werden konnten, die sich aus Sicht der Polizeibeamten strafbar verhielten. Diese Aufnahmen sind nach der Strafprozeßordnung gerechtfertigt. Der Verdacht, daß Straftaten vorlagen, wurde bereits während der Versammlung und nicht erst aufgrund der Auswertungen von Aufnahmen angenommen, so daß sich auch insofern keine datenschutzrechtlichen Bedenken ergeben. Ob der Verdacht tatsächlich begründet war, ist keine datenschutzrechtliche Frage, sondern obliegt zunächst der Beurteilung durch die Staatsanwaltschaft und schließlich durch die Gerichte.

Unterschiedliche Auffassungen zwischen uns und der Behörde für Inneres bestanden jedoch darüber, ob nach dem weiteren Verlauf die Fortsetzung der Aufnahmen über die Versammlung insgesamt zulässig gewesen wäre. Wir haben die Auffassung vertreten, daß nach dem festgestellten Ablauf der Versammlung spätestens vom Zeitpunkt des Abmarsches die Videoaufnahmen hätten eingestellt werden müssen, weil die Prognose auf erhebliche Gefahren für die öffentliche Sicherheit sich nicht realisiert hatte. Die Behörde für Inneres hat dagegen betont, daß die polizeilichen Feststellungen während der Versammlung auch Videoaufnahmen über den Gesamtverlauf gerechtfertigt hätten. Da tatsächlich nur noch ca. 5 Minuten aufgenommen wurden und es sich bei der Frage, ob Videoaufnahmen nach dem Versammlungsgesetz zulässig sind, um eine situationsabhängige Prognoseentscheidung handelt, erschien uns eine weitere Auseinandersetzung über diese Frage im Nachhinein nicht sinnvoll.

Die Ermittlungsverfahren, die aufgrund der Teilnahme an der Demonstration wegen Nötigung eingeleitet worden waren, sind inzwischen von der Staatsanwaltschaft eingestellt worden. Speicherungen in kriminalpolizeilichen Sammlungen aufgrund dieser Verfahren sind nach Überprüfung der staatsanwaltschaftlichen Einstellungsentscheidungen gelöscht worden.

17.8.2 Videoüberwachung am Hauptbahnhof

Im April 1993 wurden wir durch Presseberichte und auch Anfragen der Bahnpolizei auf die neu eingerichtete Melde- und Koordinierungsstelle für die verschie-

denen Videoüberwachungsanlagen im Hamburger Hauptbahnhof aufmerksam gemacht. Da die Bahnpolizei zum Bundesgrenzschutz gehört, mußten wir sie darauf verweisen, daß wir ihre datenschutzrechtlichen Fragen nicht beantworten können, sondern daß hierfür der Bundesbeauftragte für den Datenschutz zuständig ist. Aus unserer Sicht war jedoch von Interesse, ob die Koordinierungsstelle auf andere Videokameras hamburgischer Stellen, insbesondere der Polizei zurückgreift und unter welchen Bedingungen Aufnahmen an die Polizei weitergegeben werden.

Die Melde- und Koordinierungsstelle wird von der Betreuungsgesellschaft für den Hamburger Hauptbahnhof GmbH (BHH), einer Tochter der Hamburger Gesellschaft für Beteiligungsverwaltung (HGV), betrieben. Auf deren Einladung haben wir im Mai 1993 die mit der Videoüberwachung im Hauptbahnhof verbundenen datenschutzrechtlichen Fragen mit Vertretern der BHH, der Hamburger Hochbahn AG (HHA), der Deutschen Bundesbahn (DB), des Bundesgrenzschutz/Bahnpolizei (BGS) sowie der Polizei Hamburg erörtert und die Koordinierungsstelle besichtigt.

Die Videoanlage dient dem in der Bürgerschaftsdrucksache 13/8003 vom 9. April 1993 beschriebenen Betreuungskonzept. Danach soll sie folgende Aufgaben unterstützen:

— Einleitung von unmittelbar erforderlichen Maßnahmen im Zuständigkeitsbereich der Beteiligten (BHH, HHA und DB)

— Anforderung der Sonderreinigungsgruppe

— Koordinierung der Einsätze der Ordnungs- und Sicherheitskräfte sowie Einleiten dieser Einsätze bei akuten Gefahrensituationen

— Erfassung von Mängeln in der baulichen und technischen Ausstattung der Gesamtverkehrsanlage Hamburger Hauptbahnhof nach einer vorgegebenen Checkliste und deren Mitteilung an die Zuständigen.

Durch die Videoanlage sollen Störungen, die von Personen im Hauptbahnhof ausgehen, festgestellt und abgewehrt werden bzw. begangene Straftaten dokumentiert werden. Zum anderen sollen auch Verunreinigungen im Bereich des Hauptbahnhofs festgestellt werden, um Reinigungskräfte in den jeweiligen Zuständigkeitsbereichen zu benachrichtigen.

Zu den 22 Videomonitoren in der Melde- und Koordinationsstelle der BHH werden die Bilder von 21 Kameras der BHH, 17 Kameras der DB und 8 Kameras der HHA übermittelt. Die Monitore werden im Schichtbetrieb rund um die Uhr von Inspektoren der BHH überwacht. Die Kameras der BHH lassen sich von hier aus steuern (Zoomaufnahmen, Schwenks), die Kameras von DB und HHA können nur aus den dortigen Diensträumen gesteuert werden. Als Aufzeichnungsgeräte stehen zwei Langzeitrekorder mit einer Aufnahmekapazität von max. 72 Stunden zur Verfügung, ferner ein Videoprinter.

Die datenschutzrechtliche Bewertung der Anlage läßt sich folgendermaßen zusammenfassen:

Angesichts der Fülle der installierten Kameras ist aus Sicht der Betreiber eine routinemäßige Daueraufzeichnung weder sinnvoll noch vorgesehen, so daß sich das Problem der Zulässigkeit von Aufzeichnungen über rechtmäßige Benutzer des Hauptbahnhofgeländes (Recht am eigenen Bild) nicht stellt.

Es bestand Einvernehmen darüber, daß Aufzeichnungen mit Abbildungen von Personen aus Anlaß von Straftaten oder sonstigen Beeinträchtigungen der Betreiber der einzelnen Bereiche im Hauptbahnhof von der BHH entweder in Wahrnehmung des eigenen oder des ihr übertragenen Hausrechts zur Beweissicherung zulässig sind. Nach einer Mitteilung der BHH vom Oktober 1993 wurden zu diesen Zwecken bisher keine Aufzeichnungen gefertigt. Die Bandaufzeichnungen wären in diesen Fällen – neben den Zeugenaussagen der Inspektoren, die die Aufzeichnungen veranlaßt haben – Beweismittel zur Erstattung von Strafanzeigen und/oder zur Durchsetzung von Schadensersatzansprüchen.

Für diese Nutzungen von Videoaufzeichnungen erscheint es sinnvoll, ein geregeltes Verfahren für die Bandauswertungen vorzusehen. Insbesondere sollte dokumentiert werden, wer wann über welche Kamera eine Aufzeichnung veranlaßt hat und was mit dieser Aufzeichnung geschehen ist (Abgabe an...; Löschung am...). Eine entsprechende Dienstanweisung wurde erarbeitet.

Die Polizei Hamburg verfügt im Bereich des Hauptbahnhofs einschließlich der Bahnhofsvorplätze nicht über eigene Kameras. Die BHH greift daher nicht auf polizeiliche Videoaufzeichnungen zu.

Die Polizei ist neben der Verfolgung von Straftaten unter den in § 8 PolDVG genannten Voraussetzungen befugt, Aufzeichnungen über Personen zu fertigen. Sofern ein gesetzlich legitimiertes polizeiliches Interesse an der Nutzung der im Bereich des Hauptbahnhofs installierten Kameras im Einzelfall auftritt, liegt es – abgesehen von den Ausnahmefällen der Beschlagnahme nach der Strafprozeßordnung oder der Inanspruchnahme nach dem Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung (SOG) – im Ermessen der Verfügungsberechtigten, ob sie der Polizei die Aufnahmemöglichkeiten zur Verfügung stellen.

Nach Mitteilung der BHH vom Oktober 1993 hat die Polizei Hamburg die Anlage bisher nicht für eigene Zwecke in Anspruch genommen. Geschieht dies, muß allerdings gewährleistet sein, daß die Steuerung von der Aufnahme bis zur Aufzeichnung ausschließlich durch die Polizei erfolgt.

Die Überlassung derartiger personenbezogener Aufnahmen an die BHH wäre nur in den Fällen möglich, in denen die Polizei Daten an nicht-öffentliche Stellen übermitteln darf. Dies kann z. B. dann der Fall sein, wenn rechtliche Interessen von den Aufnahmen abhängen. Wenn im Einzelfall gezielte polizeiliche

Aufnahmen über bestimmte Personen erforderlich sein sollten, wären Personen, die nicht der Polizei angehören, bereits beim Aufnahmevorgang auszuschließen. Die Polizei bereitet eine interne Dienstanweisung hierzu vor.

17.9 Einsatz besonderer Befugnisse zur Datenerhebung

Das hamburgische Gesetz über die Datenverarbeitung der Polizei (PolDVG) und die durch das Gesetz zur Bekämpfung der Organisierten Kriminalität (OrgKG) novellierte Strafprozeßordnung lassen die Erhebung personenbezogener Daten mit verdeckten Methoden zu. Die einschlägigen Vorschriften der Strafprozeßordnung sind dann anwendbar, wenn der Verdacht besteht, daß eine Straftat bereits begangen worden ist (siehe unten 19.8). Das PolDVG ist anwendbar, wenn Straftaten noch nicht begangen worden sind, sondern ihre bevorstehende Begehung verhütet werden soll oder andere Gefahren abgewehrt werden sollen.

Im 11. TB (17.7) sind die einzelnen Befugnisse nach dem PolDVG beschrieben worden. Im folgenden werden daher nur noch die Zahlen für den Zeitraum zwischen September 1992 und September 1993 mit den Vergleichszahlen vom Vorjahr genannt.

Danach ist in 12 (Vorjahr 6) Fällen eine längerfristige Observation nach § 9 PolDVG angeordnet worden.

Anordnungen über den verdeckten Einsatz technischer Mittel nach § 10 Abs. 1 PolDVG sind in 37 (38) Fällen ergangen.

Es hat wie im Vorjahr keine Anordnungen zum Einsatz von verdeckten technischen Mitteln zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person in oder aus Wohnungen gegeben, die nach § 10 Abs. 2 PolDVG grundsätzlich dem Richter vorbehalten sind.

Die Behörde hat auch auf unsere Fragen nach Anordnungen für den Einsatz verdeckter Ermittler nach § 12 PolDVG und sog. V-Personen nach § 11 PolDVG geantwortet. Sie hat jedoch einer Veröffentlichung der Angaben über diesen Personenkreis wie im letzten Jahr nicht zugestimmt.

Gemeinsame Voraussetzung für die Anordnung dieser besonderen Methoden ist es, daß ihr Einsatz zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist. Ferner kann der Einsatz dieser Methoden – mit Ausnahme der verdeckten Datenerhebung aus Wohnungen nach § 10 Abs. 2 PolDVG – angeordnet werden, wenn Tatsachen die Annahme rechtfertigen, daß die Person sog. Straftaten von erheblicher Bedeutung begehen wird, zu deren Verhütung die verdeckte Datenerhebung erforderlich ist. Die Straftaten von erheblicher Bedeutung werden in § 1 Abs. 4 PolDVG abschließend aufgezählt. Es handelt sich dabei um eine Reihe von Verbrechen, also Straftaten, die mit einer Freiheitsstrafe von mindestens einem Jahr bedroht sind, sowie gewerbs- und bandenmäßige Straftaten.

Polizeiliche Beobachtungen nach § 13 PolDVG sind in 42 (66) Fällen angeordnet worden.

Eine Rasterfahndung auf der Grundlage von § 22 PolDVG hat wie im Vorjahr nicht stattgefunden.

17.10 Datenschutz für Polizeibedienstete

17.10.1 Mitteilungen über Strafanzeigen gegen Polizeibedienstete

Aufgrund der Schilderung im 14. Tätigkeitsbericht 1992 (4.1.3.5) des Landesbeauftragten für den Datenschutz Schleswig-Holstein sind wir erstmalig auf das Problem aufmerksam geworden, daß Bedienstete der Polizei durch polizeiinterne Regelungen erheblich schlechter gestellt sind als andere Angehörige des öffentlichen Dienstes. Diese Schlechterstellung tritt immer dann ein, wenn gegen Polizeibeamte Strafanzeigen gestellt werden.

1992 wurden 387 Ermittlungsverfahren gegen Polizeibedienstete eingeleitet, 291 aufgrund von Strafanzeigen von Bürgern, 96 von Amts wegen. Die weitaus überwiegende Anzahl dieser Ermittlungsverfahren wurden von der Staatsanwaltschaft mangels hinreichenden Tatverdachts eingestellt; es kam nur zu einer Verurteilung bei ebenfalls einem Freispruch (Bürgerschaftsdrucksache 14/4032). Zahlen über Ermittlungsverfahren gegen Bedienstete in anderen Bereichen der Verwaltung liegen uns nicht vor.

Für Angehörige des öffentlichen Dienstes gilt nach Nr. 15 der Anordnung über Mitteilungen in Strafsachen (MiStra), daß erst die Erhebung der öffentlichen Klage, das Urteil und der Verfahrensausgang dem Dienstherrn (in Hamburg dem Senatsamt für den Verwaltungsdienst) mitzuteilen sind. Eine vorherige Mitteilung bereits bei Einleitung eines Ermittlungsverfahrens kommt nach Nr. 2 Abs. 2 MiStra nur dann in Betracht, wenn sie wegen des erheblichen öffentlichen Interesses unerläßlich ist. In diesen Fällen ist der Betroffene über die Mitteilung regelmäßig zu unterrichten. Die Mitteilungen nach der MiStra erfolgen nicht durch die Polizei, sondern durch die Staatsanwaltschaft oder das Gericht.

Für Polizeibedienste gilt dagegen nach Teil 6 des Erlasses über die Meldung wichtiger Ereignisse (WE-Erlaß), daß sämtliche Strafanzeigen gegen Bedienstete der Polizei (einschließlich Verkehrsunfällen mit möglicher strafrechtlicher Relevanz) polizeiintern gemeldet werden müssen.

Diese Meldungen werden – personenbezogen – unabhängig von den Zuständigkeiten zur Ermittlungsführung an eine ganze Reihe von Führungsstellen des Polizeivollzugs (z. B. den Leiter des Amtes Polizei, den Leiter der Landespolizeidirektion, den Leiter des Landeskriminalamtes, Stellen des Führungsstabs der Landespolizeiverwaltung und des Amtes für Innere Verwaltung und Planung der Behörde für Inneres) gegeben. Adressaten sind auch weitere Führungsstellen anderer Bereiche und des örtlichen Polizeivollzugs, wenn Bedienstete der jeweiligen Organisationseinheiten betroffen sind, sowie zusätzlich die für Diszi-

plinarangelegenheiten zuständigen Dienststellen. Eine Unterrichtung der Betroffenen ist nicht vorgesehen.

Auf den ersten Blick sieht diese Regelung wie eine weite Streuung sensibler personenbezogener Daten ohne Beachtung der Zuständigkeiten für das konkrete Ermittlungsverfahren aus. Für diese Regelung bestehen allerdings auch gewichtige Gründe.

Die Meldungen sollen z. B. ermöglichen, daß organisatorische Maßnahmen zur Ermittlungsführung und Sachverhaltsaufklärung erfolgen. Als z. B. zu Beginn der achtziger Jahre der Verdacht aufkam, daß auch Polizeibeamte in einen Komplex von systematisch begangenen Eigentumsdelikten verwickelt seien, wurde eine eigene Sonderkommission zur Aufklärung dieses Verdachts eingerichtet.

Ferner sollen auch Sofortmaßnahmen aufgrund der Meldungen erfolgen, z. B. die Einziehung einer Dienstwaffe beim Verdacht auf strafbaren Gebrauch. Die Tatsache der Einleitung polizeilicher Ermittlungen muß ferner im Auswahl- und Ernennungsverfahren berücksichtigt werden, um zu vermeiden, daß Bedienstete in Unkenntnis laufender Ermittlungen befördert werden. Schließlich sollen die Meldungen auch der Vermeidung von Risiken in vergleichbaren Tätigkeitsbereichen dienen. Insgesamt ist die Regelung als Maßnahme zur Verhinderung des Vertrauensverlustes für die Polizei und auch zur objektiven Sachverhaltsdarstellung gedacht.

Andererseits ist diese Praxis rechtlich nicht abgesichert. Dies wäre erforderlich, denn die Mitteilungen über eingeleitete Strafermittlungsmaßnahmen greifen tief in das Recht auf informationelle Selbstbestimmung der Betroffenen ein. Auch der Gesichtspunkt der beamtenrechtlichen Fürsorgepflicht, auf den die Polizei und die Staatsanwaltschaft die behördeninternen Mitteilungen stützen, reicht als Rechtfertigung nicht aus, da er eine klare, die Interessen des Dienstherrn und der Betroffenen ausgleichende gesetzliche Regelung nicht ersetzen kann.

Das OLG Stuttgart hat in einer neueren Entscheidung eine polizeiinterne Mitteilungspraxis abgelehnt (veröffentlicht in Recht der Datenverarbeitung 1993 Seite 132 ff.). Obwohl in dem entschiedenen Fall ein gewichtiger Vorwurf in unmittelbarem Zusammenhang mit der dienstlichen Tätigkeit des Betroffenen erhoben wurde, hat das Gericht eine Unterrichtung des Dienstvorgesetzen für unzulässig erklärt, die ohne Entscheidung der zuständigen Staatsanwaltschaft erfolgte. Grundsätzlich muß nach dieser Gerichtsentscheidung mit der Erteilung von Auskünften bis zum Abschluß des Ermittlungsverfahrens gewartet werden. Wenn aus Sicht der Staatsanwaltschaft unverzüglich notwendige Maßnahmen oder Anordnungen des Dienstvorgesetzten ergehen müssen, kann dieser vor Abschluß des Ermittlungsverfahrens informiert werden. Bei seiner Entscheidung hat sich das Gericht an den geltenden Regelungen der MiStra und dem Regierungsentwurf für ein Justizmitteilungsgesetz orientiert, die die

Mitteilungsbefugnis jeweils der ermittlungsführenden Staatsanwaltschaft zuweisen (Nr. 4 MiStra; § 14 Einführungsgesetz zum Gerichtsverfassungsgesetz – EGGVG – in der Fassung des Entwurfs für ein Justizmitteilungsgesetz).

Der Gesetzentwurf sieht auch eine entsprechende Änderung des Beamtenrechtsrahmengesetzes vor. Dies spricht ebenfalls gegen die Heranziehung allgemeiner beamtenrechtlicher Grundsätze zur Rechtfertigung der gegenwärtigen Praxis.

Angesichts der insoweit übereinstimmenden untergesetzlichen Verwaltungsvorschriften, des Gesetzentwurfs und der Rechtsprechung haben wir Änderungen des derzeitigen polizeiinternen Mitteilungsverfahrens gefordert:

Im Unterschied zur bisherigen Regelung sollte hinsichtlich des Anlasses, des Zwecks und des Adressatenkreises der Meldungen differenziert werden. Es sollte grundsätzlich auf die Meldungen in den Fällen verzichtet werden, in denen keine besonderen dienstlichen Gründe ersichtlich sind, die die Meldungen erforderlich machen, z. B. in Privatklageverfahren und bei fahrlässigen Taten ohne besondere Folgen, wenn sie ohne Bezug zur Dienstausübung begangen wurden. Nach dem Entwurf für ein Justizmitteilungsgesetz scheiden Mitteilungen in diesen Fällen aus.

Die Polizei hat angekündigt, den Erlaß zu ändern. Danach sollen künftig Amtsdelikte und bei der Ausübung des Dienstes begangene Straftaten mitgeteilt werden. Meldungen über sonstige Ermittlungsverfahren ohne unmittelbaren Bezug zur Dienstausübung erfolgen nur noch bei Verbrechen oder bei Strafvorwürfen, die Zweifel an der Zuverlässigkeit oder Eignung der beschuldigten Beamten hervorrufen, sowie dann, wenn eine besondere Schädigung des Ansehens der Polizei hiermit verbunden ist. In der Sache entspricht diese Regelung dem Gesetzentwurf.

Die Erfordernisse, in Einzelfällen organisatorische Maßnahmen zur Ermittlungsführung zu treffen oder Risiken in vergleichbaren Tätigkeitsbereichen zu vermeiden, und auch die objektive Sachverhaltsdarstellung werden ohne unmittelbaren Personenbezug erfüllbar bleiben. Daher sollten die Meldungen über relevante Strafermittlungsverfahren gegen Bedienstete an den Kreis der Führungsstellen nur noch ohne Nennung des Namens des betroffenen Mitarbeiters erfolgen. Dabei ist allerdings nicht zu verkennen, daß sich etwa aufgrund einer im Einzelfall erforderlichen detaillierten Sachverhaltsschilderung und eines Hinweises auf die Organisationseinheit ein mittelbarer Personenbezug nicht ausschließen läßt. Jedenfalls wird jedoch durch den Verzicht auf die Namensnennung gegenüber einem großen Verteiler die unmittelbare Beeinträchtigung der Betroffenen vermieden.

Dem ist die Polizei nicht gefolgt. Sie will die personenbezogenen Meldungen auch an den Kreis der Führungsstellen und der im Amt für Innere Verwaltung und Planung Zuständigen beibehalten.

Für Sofortmaßnahmen und für Auswahl- und Ernennungsverfahren lassen die MiStra und das zukünftige Justizmitteilungsgesetz vorzeitige Meldungen wegen besonderer öffentlicher Interessen zu. Zu diesen Zwecken ist eine personenbezogene Mitteilung an die zuständigen Stellen vertretbar. Hierbei muß jedoch während eines laufenden Ermittlungsverfahrens der Entscheidungsvorbehalt der Staatsanwaltschaft gewahrt bleiben und der Betroffene regelmäßig unterrichtet werden.

Hierzu vertreten Polizei und Staatsanwaltschaft eine andere Auffassung. Sie meinen, die dienstrechtlichen Gesichtspunkte, die für die polizeiinternen Mitteilungen sprechen, seien von den strafverfahrensrechtlichen Regelungen zu trennen. Der Entscheidungsvorbehalt der Staatsanwaltschaft gelte nur für Meldungen an Dritte. Dies trifft weder nach der geltenden MiStra noch nach dem Entwurf für das Justizmitteilungsgesetz zu, die gerade die dienstrechtlich relevanten Mitteilungen betreffen und unter den Entscheidungsvorbehalt der Staatsanwaltschaft stellen.

In jedem Fall wird zu berücksichtigen sein, daß der Gesichtspunkt „Sofortmaßnahmen" eine Meldung vor Abschluß der Ermittlungen nur in Ausnahmefällen begründen kann. Da die weitaus überwiegende Anzahl von Ermittlungsverfahren gegen Polizeibedienstete eingestellt wird, handelt es sich in aller Regel um Fälle, in denen nach Abschluß der Ermittlungen eine Mitteilung nach der MiStra und dem Justizmitteilungsgesetz unterbleibt. Dann kann auch die Ausnahmeregelung nicht dazu führen, daß routinemäßig vor Abschluß der Ermittlungen Meldungen erfolgen.

Auch dies sieht die Polizei anders, da sie die — unserer Auffassung nach nicht stichhaltige — Meinung vertritt, strafprozessuale Mitteilungen und beamtenrechtliche Fürsorgepflicht seien jeweils unabhängig voneinander zu betrachten.

Eine Einschränkung der Mitteilungspraxis in dem von uns vorgeschlagenen Sinne ließe die strafprozessualen Ermittlungsbefugnisse der jeweils zuständigen Polizeidienststellen unberührt, so daß die rechtlich gebotene Aufklärung des Tatvorwurfs immer gewährleistet bliebe.

Wir haben ferner vorgeschlagen, den bisherigen Adressatenkreis der Meldungen daraufhin zu überprüfen, ob tatsächlich alle genannten Stellen die Informationen brauchen. Insbesondere bei den personenbezogenen Mitteilungen für Sofortmaßnahmen muß sichergestellt werden, daß die Mitteilung nur an die Stelle geht, die auch die Sofortmaßnahmen treffen kann. Eine weitere „Streuung" der Mitteilungen sollte dagegen unterbleiben.

Die vorgesehene Neuregelung des Erlasses sieht zwar die Streichung einiger weniger Adressaten vor; dafür sollen jedoch – anders als bisher – sämtliche Meldungen auch an den Staatsrat der Behörde für Inneres gerichtet werden, der nach der bestehenden Regelung nur in besonderen Fällen zu unterrichten war. Diese Ausweitung ist nicht nachvollziehbar, da keine Gründe ersichtlich sind, warum alle personenbezogenen Mitteilungen an die Behördenleitung

gerichtet werden müssen, wenn die im Einzelfall zuständigen Funktionsträger parallel unterrichtet werden.

17.10.2 Sonstige Mitteilungen

Der polizeiinterne Erlaß über Meldungen „wichtiger Ereignisse" sieht ferner vor, daß Mitteilungen erfolgen über Freitodfälle und -versuche, Verkehrsunfälle mit wesentlichem Sachschaden, an denen Polizeibedienstete dienstlich beteiligt waren, sowie wesentliche Dienstunfälle.

Für die Mitteilung von Ereignissen, die nicht zu Strafermittlungsverfahren führen, gibt es aufgrund von geltenden oder zukünftigen Rechtsvorschriften keine Grundlage. Insbesondere die hier vorgesehene routinemäßige personenbezogene Mitteilung von Freitodfällen und Freitodversuchen von Polizeibediensteten an einen großen Empfängerkreis ist bedenklich. Die Polizei will sie jedoch beibehalten. Dies bedarf weiterer Erörterungen, die bei Redaktionsschluß noch nicht abgeschlossen waren.

17.10.3 Speicherung von Polizeibediensteten in polizeilichen Dateien

Überrascht hat uns die Mitteilung, daß in über 20 Fällen sogar Speicherungen im polizeilichen Auskunftssystem (POLAS) und den dazugehörigen Kriminalakten über Polizeibeamte, die sich noch im Dienst befinden, vorliegen. Dies erschien uns widersprüchlich, da eine Speicherung immer die Annahme von Wiederholungsgefahr voraussetzt. Warum sollte ein Beamter seinen Dienst weiter verrichten können, wenn der Dienstherr zur Einschätzung kommt, daß die Gefahr besteht, er werde in Zukunft weitere Straftaten begehen?

Die Polizei hat jedoch zutreffend darauf hingewiesen, daß auch eine begründbare Prognose auf zukünftige Straftaten der Betroffenen beamtenrechtlich nicht zur Entlassung ausreicht. Lediglich eine rechtskräftige Verurteilung zu einer Freiheitsstrafe von einem Jahr oder in besonderen Fällen zu mindestens sechs Monaten führt zur Beendigung des Beamtenverhältnisses. Somit kann es Fälle geben, in denen die Voraussetzungen für die Speicherung von aktiven Polizeibeamten in polizeilichen Dateien vorliegen.

Auf die Datensätze der Betroffenen können jedoch nicht alle Kollegen zugreifen, sondern nur eine sehr begrenzte Anzahl von zuständigen Dienststellen.

18. Verfassungsschutz

18.1 Entwurf eines Hamburgischen Verfassungsschutzgesetzes

Die Verfassungsschutzbehörden des Bundes und der Länder greifen zur Erfüllung ihrer Aufgaben in Persönlichkeitsrechte der Betroffenen ein, insbesondere in das Recht auf informationelle Selbstbestimmung. Die Anforderungen aus dem Volkszählungsurteil sind in diesem Bereich mit erheblichen Verzögerun-

gen umgesetzt worden. Während das Bundesverfassungsschutzgesetz (BVerfSchG) am 30. Dezember 1990 in Kraft getreten ist, ist die Novellierung des Hamburgischen Verfassungsschutzgesetzes noch nicht abgeschlossen. Das derzeit geltende Gesetz vom 13. Februar 1978 erfüllt nicht die Anforderungen des Volkszählungsurteils nach einer bereichsspezifischen gesetzlichen Regelung.

Im Berichtsjahr ist der Entwurf des Hamburgischen Verfassungsschutzgesetzes auf Behördenebene abgestimmt worden. Der Senat hat dann den Gesetzentwurf der Bürgerschaft zugeleitet. Die parlamentarische Beratung steht noch bevor. Aus datenschutzrechtlicher Sicht konnten in Teilbereichen erhebliche Fortschritte für das Recht auf informationelle Selbstbestimmung erzielt werden, wenn auch Schwächen des Entwurfes nicht zu übersehen sind.

18.1.1 Einzelperson als Bestrebung

Der Entwurf geht nach wie vor davon aus, daß auch isolierte Einzelpersonen Bestrebungen im Sinne des Verfassungsschutzgesetzes sein können, so daß sie Objekt der Tätigkeit des Verfassungsschutzes werden können. Allerdings wurde die relativ weite Formulierung des ersten Entwurfes, der sich insoweit an den entsprechenden Formulierungen des Bundesverfassungsschutzgesetzes orientierte, deutlich präzisiert (vgl. 11. TB, 18.1).

Auch die Regelung der Zusammenarbeit mit anderen Behörden, insbesondere über die dortige Akteneinsicht durch das Landesamt für Verfassungsschutz, konnte weiter verbessert werden. Die Einsichtnahme ist nur noch zulässig, wenn die Aufklärung auf andere Weise nicht möglich erscheint und die betroffene Person durch eine anderweitige Aufklärung unverhältnismäßig beeinträchtigt würde. Insbesondere ist klargestellt worden, daß dann, wenn der Akteneinsicht besondere gesetzliche Geheimhaltungsvorschriften oder ein Berufsgeheimnis entgegenstehen, die Akteneinsicht unzulässig ist. Auch sind alle Einsichtnahmen unabhängig davon, ob sie inhaltlich erfolgreich sind oder nicht, zu protokollieren.

18.1.2 Speicherung Jugendlicher

Problematisch ist die immer noch vorgesehene Möglichkeit, Minderjährige zu speichern, die älter als 14 Jahre sind. Zwar ist die Datenverarbeitung, insbesondere die Einspeicherung in das bundesweit für Verfassungsschutzbehörden zugängliche System NADIS, nur beschränkt möglich. Auch ist eine verkürzte Überprüfungs- und Löschungsfrist für derartige „Jugendsünden" vorgesehen. Es sollte aber in der parlamentarischen Beratung erwogen werden, die Speicherung von Jugendlichen ganz auszuschließen.

18.1.3 Unterscheidung von Kontaktpersonen und Beobachtungspersonen

Insbesondere durch die fortschreitende Automatisierung im Landesamt für Verfassungsschutz könnte die Unterscheidung zwischen Beobachtungspersonen

und sonstigen Personen zukünftig problematisch werden. Bisher ist z.B. der Bäcker, bei dem die Mitglieder eines Beobachtungsobjekts regelmäßig Brötchen einkaufen, nur in den Sachakten im Rahmen von Observationsberichten möglicherweise erwähnt. Der Zugriff auf den Namen des Bäckers ist bisher aber direkt nicht möglich, da er in der Referatsarbeitskartei (RAK) nicht verzeichnet ist und auch sonst ein alphabetischer Namensindex insoweit nicht existiert. In der RAK werden nur diejenigen Personen gespeichert, die in den beobachteten Bestrebungen tätig sind.

Sofern die Automatisierung – vor allem durch die Möglichkeit der Volltextrecherche – nicht nur den Bereich der RAK, sondern auch das generelle Schreibwerk des Verfassungsschutzes umfaßt, würde auch der Name des Bäckers maschinell suchfähig werden. Damit würde die Trennung zwischen den in Bestrebungen tätigen Personen, die zulässigerweise vom Verfassungsschutz ins Blickfeld genommen werden, und unbescholtenen Personen, die nicht in das Blickfeld des Verfassungsschutzes gelangen sollen, aufgehoben. Wir haben uns dafür ausgesprochen, daß dies durch geeignete Vorkehrungen verhindert wird. Das Landesamt für Verfassungsschutz erwägt, auf die Möglichkeiten der Volltrextrecherche insbesondere bei der RAK zu verzichten.

18.2 Sicherheitsüberprüfungsgesetz

Bisher sind die Voraussetzungen und das Verfahren zur Durchführung einer Sicherheitsüberprüfung, die Umstände, die ein Sicherheitsrisiko begründen, und die Folgen für Beschäftigte bei Vorliegen eines Sicherheitsrisikos noch nicht in gesetzlichen Vorschriften geregelt. Bei der Sicherheitsüberprüfung wird nicht nur anhand der Karteien und Dateien von Polizei und Verfassungsschutz festgestellt, ob ein Sicherheitsrisiko vorliegen könnte. In Abhängigkeit z.B. vom Grad der Vertraulichkeit der Dokumente, auf die der Mitarbeiter Zugriff haben soll, werden auch Ausforschungen im privaten Bereich durch Befragung von Dritten durchgeführt. Derartig intensive Eingriffe in das informationelle Selbstbestimmungsrecht der betroffenen Mitarbeiter bedürfen einer spezialgesetzlichen Grundlage. Eine solche fehlt auf Bundes- und Landesebene.

18.2.1 Entwurf der Bundesregierung

Der Bundestag hat am 2. Dezember 1993 den Entwurf eines Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes verabschiedet. Aus der Begründung des Entwurfes zu § 14 Abs. 4 Sicherheitsüberprüfungsgesetz läßt sich entnehmen, daß die Ablehnung der Erteilung eines Sicherheitsbescheides nicht als Verwaltungsakt anzusehen ist, obwohl die Versagung des Sicherheitsbescheides unter Umständen massive Auswirkungen auf den Betroffenen haben kann bis hin zum Verlust des Arbeitsplatzes.

Dagegen hat das Oberverwaltungsgericht Münster in einer Entscheidung vom 29. April 1993 sowohl die Erteilung als auch den Widerruf eines Sicherheitsbe-

scheides als Verwaltungsakt angesehen. Im Interesse der Rechtsklarheit sollte die Verwaltungsaktqualität des Sicherheitsbescheides ausdrücklich im Gesetz normiert werden, damit der Betroffene die Rechtmäßigkeit eines Bescheides verwaltungsgerichtlich klären lassen kann.

Positiv ist zu werten, daß zwischen der Sicherheitsakte und der Personalakte eine strikte Trennung besteht. Dadurch soll gewährleistet werden, daß Erkenntnisse, die nur der sicherheitsmäßigen Beurteilung dienen, nicht für andere personalverwaltende Maßnahmen genutzt werden können. Die personalverwaltende Stelle erhält dementsprechend keine Befugnis zur Einsicht in die Sicherheitsakte.

Unter gewissen Voraussetzungen kann der Betroffene Einsicht in die Sicherheitsakte nehmen. Diese Möglichkeit zur Akteneinsicht im sensiblen Bereich der Sicherheitsüberprüfung sollte dem Betroffenen ohne Einschränkung offen stehen.

18.2.2 Einbeziehung der Lebenspartner

Auch nach dem jetzigen Entwurf können hinsichtlich des Lebenspartners eines Mitarbeiters Karteien geprüft werden, ohne daß dies von der Zustimmung des betroffenen Lebenspartners abhängig ist. Lediglich dann, wenn diese Einsichtnahme Anhaltspunkte für ein Sicherheitsrisiko ergibt, ist die Zustimmung des betroffenen Lebenspartners für weitergehende Ermittlungen notwendig.

Schon die Einbeziehung in der Form der Karteieinsicht stellt einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Von daher ist anzustreben, daß auch die Durchsicht von Karteien nur mit Einverständnis des einbezogenenen Lebenspartners erfolgen darf.

18.3 Referatsarbeitskartei des Landesamtes für Verfassungsschutz (RAK)

Der Berichtszeitraum war gekennzeichnet durch den Übergang von der bisher manuell geführten RAK zu dem neuen automatisierten System.

Mehrere Vorgänge, u.a. auch Eingaben über die Speicherung von Personen, konnten nicht zu unserer Zufriedenheit abgeschlossen werden. So blieb bis zuletzt die Speicherung von Einzelfällen kontrovers. Das Landesamt für Verfassungsschutz hielt die Speicherung aufrecht und erteilte darüber hinaus auch keine Zustimmung zur Bekanntgabe der Speicherungsinhalte durch uns an die Betroffenen.

18.3.1 Prüfung der manuellen RAK

Der Hamburgische Datenschutzbeauftragte hat die manuell geführte RAK einer intensiven Prüfung unterzogen. Dabei wurde zunächst eine umfangreiche Stichprobe gezogen. Die in dieser Stichprobe enthaltenen Speicherungen wurden dann auf die Einhaltung datenschutzrechtlicher Bestimmungen

geprüft. In mehreren Einzelfällen ergab die Prüfung, daß Datensätze sofort zu löschen waren. Bei der Prüfung trat überdies eine Reihe von strukturellen Mängeln zu Tage. So war z. B. die Einhaltung von Prüffristen aufgrund eines methodischen Fehlers nicht gewährleistet.

Auch wurden mehrere Fälle festgestellt, wo nach alten Verkartungsplänen zulässige Speicherungsinhalte mittlerweile mehrere interne Prüfungen ohne Löschungen überstanden hatten, obwohl zwischenzeitlich derartige Umstände nach den neuen Verkartungsplänen nicht (mehr) hätten gespeichert werden sollen. Diese Umstände hätten früher gelöscht werden müssen.

Das Landesamt für Verfassungsschutz hat nach Bekanntgabe der Zwischenergebnisse, verbunden mit unserer Ankündigung, eine weitere Stichprobe zu ziehen, von sich aus eine Vollrevision der gesamten manuellen Kartei durchgeführt. Diese Vollrevision war durch die Prüfung initiiert worden und wurde auch im wohlverstandenen Eigeninteresse des Landesamtes für Verfassungsschutz zur Reduktion des Einleseaufwandes im automatisierten Verfahren durchgeführt. Dabei wurden 2.786 Datensätze gelöscht – ein Erfolg für den Datenschutz und die effektivere, um Ballast reduzierte Arbeit des Landesamtes für Verfassungsschutz. Eine danach von uns gezogene vergleichbare Stichprobe wies die dargestellten Mängel nicht auf.

18.3.2 Automationsvorhaben RAK

Die im 11. TB (18.3) dargestellten Probleme hinsichtlich der strukturellen Unsicherheiten der automatisierten RAK und des Aufwandes für deren Beseitigung haben sich bisher bestätigt. Das Landesamt für Verfassungsschutz hat sich die Sicherheitsanforderungen, die vom Hamburgischen Datenschutzbeauftragten aufgestellt wurden, zu eigen gemacht. Bisher erfüllt das System die Sicherheitsanforderungen noch nicht. Die Arbeiten sind allerdings noch nicht abgeschlossen. Auch scheint der manuelle Aufwand der Korrektur maschinell eingelesener Datensätze erheblich zu sein.

Offen ist auch noch die unter 18.1 beschriebene Differenzierung zwischen Kontaktperson und Beobachtungsperson und die Speicherung derartiger Personen in den Systemen des Landesamtes für Verfassungsschutz. In der RAK sollen Kontaktpersonen jedenfalls nicht gespeichert werden. Es wird nach neuesten Überlegungen erwogen, auf die Möglichkeit der Volltextrecherche zu verzichten.

18.4 Sicherheitsüberprüfung von Beschäftigten

Bei einer Prüfung der Datei über diejenigen Personen, die einer Sicherheitsüberprüfung unterzogen worden sind und eine sicherheitsrelevante Tätigkeit ausüben, waren seinerzeit gravierende Mängel in der Datensicherheit festgestellt worden (11. TB, 18.2).

Das Landesamt für Verfassungsschutz hatte mitgeteilt, daß die Mängel bis Oktober 1992 beseitigt sein sollten. Bei einer Prüfung im Oktober 1993 wurde festgestellt, daß die ein Jahr zuvor beschriebenen Mängel noch immer nicht beseitigt worden waren. Überdies waren neue Mängel im Bereich der technischen Datensicherheit hinzugekommen. Wir haben erneut zur Beseitigung der Mängel aufgefordert und kurzfristig Abhilfe erwartet, damit eine Beanstandung vermieden werden kann. Bei einer weiteren Nachschau wurde festgestellt, daß die Mängel beseitigt worden waren.

19. Justiz

19.1 Lauschangriff

Der Lauschangriff zur Strafverfolgung stellt in einer ganzen Kette von neuartigen Eingriffen in Grundrechte einen weiteren Schritt zum Verlust von individuellen Freiheitsrechten dar (siehe 1.1 und 1.2 sowie 11. TB, 19.1).

Die Antwort auf die Frage, ob die Beschränkung des Freiheitsrechts der Unverletzlichkeit der Wohnung gerechtfertigt ist oder nicht, muß grundsätzlich abwägen zwischen der Intensität des Eingriffs, dem angenommenen Gefahrenpotential, den Erfolgsaussichten einer Abwehr und etwaigen Alternativen.

Die Intensität des Eingriffs durch den Lauschangriff ist immens. Der Bundesgerichtshof hat es als einen Verstoß gegen die Menschenwürde angesehen, wenn der Staat für sich das Recht in Anspruch nehmen würde, die im engsten Familienkreis geführten Gespräche zu kontrollieren. Die Möglichkeit, Empfindungen, Gefühle, Ansichten oder Eindrücke von Erlebnissen zum Ausdruck bringen zu können, wäre unerträglich behindert, wenn die Angst bestehen müßte, daß staatliche Behörden die Unterhaltung überwachen. Dem Bürger müsse ein Innenraum verbleiben, der ihm um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen verbleiben muß. In diesen zentralen unantastbaren Bereich des allgemeinen Persönlichkeitsrechts greift der Lauschangriff ein.

Betrachtet man die mit der Einführung des Lauschangriffs beabsichtigte Bekämpfung der organisierten Kriminalität, so ist festzustellen, daß diese eine erhebliche Gefahr für die Gesellschaft darstellt. Die Frage, ob wir bereits heute Zustände haben, die keine Alternative zur Einführung des Lauschangriffes lassen, ist aber weiter umstritten. Bisher mangelt es jedenfalls an eindeutigen Fakten, die die Notwendigkeit dieses schweren Eingriffs offensichtlich machen. Daher muß besonderer Bedacht auf die Erfolgsaussichten bzw. die Entwicklung von Alternativen gelegt werden. Dabei ist festzustellen, daß die Erfolgsaussichten als eher gering anzusehen sind. Bei Tätern der organisierten Kriminalität ist zu erwarten, daß sie technische Schutzmaßnahmen nutzen oder entwickeln werden, daß sie Probleme bei „Waldspaziergängen" besprechen, daß sie abhörsicher im D-Netz telefonieren usw.. Auch ist wie bei der Telefonüberwachung zu erwarten, daß die Betroffenen eine kodierte Sprache entwickeln werden, die eine beweiskräftige Überführung sehr schwer macht.

Insgesamt läßt sich feststellen, daß die Betroffenen bereits heute über effektive Gegenstrategien verfügen. Demnach steht einer Gefahrenprognose eine geringe Effizienz der Maßnahmen bei hoher Eingriffsintensität gegenüber. Dabei ist insbesondere zu berücksichtigen, daß durch einen Lauschangriff unvermeidlich die Rechte einer Vielzahl von Bürgern betroffen werden, die oft unbeteiligt oder unschuldig sind.

Vorzuziehen wären dagegen Alternativen, während bisher die ganze Diskussion von dem empfindlichsten Punkt der organisierten Kriminalität, dem Geldfluß, ablenkt. Organisierte Kriminalität ist darauf angewiesen, die im Regelfall als Bargeschäft abgewickelten Vorgänge in den regulären Wirtschaftskreislauf einzuschleusen und damit das Geld zu waschen. Der Zugriff auf das Bank- und Steuergeheimnis würde bei relativ geringer Eingriffsintensität die organisierte Kriminalität vor erheblich größere Probleme stellen, als der Lauschangriff.

Die geringere Eingriffsintensität ergibt sich zum einen daraus, daß die Wohnung und das allgemeine Persönlichkeitsrecht durch das Grundgesetz geschützt sind, nicht aber das Steuer- und Bankgeheimnis. Zum anderen hat ein Zugriff auf die Finanzen des Betroffenen geringe oder keine Auswirkungen auf den innersten Lebensbereich, zumal der Betroffene ggf. durch Nachweis des legalen Gelderwerbs den Eingriff beenden kann. Diese Form des Eingriffs hat die überwiegende Mehrzahl der Bürger ganz im Gegensatz zu dem Lauschangriff nicht zu fürchten, da sie über illegale Einnahmequellen im Regelfall nicht verfügen.

Die Konferenz der Datenschutzbeauftragten hat sich am 26./27. Oktober 1993 mit dem Lauschangriff befaßt und an der Entschließung vom 1./2. Oktober 1992 festgehalten. In dieser Entschließung hatten die Datenschutzbeauftragten (bei Gegenstimme Bayern) sich gegen die Zulassung des Lauschangriffs auf Privatwohnungen zur Strafverfolgung ausgesprochen.

Außerdem haben die Datenschutzbeauftragten begrüßt, daß der Landtag Mecklenburg-Vorpommern am 20. Oktober 1993 einen Beschluß mit breiter Mehrheit zum Wohnungsbegriff gefaßt hat, der ihrer Entschließung entspricht. In dem Landtagsbeschluß heißt es ausdrücklich: „Der engste Bereich privater Lebensgestaltung soll dabei nicht angetastet werden."

19.2 Justizmitteilungsgesetz

Auch 10 Jahre nach dem Volkszählungsurteil fehlt es an einer bereichsspezifischen Regelung der Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen. Bisher machen Gerichte, überwiegend aufgrund bundeseinheitlicher Verwaltungsvorschriften, Mitteilungen an Gerichte, Staatsanwaltschaften und andere öffentliche Stellen von der Einleitung und dem Ausgang von Straf- und Zivilverfahren. Der Umfang der Übermittlungen ist beträchtlich und reicht von

Mitteilungen über den Eingang von Räumungsklagen betreffend Wohnungen an die Sozialämter bis zur Mitteilung über Strafverfahren gegen Beamte an deren Dienstherren.

Die Vielzahl der möglichen Datenübermittlungen stellt ein besonderes Problem deshalb dar, weil die ursprüngliche Datenerhebung z. B. aus der Tätigkeit der Polizei bereichsspezifisch streng durchgeregelt ist. Die mit erheblichen Eingriffen in Bürgerrechte ermittelten Daten werden aber dann aufgrund relativ großzügiger Regelungen durch die Gerichte an Stellen der öffentlichen Verwaltung, aber auch an private Stellen verteilt. Dies hat für den Betroffenen erhebliche Folgen, die über die mit einem Strafverfahren notwendigerweise verbundenen Auswirkungen hinausgehen. So sehen die Mitteilungen in Strafsachen (MiStra) z. B. vor, daß die Tatsache der Anklageerhebung gegen einen Beamten an seinen Dienstherren weiterzuleiten ist – mit unter Umständen massiven Folgen für seinen Arbeitsplatz. Derartige Folgen können nur teilweise rückgängig gemacht werden, wenn der Betroffene z. B. später gerichtlich freigesprochen wird.

Der Gesetzentwurf, zu dem inzwischen der Bundesrat Stellung genommen hat und die Bundesregierung eine Gegenäußerung abgegeben hat, stellt gegenüber den bisherigen Verfahren nur eine geringfügige Verbesserung dar. Im großen und ganzen werden die bisher sehr weitgehenden Übermittlungsbefugnisse nicht entsprechend den Grundzügen des Volkszählungsurteils eingeschränkt. Vielmehr wird die bisherige Praxis überwiegend gesetzlich festgeschrieben.

Über diese Gesamtbeurteilung können auch die kleinen Verbesserungen wie eine Nachberichts- oder Berichtigungspflicht bei überholten oder falschen Daten nicht hinwegtäuschen. Zu erwähnen ist hierbei auch die Unterrichtung des Betroffenen über die erfolgten Datenübermittlungen sowie die Verlagerung eines Teils der Übermittlungsentscheidungen auf Richter oder Staatsanwälte. Positiv hervorzuheben ist, daß nunmehr ein Rechtsschutz gegen die Anordnung von Mitteilungen vorgesehen ist.

Bedauerlich ist, daß der Entwurf des Justizmitteilungsgesetzes im Bereich der Strafsachen lediglich Mitteilungsbefugnisse regelt, die erst durch Verwaltungsvorschriften zu Mitteilungspflichten werden. Damit ist im Rahmen des Gesetzgebungsverfahrens unklar, wie im Detail die Mitteilungspflichten gehandhabt werden sollen.

Das Wesentliche soll offensichtlich wie bisher in Verwaltungsvorschriften festgeschrieben werden. Ob mit dieser Konstruktion den Grundsätzen des Volkszählungsurteils nach einer bereichsspezifischen gesetzlichen Regelung Rechnung getragen werden kann, muß bezweifelt werden. Es bleibt abzuwarten, ob und wann der Gesetzentwurf verabschiedet wird.

19.3 Registerverfahrensbeschleunigungsgesetz

Das Registerverfahrensbeschleunigungsgesetz betrifft verschiedene, bisher überwiegend manuell geführte Register wie das Grundbuch, das Handels- und Genossenschaftsregister und weitere Verzeichnisse.

Um die wirtschaftliche Entwicklung in den neuen Ländern zu fördern, sollen durch den Einsatz von EDV und die Straffung von Verfahren verwaltungsmäßige Abläufe beschleunigt werden. Dieses unterstützungswürdige Ziel wird allerdings weniger dadurch erreicht, daß Abläufe gestrafft werden, als vielmehr dadurch, daß eine Reihe von Auskunftserteilungen nunmehr verstärkt in Selbstbedienung erfolgen sollen. Dies hat zur Folge, daß datenschutzrechtlich bisher von Behördenmitarbeitern durchgeführte Prüfungen, ob der Auskunftssuchende z. B. ein berechtigtes Interesse an der Auskunftserteilung hat, zukünftig tendenziell entfallen.

So sind z. B. Möglichkeiten für Online-Abrufverfahren vorgesehen. Ein solches Verfahren kann für öffentliche, aber auch nicht-öffentliche Stellen zugelassen werden. Dabei wird die bisherige Überprüfung, ob der Anfragende im Einzelfall an einer Einsicht ein berechtigtes Interesse hat, ersetzt durch eine generalisierende Betrachtung im Rahmen eines Genehmigungsverfahrens. Es bestehen starke Zweifel daran, ob die differenzierten Überlegungen eines Grundbuchbeamten im Einzelfall noch pauschal in einem Genehmigungsverfahren für eine unbeschränkte Zahl von Zugriffen erfaßt werden können, ohne daß die Regelungen des § 12 Grundbuchordnung (GBO) über den Nachweis eines berechtigten Interesses leerlaufen. Die vorgesehenen Schutzvorschriften werden sich technisch im Online-Verfahren kaum verwirklichen lassen.

Auch auf die anderen Register wie das Handelsregister, das Vereinsregister und das Genossenschaftsregister soll ein Online-Zugriff – zum Teil unter noch weiter erleichterten Voraussetzungen – ermöglicht werden.

Diese im Einzelfall nicht besonders problematisch erscheinenden Zugriffsmöglichkeiten bedeuten aber im Ergebnis einen Schritt weiter hin zum gläsernen Menschen. Zwar kann bisher unter bestimmten Voraussetzungen oder auch voraussetzungslos bei den entsprechenden Registern eine Abfrage schriftlich oder durch persönliches Erscheinen in der registerführenden Stelle erfolgen. Dieser sachliche Aufwand (Brief schreiben, Antwort abwarten, Antworten auswerten und gegebenenfalls in ein EDV-System eingeben) stellt aber auch einen gewissen Schutz dar. Bemerkenswert ist auch, daß der Gesetzentwurf die Probleme eher pauschal regelt und die Detailregelung Rechtsverordnungen überläßt. Dieses Verfahren hat den Nachteil, daß – je nach Sachlage – im Gesetzentwurf bei datenschutzrechtlichen Bedenken darauf hingewiesen wird, dies sei im Rahmen der Rechtsverordnung zu klären. Es gehört nur eine geringe Prognosefähigkeit dazu, daß bei dem Erlaß der Rechtsverordnung viele im Gesetz ungeregelte Punkte nicht mehr berücksichtigt werden können.

19.4 Zentralkartei der Staatsanwaltschaft

Die Zentralkartei der Staatsanwaltschaft wurde einer datenschutzrechtlichen Querschnittsprüfung unterzogen. Bei dem technisch veralteten und tendenziell abgängigen System wurden erhebliche Mängel festgestellt.

Einer der Mängel betrifft das Auskunftsverhalten der Zentralkartei. Für die Zentralkartei existiert eine Liste von Behörden, die in unterschiedlichem Umfang telefonisch abfrageberechtigt sind. Insgesamt umfaßt der Personenkreis, der direkt telefonisch Auskunft aus der Zentralkartei erlangen kann, mehrere hundert Personen außerhalb von Staatsanwaltschaft und Gerichten. Angesichts der Vielzahl von Abfragen sind erhebliche Mängel bei der Prüfung, ob der Abfragende dazu berechtigt ist, sowie bei der Dokumentation der Abfrage festzustellen, zumal die Zentralkartei generell unzureichend besetzt ist.

Wir haben darauf hingewiesen, daß die Form der Auskunftserteilung nach Art und Umfang nicht hinnehmbar ist. Das Risiko, daß nicht zur Abfrage Berechtigte eine Abfrage durchführen und an personenbezogene Daten gelangen, die durchaus sensibel sein können, ist beträchtlich. Die Staatsanwaltschaft hat zugesagt, eine Straffung und Änderung der Abfrageberechtigungen und der Art und Weise des Vorgehens vorzunehmen. Zwischen der Staatsanwaltschaft und dem Hamburgischen Datenschutzbeauftragten besteht Einvernehmen darüber, daß diese Form der Auskunftserteilung deutlich verändert werden muß.

Aber auch hinsichtlich der Inhalte wurden erhebliche Mängel festgestellt. So werden Datensätze zwar nach Ablauf von 5 Jahren gesperrt, was datenschutzrechtlich in seiner Wirkung einer Löschung gleichkommen soll. Gleichwohl wird aber in Einzelfällen über gesperrte Daten Auskunft erteilt. Ein weiteres Problemfeld stellen die beträchtlichen Rückstände unerledigter Mitteilungen dar, die die Vollständigkeit und Richtigkeit der Daten in der Zentralkartei der Staatsanwaltschaft doch sehr in Frage stellen. So wurde bei der Prüfung ein Rückstand von ca. 20.000 Vorgängen festgestellt. Überwiegend handelt es sich bei den Rückständen um die Erfassung der Mitteilung über den Ausgang eines Strafverfahrens.

Neben dem kurzfristigen Ersatz der abgängigen Zentralkartei ist eine längerfristige Automatisierung im Bereich der Staatsanwaltschaft vorgesehen. Dieses Automatisierungsvorhaben, das von der Justizbehörde im Zusammenarbeit mit der Staatsanwaltschaft entwickelt wird, soll die Funktionen einer Zentralkartei, eines Vorgangsverwaltungssystems und der Vorgangsbearbeitung umfassen. Datenschutzrechtlich wird darauf Bedacht genommen werden müssen, daß die drei Funktionen Aktenindex, Vorgangsbearbeitungssystem und Namensindex funktional sauber voneinander getrennt werden, damit jeder Mitarbeiter der Staatsanwaltschaft nur auf die für seine konkrete Aufgabenerfüllung notwendigen Informationen zugreifen kann.

Positiv ist zu vermerken, daß bei der Entwicklung dieses Verfahrens der Hamburgische Datenschutzbeauftragte rechtzeitig im Sinne der Beteiligungsrichtlinie unterrichtet wurde. Dies kann nicht von allen Bereichen und Vorhaben der Justizbehörde gesagt werden. So wurde die teilweise Verlagerung von Zuständigkeiten für die Gewährung von Akteneinsicht zu Forschungsszwecken von der Staatsanwaltschaft hin zur Justizbehörde dem Hamburgischen Datenschutzbeauftragten eher zufällig bekannt. Auch wurde die Entwicklung und Installation eines Programms, welches personenbezogene Daten von Strafgefangenen erfaßt und verwaltet, dem Hamburgischen Datenschutzbeauftragten erst durch eine Dateimeldung bekannt.

19.5 Gnadenwesen

Auf die Ausübung des Gnadenwesens findet gemäß § 2 Abs. 5 HmbDSG das Hamburgische Datenschutzgesetz keine Anwendung. Bei der Vorbereitung einer Gnadenentscheidung werden jedoch personenbezogene Daten, die als sensibel einzustufen sind, in beträchtlichem Umfang verarbeitet.

Aus dem Volkszählungsurteil ist abzuleiten, daß dieser Eingriff in das informationelle Selbstbestimmungsrecht einer normenklaren gesetzlichen Regelung bedarf. Die Herausnahme aus dem Geltungsbereich des Hamburgischen Datenschutzgesetzes ist 10 Jahre nach Erlaß des Volkszählungsurteils nur dann akzeptabel, wenn eine bereichsspezifische Regelung in einem speziellem Gesetz über das Gnadenwesen getroffen wird.

Eine solche gesetzliche Regelung müßte zum einen die im Rahmen der Gnadenentscheidung zulässigerweise zu ermittelnden Daten abschließend beschreiben, die Datenerhebung von der Einwilligung des Betroffenen abhängig machen und das Verhältnis zwischen dem Hamburgischen Datenschutzgesetz und dem Gnadengesetz regeln. Es müßte auch die Frage geregelt werden, ob und ggf. unter welchen Voraussetzungen der Betreffende einen Anspruch auf Bekanntgabe derjenigen Tatsachen hat, die in die Gnadenentscheidungen eingeflossen sind. Dies wäre z. B. durch ein Akteneinsichtsrecht des Betroffenen gewährleistet.

Bisher ist die Hamburger Praxis dergestalt, daß die Gnadenabteilung wegen § 5 Abs. 2 HmbDSG uneingeschränkt Auskünfte z. B. aus der Zentralkartei der Staatsanwaltschaft einholen kann. Die rechtliche Regelungsbedürftigkeit des Gnadenwesens wird durch den Entwurf des Justizmitteilungsgesetzes bestätigt, der dazu ansatzweise Regelungen enthält. Den Landesgesetzgebern verbleibt dann die nähere gesetzliche Ausgestaltung, wie sie jetzt im Entwurf eines Saarländischen Gnadengesetzes enthalten ist.

19.6 Akteneinsicht zu wissenschaftlichen Zwecken

Unterschiedliche wissenschaftliche Forschungsvorhaben aus dem Bereich der Kriminologie sind auf die Einsicht in Originalakten angewiesen. Die Staatsan-

waltschaft, die über die Gewährung der Akteneinsicht zu entscheiden hat, unterrichtet den Hamburgischen Datenschutzbeauftragten von der Gewährung der Akteneinsicht. Die Justizbehörde ist für die Gewährung der Akteneinsicht für Strafsachen aus der Zeit vor dem 8. Mai 1945 zuständig geworden.

In einem öffentlich diskutierten Einzelfall wurde einem Buchautor gestattet, die Akten über einen umfangreichen Ermittlungskomplex einzusehen, soweit sie Gegenstand der öffentlichen Hauptverhandlung waren. Dabei war vom Autor die geforderte und übliche Erklärung unterzeichnet worden, personenbezogene Daten nur anonymisiert zu veröffentlichen. Das veröffentlichte Werk enthielt dann aber eine Reihe von Passagen wortgleich mit dem Text eines Protokolls über eine Zeugenvernehmung usw., der in den Akten enthalten war.

Die Staatsanwaltschaft prüft noch, ob diese Passagen im Rahmen der Akteneinsicht dem Autor zugänglich gemacht werden. Er hat sich während der Akteneinsicht dahingehend eingelassen, daß er die wesentlichen Informationen bereits vor Akteneinsicht in Form von Kopien gekannt und die Einsicht in die Originalakten lediglich zur Bestätigung durchgeführt habe. Die abschließende datenschutzrechtliche Bewertung steht noch aus.

Der Hamburgische Datenschutzbeauftragte hat sich an die Justizbehörde mit der Anregung gewandt, die übliche Erklärung über die vertrauliche Behandlung der Akten weiter zu präzisieren. Die Justizbehörde hat sich für eine Klärung der Rechtslage ausgesprochen und will hierzu an die Landesjustizverwaltungen herantreten. Ob dies ausreicht, die Strafbarkeit eines Verstoßes gegen die Anonymisierungspflicht zu begründen oder ob Änderungen gesetzlicher Bestimmungen erforderlich sind, muß noch geprüft werden. Ob außerdem das Zivilrecht als Korrektiv für derartige Eingriffe in das allgemeine Persönlichkeitsrecht der Betroffenen ein ausreichendes Instrumentarium darstellt, bleibt abzuwarten.

19.7 Schuldnerverzeichnis

Der Hamburgische Datenschutzbeauftragte ist an die Justizbehörde mit der Frage herangetreten, ob der Umfang der Eintragungen im Schuldnerverzeichnis nicht erweitert werden sollte. Bisher werden Schuldner, unabhängig davon, wie hoch die Schulden sind und aus welchem Grund deren Begleichung unterbleibt, z. B. mit der Haftandrohung in das Schuldnerverzeichnis eingetragen.

Es wäre zu erwägen, ob nicht ein Erläuterungsfeld, in dem zum Beispiel auf der Grundlage von Angaben des Schuldners eine Zahlungsverweigerung aus persönlichen Gründen aufgenommen werden könnte, ein zutreffenderes Bild von der Zahlungsfähigkeit des Betroffenen geben könnte. Im Bereich der privaten Auskunfteien wird diese Möglichkeit zur eigenen Darstellung und Zuspeicherung teilweise eingeräumt (siehe 25.2.6 und auch 23.4). Die Justizbehörde sieht für eine derartige Erweiterung keinen Bedarf.

19.8 Einsatz besonderer Befugnisse zur Datenerhebung

Die Erhebung personenbezogener Daten mit verdeckten Methoden kann zur Abwehr einer konkreten Gefahr (siehe oben 17.9) oder zum Zwecke der Strafverfolgung zulässig sein.

Das Gesetz zur Bekämpfung der Organisierten Kriminalität (OrgKG), das die schon bestehenden Befugnisse zur verdeckten Datenerhebung nach der Strafprozeßordnung erheblich erweitert hat, ist am 15. September 1992 in Kraft getreten.

Um den Umfang der Nutzung dieses Instrumentariums und damit den Umfang des Eingriffs in Bürgerrechte zu erfahren, hat der Hamburgische Datenschutzbeauftragte die Strafverfolgungsorgane gebeten, aufgeteilt nach den gesetzlichen Möglichkeiten, die Anzahl der getroffenen Maßnahmen darzustellen.

Während die Staatsanwaltschaft bei dem Landgericht Hamburg Auskunft erteilte, verweigerte die Staatsanwaltschaft bei dem Oberlandesgericht Hamburg jede Auskunftserteilung. Sie vertritt die Auffassung, daß das Auskunftsbegehren nicht mit den in § 23 HmbDSG dem Hamburgischen Datenschutzbeauftragten zugewiesenen Aufgaben in Einklang stünde. Im übrigen stünden Kapazitätsmängel einer Ermittlung der Anzahl der getroffenen Maßnahmen entgegen. Die Rechtsauffassung teilen wir nicht, weil wir auch Auskünfte über alte Einzelfälle und damit eine vollständige Auflistung verlangen könnten. Soweit Auskunft erteilt wurde, ergibt sich folgendes Bild:

§ 100a StPO läßt die Überwachung des Fernmeldeverkehrs zu, wenn der Verdacht der Begehung bestimmter, im Gesetz bezeichneter Straftaten gegen einen Tatverdächtigen besteht und die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Tatverdächtigen auf andere Weise nicht möglich oder wesentlich erschwert ist. Die Durchführung der Maßnahme bedarf der Anordnung durch einen Richter.

In ca. 170 Fällen (die genaue Zahl ist dem Hamburgischen Datenschutzbeauftragten bekannt) bei einer geringeren Zahl von Strafverfahren wurde eine derartige Maßnahme durchgeführt. Im Bereich der Staatsanwaltschaft bei dem Landgericht Hamburg ist durch organisatorische Maßnahmen sichergestellt, daß die vom Gesetz vorgeschriebene Benachrichtigung der Betroffenen nach Abschluß der Maßnahme auch wirklich erfolgt.

§§ 110a, 110b Abs. 1 und 2 StPO lassen den Einsatz verdeckter Ermittler bei bestimmten Straftaten zu. Die Durchführung bedarf aber der staatsanwaltschaftlichen Anordnung und in Sonderfällen der richterlichen Anordnung. Von dieser Befugnis wurde Gebrauch gemacht. Von der Veröffentlichung der dem Hamburgischen Datenschutzbeauftragten bekannten Zahlen wird aus Sicherheitsgründen abgesehen.

Zu den weiteren durch das OrgKG erweiterten Befugnissen, wie dem Einsatz technischer Mittel nach § 100c StPO, der Schleppnetzfahndung nach § 163

StPO, der Polizeilichen Beobachtung gemäß § 163e StPO und der Rasterfahndung gemäß § 98a StPO waren durch die Staatsanwaltschaft Angaben mit vertretbarem Aufwand nicht zu ermitteln. Die Polizei hat uns zu diesen Maßnahmen Informationen übermittelt. Von der Veröffentlichung wird aus Sicherheitsgründen abgesehen.

20. Strafvollzug

20.1 Postkontrolle im Strafvollzug

Die bereits in der Vergangenheit (vgl. 11. TB, 20; 10. TB, 20.2) dargestellten Bedenken gegen die Praxis der Überwachung des Schriftverkehrs im Strafvollzug bestehen nach wie vor.

In der Sitzung des bürgerschaftlichen Unterausschusses Datenschutz haben die Vertreter des Strafvollzugsamtes dargestellt, daß eine Vollkontrolle der Post unbedingt erforderlich sei und auch praktisch durchgeführt werde. Dies wurde mit Sicherheitsbedenken begründet. Dabei komme es nach der Auffassung des Strafvollzugsamtes nicht darauf an, ob – wie es das Strafvollzugsgesetz vorsieht – von dem betreffenden Strafgefangenen eine Gefahr für die Anstaltssicherheit ausgehe. Es reiche vielmehr aus, wenn eine Strafanstalt als „mit hohem Sicherheitsstandard ausgestattet" anzusehen sei.

Bei unserer Querschnittsprüfung von Strafanstalten wurde der Art und Weise der Durchführung der Postkontrolle besondere Bedeutung zugemessen.

Zunächst ist festzuhalten, daß annähernd jeder Strafgefangene über Telefonkarten verfügt und die in einigen Stationen aufgestellten Kartentelefone benutzen kann. Eine Überwachung dieses Telefonverkehrs findet nach Auskunft der Strafanstalt regelmäßig nicht statt. Soweit die Anstaltssicherheit betroffen ist, gibt es also für jeden Strafgefangenen – neben dem im Regelfall unkontrollierten Gespräch mit Besuchern – darüber hinaus grundsätzlich die Möglichkeit, telefonisch auch für die Anstaltssicherheit abträgliche Fragen besprechen zu können.

Eine Prüfung der einzelnen Abteilungsleiter hinsichtlich der Art und Weise, wie die Postkontrolle durchgeführt wird, hat ein völlig uneinheitliches Bild ergeben. Von der persönlichen Vollkontrolle über deren Durchführung durch Mitarbeiter bis zur fast nie durchgeführten Postkontrolle sind auf den jeweiligen Ebenen fast alle Kombinationen vertreten. Außerdem haben uns Strafvollzugsmitarbeiter mitgeteilt, daß seit der Möglichkeit, grundsätzlich frei zu telefonieren, die Postkontrolle im Regelfall unergiebig sei. Dies bestärkt den Hamburgischen Datenschutzbeauftragten in seiner Auffassung, daß es aus Sicherheitsgründen nicht erforderlich ist, eine Vollkontrolle durchzuführen. Im Gegenteil zeigt gerade die Praxis in den Strafanstalten eine differenziertere Vorgehensweise, als sie von den Vertretern des Strafvollzugsamtes dargestellt wird. In Gesprächen mit den jeweiligen Abteilungsleitern stellte sich heraus, daß sie ganz

bestimmte Strafgefangene als für die Sicherheit der Strafanstalt problematisch angesehen und dort eine Postkontrolle im Einzelfall durchgeführt haben. Dieses Verfahren deckt sich auch mit den gesetzlichen Regelungen.

Bei dieser Sachlage ist es unverständlich, wieso das Strafvollzugsamt auf der Berechtigung zur Vollkontrolle ohne Nachweis einer Sicherheitsgefährdung im konkreten Einzelfall besteht. Demgegenüber hat die Vollzugspraxis einen Weg gefunden, sicherheitsrelevante Fragen für den Einzelfall sachgerecht zu beantworten.

Im Berichtszeitraum wurde dem Hamburgischen Datenschutzbeauftragten – im Gegensatz zum vorherigen Jahr – kein Fall bekannt, in dem die Korrespondenz mit ihm oder einer Volksvertretung überprüft worden ist. Insofern dürften die Bemühungen der Justizbehörde, rechtlich einwandfreie Zustände zu erreichen, erfolgreich gewesen sein.

20.2 Querschnittsprüfung von Justizvollzugsanstalten

Die Datenverarbeitung der Justizvollzugsanstalten I und II (JVA) war Gegenstand einer umfassenden datenschutzrechtlichen Querschnittsprüfung. Die Datenverarbeitung erfolgt im wesentlichen in Akten und Karteien.

Über jeden Gefangenen wird eine Gefangenenpersonalakte angelegt, die alle Vorgänge enthält, die während der Strafzeit anfallen. Neben dem Urteil, in dem sich auch Ausführungen z. B. zu psychiatrischen Auffälligkeiten befinden können, werden alle Anträge des Gefangenen, Beurteilungen über den Gefangenen sowie Vorkommnisse, aber auch Mitteilungen von Informanten über den Strafgefangenen aufgenommen. In diese Akte hat der Strafgefangene keine Akteneinsicht (siehe hierzu 20.3).

Zu dieser Akte haben andererseits alle Bediensteten der Strafanstalt uneingeschränkten Zugang. Eine irgendwie geartete Kontrolle über die Akteneinsicht von Mitarbeitern war nicht ersichtlich. Die Anstalt hatte als „ Regelung" lediglich die Anordnung erlassen, daß sich nach 16 Uhr alle Akten wieder in der Geschäftstelle befinden müssen. Bei der Masse der Akten und der Form der Lagerung wäre die Anordnung nur dann zu überwachen gewesen, wenn mehrere hundert Gefangenenpersonalakten auf Vollständigkeit überprüft werden würden.

Die Mitarbeiter der Strafanstalt haben unterschiedlich intensiven Kontakt zu den Strafgefangenen. Dabei existiert in der Strafanstalt das sogenannte Ebenenkonzept. Die JVA II ist in mehrere Ebenen eingeteilt, bei der für eine bestimmte Gruppe von Gefangenen bestimmte Bedienstete für den Behandlungsvollzug zuständig sind. Kontakte bestehen aber auch zu anderen Ebenen. Unter Bezugnahme auf eine Regelung im Strafvollzugsgesetz, die für alle Bediensteten eine Mitwirkungspflicht beim Behandlungsvollzug vorsieht, argumentierte die Strafanstalt, daß dies auch deren unbeschränkten Zugang zur Gefangenenpersonalakte erforderlich mache.

Diese Auffassung berücksichtigt überhaupt nicht den Grundsatz der Erforderlichkeit. In allen Verwaltungsbereichen einschließlich dem Strafvollzug ist nach den verschiedenen Aufgaben zu differenzieren. Die Mitarbeiter der Strafanstalt haben unterschiedliche Aufgaben und einen unterschiedlich intensiven Kontakt zu dem einzelnen Strafgefangenen. Die Mitwirkung aller Mitarbeiter am Behandlungsvollzug bedeutet nicht, daß alle alles tun. Der Behandlungsvollzug erfolgt vielmehr arbeitsteilig. Diesen aus der jeweiligen arbeitsteiligen Aufgabenstellung resultierenden Informationsbedürfnissen über die Gefangenen muß auch durch eine differenzierte Zugriffsregelung Rechnung getragen werden.

Nach langwierigen Diskussionen mit unserer Ankündigung, eine förmliche Beanstandung gemäß § 25 HmbDSG auszusprechen, hat die Justizbehörde den datenschutzrechtlichen Grundsatz anerkannt, daß Zugang zu Informationen nur insoweit eröffnet werden darf, wie es die jeweiligen Aufgaben der Mitarbeiter in der Strafanstalt erfordern. Die nähere Ausgestaltung ist noch nicht abgeschlossen. Hierzu ist denkbar, daß die Gefangenenpersonalakte in Teile mit Grunddaten für alle Mitarbeiter und andererseits in Aktenteile mit Daten aufgeteilt wird, die nur bestimmten Mitarbeitern der jeweiligen Ebene zugänglich sind.

Die Justizbehörde hat uns gegenüber darauf hingewiesen, daß dies wegen bundeseinheitlicher Verwaltungsvorschriften nicht ohne die Mitwirkung der anderen Länder gehe. Dabei ist aber zu berücksichtigen, daß schon die Aktenhaltung in der heutigen Form datenschutzrechtlich unzulässig ist. Der Eingriff in das Grundrecht auf informationelle Selbstbestimmung, das auch Strafgefangenen zur Seite steht, bedarf einer bereichsspezifischen gesetzlichen Regelung über Art und Umfang der Daten, die in Gefangenenpersonalakten gespeichert werden dürfen. Verwaltungsvorschriften reichen hierfür nur noch übergangsweise aus.

Bei der mangelnden Überwachung des Aktenverbleibs insgesamt und der Akteneinsicht wäre es nicht verwunderlich, wenn personenbezogene Informationen unzulässig verwendet oder übermittelt würden. Den Hamburgischen Datenschutzbeauftragten erreichte u. a. eine Eingabe, in der ein Strafgefangener berichtete, daß ihm seine Gefangenenpersonalakte und seine Krankenakte zum Kauf angeboten worden seien. Eine Überprüfung ergab, daß ein Band seiner umfangreichen Krankenakte nicht aufzufinden war. Dabei wurde weiter festgestellt, daß die früheren Bände von Krankenakten generell in einem Umkleideraum unverschlossen gelagert wurden. Auch erfolgte eine Protokollierung des Ausgangs von Krankenakten nicht in in allen Fällen. Die Prüfung des Vorgangs ist noch nicht abgeschlossen.

Die weitere Tatsache, daß auch außerhalb der Strafanstalt Originalteile einer Gefangenenpersonalakte aufgetaucht sind, belegt, daß unabhängig vom konkreten Fall die Aktenhaltung doch deutliche Mängel aufweist.

Bei der Durchführung der Prüfung erhielt der Hamburgische Datenschutzbeauftragte den Hinweis, daß Protokolle von Abteilungsleitersitzungen, in denen neben Sicherheitsbelangen auch personenbezogene Fragestellungen erörtert werden können, sich in den Händen von Strafgefangenen befinden sollen. Weitere Recherchen ergaben, daß diese Behauptung zutreffend war und von der Strafanstalt auch eingeräumt wurde.

Aber auch auf den einzelnen Ebenen zeigten sich erhebliche Mängel bei der Datenverarbeitung. Von Ebene zu Ebene wurden in unterschiedlich intensivem Maße über die Strafgefangenen zusätzliche Angaben gesammelt und auf der jeweiligen Ebene auch gespeichert. Die erhobenen und gespeicherten Daten umfaßten bei einzelnen Ebenenleitern sehr detaillierte Angaben; andere Ebenenleiter berichteten aber, daß sie überhaupt keine eigenen Sammlungen hätten, sondern alles, was sie brauchten, in der Gefangenenpersonalakte enthalten sei.

Die Aktenhaltung wird durch eine Vielzahl von Karteien in verschiedenen Abteilungen ergänzt. Die weitere Bewertung wird zeigen, ob und gegebenfalls welche Karteien nicht erforderlich sind.

Die sehr umfangreichen Sachverhaltsdarstellungen sind zwischenzeitlich mit den Strafanstalten abgestimmt worden. Als Sofortmaßnahme hat der Hamburgische Datenschutzbeauftragte die Einrichtung einer funktionsfähigen Aktenüberwachung unter Berufung auf die für alle Behörden geltende Aktenordnung verlangt. Die Strafanstalt hat sich auf den Standpunkt gestellt, daß die Aktenordnung für sie nicht gelte, aber eingeräumt, daß sich aus der Vollzugsgeschäftsordnung eine entsprechende Verpflichtung ergäbe. Sie hat zugesagt, die Entnahme der Akten durch eine Ausleihkarte zu dokumentieren.

Der Hamburgische Datenschutzbeauftragte hat eine grundlegende Änderung von Art und Inhalt der Datenerhebungen sowie von der Art und Weise der Anlage der Akten und des Zugangs verlangt. Die Forderungen sind so grundlegend, daß die Umsetzung eine langfristige Aufgabe darstellt.

20.3 Akteneinsicht durch Gefangene

Problematisch aus datenschutzrechtlicher Sicht ist die Verweigerung der Einsicht von Strafgefangenen in ihre Gefangenenpersonalakte.

Dort befinden sich nicht nur Vorgänge, von denen der Strafgefangene Kenntnis hat, wie z.B. Anträge und Genehmigungen. Vielmehr nimmt jeder Mitarbeiter des Strafvollzuges für sich in Anspruch, Vermerke über das Verhalten des Gefangenen zu fertigen und in die Gefangenenpersonalakte zu geben, ohne daß der Gefangene hiervon Kenntnis erlangt. Die Vermerke reichen von Hinweisen auf renitentes Verhalten bis zu ausführlichen Beurteilungen.

Alle diese Vorgänge bleiben dem Strafgefangenen im Regelfall verschlossen. Sie haben allerdings zum Teil gravierende Auswirkungen auf sein zukünftiges

Verbleiben in der Anstalt. Die Akten gehen u.a. im Rahmen der Prüfung von Vollzugslockerungen oder vorzeitigen Entlassungen z.B. an Strafvollstreckungskammern, ohne daß dem Gefangenen vollständig bekannt ist, welchen Inhalt seine Akte hat. Vor der Entscheidung der zuständigen Stelle, z.B. der Strafvollstreckungskammer, wird der Strafgefangene aber regelmäßig zu den entscheidungserheblichen Tatsachen gehört.

Die bisherige Verweigerung der Akteneinsicht ist mit den Grundsätzen des Volkszählungsurteils, wonach grundsätzlich jeder wissen können muß, was über ihn wo gespeichert ist, nicht vereinbar. Die Möglichkeit, Informationen aus der Akte zu erhalten, besteht lediglich insoweit, als ein Bediensteter dem Gefangenen den Inhalt der Akte vermittelt. Hierzu muß der Strafgefangene dem Bediensteten die Vorgänge konkret benennen, über die ihm Auskunft erteilt werden soll. Eine eigene Einsichtnahme, um Richtigkeit und Vollständigkeit der Angaben zu überprüfen, bekommt der Strafgefangene nicht.

Da das Strafvollzugsgesetz datenschutzrechtliche Regelungen, die den Ansprüchen des Volkszählungsurteils genügen, nicht enthält, finden die Bestimmungen des Hamburgischen Datenschutzgesetzes Anwendung.

Der weitere Verlauf der Prüfung und die Diskussion mit der Justizbehörde wird zeigen, inwieweit die Bereitschaft besteht, die nicht mehr zeitgemäßen Verfahrensweisen im Strafvollzug an moderne datenschutzrechtliche Standards anzupassen.

20.4 Besucherkontrolle

Grundsätzlich lassen sich zwei Arten von Besuchern in der Strafanstalt unterscheiden: die Besucher von Strafgefangenen und die Mitarbeiter von Lieferanten.

Besucher von Strafanstalten müssen, wenn es sich um Privatpersonen handelt, vom Strafgefangenen angemeldet werden. Im Rahmen des Anmeldeverfahrens werden verschiedene Dateien und Karteien geprüft. Stellen sich dabei Sicherheitsbedenken heraus, wird der Zugang verwehrt. Ergeben sich keine Sicherheitsbedenken, wird auf einer für jeden Strafgefangenen geführten Karteikarte der Name des Besuchers vermerkt.

Hinsichtlich der Mitarbeiter von Lieferanten ziehen – in noch zu klärendem Umfang – die Pförtendienste z.B. in der Zentralkartei der Staatsanwaltschaft Erkundigungen ein und gestatten ggf. den Zugang mit mehr oder weniger aufschlußreichen Bemerkungen. So wurde einem Petenten die Zufahrt mit dem Hinweis gestattet, daß er Glück habe, einfahren zu dürfen; auf Nachfrage wurde ihm mitgeteilt, es läge eine Eintragung wegen Körperverletzung vor. Nachprüfungen ergaben nach Angaben des Strafvollzugsamtes, daß wahrscheinlich aus der Zentralkartei hinsichtlich des Petenten nachgefaßt worden war.

Auch im Rahmen der Besucherüberprüfung werden Anfragen bei verschiedenen Behörden durchgeführt. Die Art und der Umfang müssen aber noch geklärt werden. Dabei gestaltet sich die Abstimmung mit der Justizbehörde ausgesprochen zäh. Gesetzte Fristen sind mehrfach nicht eingehalten worden. Auch berief sich die Justizbehörde in ihrer ersten fundierten Stellungnahme auf Bestimmungen des Hamburgischen Datenschutzgesetzes, die seit mehreren Jahren nicht mehr gültig sind.

Insgesamt bestehen unterschiedliche Abfragemöglichkeiten, z.B. in der Zentralkartei der Staatsanwaltschaft, durch Strafvollzugsanstalten, aber auch vom Strafvollzugsamt, die datenschutzrechtlich zweifelhaft sind und einer weiteren Überprüfung unterzogen werden müssen (siehe auch 19.4).

21. Gesundheitswesen

21.1 Bereichsspezifische Regelungen und automatisierte Patientendatenverarbeitung

Die Entwicklung zum Thema „Datenschutz im Gesundheitswesen" in den zehn Jahren seit dem Volkszählungsurteil des Bundesverfassungsgerichts ergibt ein widersprüchliches Bild.

Zum einen hat die bereichsspezifische Normierung des Datenschutzes in Hamburg Fortschritte gemacht: Das Krebsregistergesetz von 1984 geht grundsätzlich von der Einwilligung des Patienten in eine Registermeldung aus; das Hamburgische Krankenhausgesetz von 1991 gibt dem Patientendatenschutz ebenso breiten Raum wie die geplante Neufassung des Gesetzes über Hilfen und Schutzmaßnahmen bei psychisch Kranken. Die Berufsordnung für Hamburger Ärzte wird derzeit überarbeitet – auch um neueren Entwicklungen des Datenschutzes gerecht zu werden. Der einzige blinde Fleck: Trotz unseres Drängens auch im letzten Jahr und neuer Gesetze in anderen Bundesländern ist eine Regelung der Datenverarbeitung im öffentlichen Gesundheitsdienst Hamburgs nach wie vor nicht in Sicht (vgl. 11. TB, 1.5.2).

Zum anderen hat sich die Verwaltung von Patientendaten in den letzten zehn Jahren durch den IuK-Einsatz revolutioniert. Überspitzt könnte man sagen: Was durch die gesetzlichen Regelungen an Klarheit und Transparenz für den Patienten erreicht wurde, ging durch die alles erfassende Automatisierung und Vernetzung insbesondere in den großen Krankenhäusern wieder verloren. Kein Patient vermag wirklich zu übersehen, wer wann welche seiner medizinischen Daten zur Kenntnis nehmen kann.

Das Gesundheitsstrukturgesetz macht zudem die problematische Dialektik zwischen Normierung und Automatisierung deutlich: Die neuen technischen Möglichkeiten, Planung und Kontrolle zu effektivieren, haben „Daten-Begehrlichkeiten" geweckt, die die Gesundheitsreform prompt befriedigt. Mehr Patientendaten als jemals zuvor werden den verschiedensten Institutionen des

Gesundheitswesens bekannt (vgl. 11. TB, 21.2). Zugleich wird die Anwendung der neuen technischen Möglichkeiten in breitem Umfang nicht nur zugelassen, sondern sogar vorgeschrieben.

Immer neue IuK-Projekte – nun besonders auch im Pflegebereich – haben in erster Linie das Ziel, die wirtschaftlichen Potentiale der Technik, also Kostendämpfungs- und Rationalisierungseffekte, auszuschöpfen. Transparenz und Kontrollmöglichkeiten fallen dem weitgehend zum Opfer. Die datenschutzrechtliche Mißbrauchsvorsorge wie etwa die Einschränkung des Zugriffs auf Patientendaten nach dem Ende der Behandlung gerät zunehmend unter Druck. Die im Hamburgischen Krankenhausgesetz für diesen Fall vorgesehene Sperrung des Direktabrufs stößt in den Krankenhäusern auf Widerstand.

Sicher segensreich ist die IuK-Revolution im Gesundheitswesen für spezielle Behandlungsmethoden und für die Qualitätskontrolle ärztlicher und pflegerischer Leistungen. Der „Strahlen-Skandal" im Universitätskrankenhaus Eppendorf offenbarte gerade hier jedoch Mängel. Aus datenschutzrechtlicher Sicht ist darauf hinzuweisen, daß allein die krankenhausinterne Qualitätskontrolle mit patientenbezogener Datenverarbeitung durchgeführt werden darf. Externe Qualitätssicherung kann und muß nach dem Hamburgischen Krankenhausgesetz mit anonymisierten bzw. aggregierten Daten auskommen (vgl. 11. TB, 21.5.3).

21.2 Empfehlungen des Landesbetriebes Krankenhäuser zum Datenschutz

Im 11. TB (21.3.2) wurde ausführlich über die Punkte berichtet, die bei der Diskussion über die geplante Dienstanweisung Datenschutz zwischen dem Hamburgischen Datenschutzbeauftragten und der Geschäftsführung des Landesbetriebes Krankenhäuser (LBK) strittig geblieben waren. Seitdem konnte in weiteren Gesprächen eine weitgehende Annäherung erreicht werden:

Der LBK entwickelte ein plausibles Konzept zur Verschlüsselung von Daten auf lokalen Netzwerken, das bei „Eigenentwicklungen" umgesetzt werden soll. Die datenschutzrechtlich bessere Version 4.0 der Netzwerksoftware NFS wird nach und nach eingeführt. Die Festlegung auf einen Termin vermied der LBK allerdings. Schließlich sicherte der LBK die Anwendung des Vier-Augen-Prinzips bei der Systemverwaltung dort zu, wo die Personalkapazität der entsprechenden Krankenhaus-Abteilung dieses zuläßt. Allein die Verschlüsselung der Daten auf Sicherungsbändern und die Protokollierung der Systemverwalter-Aktivitäten blieben strittig.

Mit Beschluß vom 14. Juli 1993 verabschiedete die Leitung des LBK mehrere „Empfehlungen der Geschäftsführung an die Allgemeinen Krankenhäuser" zum Thema „Datenschutz im LBK". Neben einem allgemeinen Teil enthält dieses Dokument die „Empfehlungen zur Führung und Herausgabe von Krankenakten und Röntgenbildern" – die geringfügig geänderte bisherige Dienstanweisung von 1987 – und die „Empfehlungen zum Datenschutz im IuK-Bereich" – den bislang diskutierten Entwurf einer Dienstanweisung.

Für die Allgemeinen Krankenhäuser sind „Empfehlungen" von geringerer Verbindlichkeit als die bisherige „Dienstanweisung" für die Führung von Krankenakten. Begründet wird diese „Umwidmung" der Richtlinien mit dem Betriebsstatut des LBK von 1991, das die sachgerechten organisatorischen Regelungen zur Sicherstellung des Datenschutzes den Krankenhäusern überlasse.

Wir versuchten dennoch, die lange diskutierten Datenschutz-Richtlinien nicht zur beliebigen Disposition der Krankenhäuser zu stellen, und forderten zumindest eine Auslegung der Empfehlungen als „Soll-Vorschriften". Die Geschäftsführung des LBK griff dies auf und erläuterte – jedenfalls uns gegenüber –, daß bei Abweichungen von den Empfehlungen eine Begründung der Krankenhäuser erforderlich sei.

Insgesamt richten wir uns darauf ein, daß selbst datenschutzrechtliche Grundsatzfragen nicht (mehr) allein mit der Geschäftsführung des LBK mit verbindlicher Wirkung für die Krankenhäuser geklärt werden können. Dies erfordert auf unserer Seite einen erheblich größeren Aufwand. Durch gemeinsame Treffen mit den für Datenschutz verantwortlichen Personen in den Krankenhäusern soll zumindest eine gewisse Koordination und abgestimmte Meinungsbildung gewährleistet werden. Das erste Gespräch bei uns fand am 25. Oktober 1993 statt.

21.3 Projekt Qualitätssicherung in der Chirurgie (Quasic)

Erhebliche datenschutzrechtliche Bedenken gegen das Projekt Quasic im AK Barmbek hatten Anfang 1992 zu Eil- und Übergangsmaßnahmen geführt, die durch eine angekündigte Neu-Programmierung durch den LBK abgelöst werden sollten (vgl. 11. TB, 21.5.1). Zugesagt war die Einführung des neuen datenschutzgerechten Konzepts für das vierte Quartal 1992.

Erst Ende 1992 erhielten wir „Leistungsbeschreibung und DV-Pflichtenheft" für das neue Verfahren „Interne Qualitätssicherung in der Chirurgie". Unsere datenschutzrechtliche Prüfung führte zu einer positiven Stellungnahme.

Im April 1993 erfuhren wir jedoch, daß das neue Quasic-Konzept „weiterentwikkelt" würde und zunächst das Mitbestimmungsverfahren passieren müsse. Unsere Anfrage nach dem Stand des Verfahrens und die Bitte um das weiterentwickelte Konzept wurden im Juni 1993 vom LBK mit dem Hinweis beantwortet, das Mitbestimmungsverfahren sei noch nicht abgeschlossen.

Nachdem wir unserer Unzufriedenheit über die große Verzögerung Ausdruck gegeben hatten, erhielten wir im September 1993 die Mitteilung, wegen eines Netzkabelschadens sei das alte System Quasic schon seit Juni/Juli 1993 nicht mehr in Betrieb. Das neue Konzept sei auf der Grundlage der Leistungsbeschreibung von 1992 – also offenbar nicht „weiterentwickelt" – am 15. Sep-

tember 1993 ausgeschrieben worden. „Der LBK hofft, daß das neue Programm . . . zum Jahresende 1993 im AK Barmbek in Betrieb genommen werden kann." Im übrigen sei jetzt nicht mehr die Geschäftsführung des LBK, sondern das AK Barmbek für das Projekt Quasic zuständig. Konzipiert war das neue System allerdings ursprünglich für alle Häuser des LBK.

Die Kooperation zwischen der Geschäftsführung des LBK und uns in dieser Angelegenheit halten wir für alles andere als optimal. Ob das neue System wenigstens ein Jahr später als zugesagt einsatzbereit ist, erscheint uns durchaus offen. Datenschutzrechtlich ist allerdings durch die – endgültige? – Außerbetriebnahme des alten Systems der Zeitdruck gewichen.

21.4 Projekt Anästhesiedokumentation

Vom Projekt Anästhesiedokumentation soll hier nur als ein weiteres Beispiel für eine ungenügende Kooperation des LBK mit dem Hamburgischen Datenschutzbeauftragten berichtet werden:

Im September 1990 stellte die IuK-Abteilung des AK Altona erstmals ausführlich die Planungen für das Projekt „Anästhesiedokumentation" mit dem „maschinenlesbaren Narkoseprotokoll (MALENA)" vor. Unsere vorläufige – grundsätzlich positive – Stellungnahme vom Oktober 1990 enthielt eine Reihe von weitergehenden Fragen. Sie bezogen sich auf den Verbleib von Narkoseprotokoll-Durchschriften, auf den Arbeitnehmerdatenschutz, auf Umfang und Dauer der Datenspeicherung und auf die Anonymisierung vor der Auswertung.

Diese Fragen wurden durch die unkommentierte Zusendung von Unterlagen zu MALENA und zur „Qualitätssicherung in der Anästhesie" im Mai 1991 nicht beantwortet und sind noch heute offen. Unsere Nachfrage vom September 1991 an das AK Altona und an die LBK-Geschäftsführung führte zunächst zum Hinweis, daß nunmehr die Rechtsabteilung des LBK zuständig sei. Nach einer unbeantworteten schriftlichen Erinnerung im Januar 1992 wurde auf unsere telefonische Nachfrage im März 1992 eine baldige Stellungnahme angekündigt. Sie blieb aus.

Statt dessen berichtete die Presse Ende April 1993 vom einem Projekt „Qualitätssicherung in der Anästhesiologie" mit bundesweitem Modellcharakter, mit dem „von Mai an alle Anästhesieabteilungen der Hamburger Krankenhäuser die Versorgung verbessern" wollen. Die aus diesem Anlaß wiederholten Erinnerungen im Mai, Juni, Juli und August erbrachten nach wiederholten Absichtserklärungen im September 1993 die lapidaren Feststellungen:

". . . ist festzuhalten, daß die Häuser des LBK Hamburg im 1. Halbjahr 1991 mit der EDV-gestützten Erfassung von Protokolldaten begonnen haben. Der Hamburgische Datenschutzbeauftragte wurde im Jahre 1990 unter Übersendung des Konzeptes in die Planungsphase des Verfahrens einbezogen. Zwischenzeitlich befindet sich das Verfahren Qualitätssicherung Anästhesie in den Krankenhäusern des LBK im Routine-Betrieb." Abschließend wird auf die Zuständigkeit des jeweiligen Krankenhauses verwiesen.

Auf eine formelle Beanstandung dieses Verstoßes gegen § 23 Abs. 5 HmbDSG habe ich nur deswegen verzichtet, weil das Konzept der Anästhesie-Dokumentation inhaltlich grundsätzlich überzeugte und es sich hinsichtlich der eigentlichen Datenverarbeitung eher um einen Fall geringer Bedeutung handelt. Als krasses Beispiel für eine Verletzung der Pflicht der staatlichen Stellen, den Hamburgischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen, sollte der Vorgang hier jedoch dokumentiert werden.

21.5 Projekte zur Pflege-Personalregelung

Art. 13 des Gesundheitsstrukturgesetzes enthält die „Regelung über Maßstäbe und Grundsätze für den Personalbedarf in der stationären Krankenpflege (Pflege-Personalregelung)". Sie sieht eine tägliche Einordnung der Patienten in eine bestimmte Pflegestufe und die vierteljährliche Übermittlung von individuellen „Patienten-Erhebungsbogen" – allerdings ohne Namen – an die Kassen vor. Anhand von Minutenwerten wird daraus der Pflegepersonal-Bedarf errechnet.

Die hohe Komplexität und Formalisierung des Einordnungs- und Berechnungsverfahrens haben den LBK und die Krankenhäuser veranlaßt, hierfür IuK-Systeme vorzusehen. Trotz der für alle Häuser gleichen Rechtslage ist eine einheitliche IuK-Anwendung jedoch nicht in Sicht:

Nachdem in der Betriebszeitschrift „LBK-Forum" bereits im April 1992 das umfassende Projekt PIK („Pflegedienst im Krankenhaus") vorgestellt und seine LBK-weite Einführung angekündigt worden war, erhielten wir im Juni 1993 das über 320 Seiten starke „Fachkonzept" von PIK. Der LBK teilte uns jedoch zugleich mit, das Projekt sei entsprechend dem LBK-Betriebsstatut „dezentralisiert und den Krankenhäusern die weitere Entwicklung und Einführung freigestellt". Ob und ggf. in welchem Haus die für 1994 angekündigte Pilot-Anwendung von PIK realisiert wird, blieb offen.

Parallel zu PIK werden andere Systeme entwickelt, die – zumindest auch – die Pflege-Personalregelung umsetzen sollen: Schon im Juni 1992 hatten wir vom Projekt PULS („Pflegedienstunterstützung für die LBK-Stationen") im AK Eilbek Kenntnis erhalten. Wir regten eine Koordination mit der LBK-Geschäftsführung an. Dies führte jedoch nicht zu einer gemeinsamen einheitlichen IuK-Planung. Dasselbe gilt für das PIK-AS-Verfahren des Hafenkrankenhauses, über das uns – auf unsere Nachfrage – im Februar 1993 ein „datenschutzrechtlicher Vermerk" zuging. Im Juli 1993 erreichte uns schließlich aus dem AK Heidberg das Konzept MobiDik („Mobile Datenerfassung im Krankenhaus") Pflege-Personalregelung. Von den anderen LBK-Krankenhäusern liegen uns keine Mitteilungen vor.

Alle genannten Systeme sollen die Pflege-Personalregelung umsetzen, einzelne gehen in ihrer Funktionalität weit darüber hinaus. Während das Hafenkrankenhaus sich mit einem Einzelplatz-PC begnügt, sehen die anderen Systeme mobile Datenverarbeitungsgeräte auf den Stationen vor, die Patienten-

Grunddaten von einem Stations-/Abteilungs-PC erhalten und aktuelle Werte an diesen übermitteln.

Datenschutzrechtlich ist vor allem die Gewährleistung der Datensicherheit bei den mobilen Geräten relevant. Die vom AK Heidberg geplante Verschlüsselung des krankenhausinternen Datenverkehrs haben wir deswegen ausdrücklich begrüßt. Alle Systeme berücksichtigen beim vierteljährlichen „Datenexport" an die Kassen die vom Gesundheitsstrukturgesetz vorgesehene faktische Anonymisierung.

Insgesamt stößt die konkrete Kontrolle und Prüfung aller IuK-Systeme zur Umsetzung der Pflege-Personalregelung (auch der vermuteten weiteren in den nicht genannten Krankenhäusern) deutlich an unsere Kapazitätsgrenze. Wir versuchen deswegen, neben einer stichprobenhaften Untersuchung vor Ort vor allem über eine gemeinsame Erörterung der datenschutzrechtlichen Grundfragen mit den für den Datenschutz Verantwortlichen der Krankenhäuser den Aufwand zu effektivieren. Auf die früher einmal in Anspruch genommene Koordinationsfunktion der Geschäftsführung des LBK können wir uns leider nicht mehr verlassen (siehe 21.2.).

21.6 Automation beim Medizinischen Dienst der Krankenversicherungen (ISmed)

Einen weiteren Baustein bei der zunehmenden Automation des Gesundheitswesens stellt das Informations- und Kommunikationssystem ISmed dar, das vom Medizinischen Dienst der Krankenversicherungen (MDK) bundesweit für UNIX-Mehrplatzanlagen entwickelt wird. Mit Hilfe des ISmed-Systems werden Patienten- und Verwaltungsdaten erfaßt und gepflegt, Terminpläne verwaltet sowie medizinische Gutachten über den Zustand eines Patienten erstellt. Beim MDK Hamburg befindet sich ISmed zur Zeit noch im Probebetrieb. Eine Entscheidung über die endgültige Einführung des Systems in Hamburg ist noch nicht getroffen worden.

In der Konzeption von ISmed sind bereits relevante technische und organisatorische Datenschutzmaßnahmen berücksichtigt worden. Ein zentraler Datenschutzmechanismus ist die Unterscheidung von fünf Benutzerklassen (Systemverwalter, Systembetreuer, Ärzte, Arztsekretärinnen, Anmeldungs-/Schalterpersonal) mit verschiedenen Zugriffsrechten. Diese Differenzierung ermöglicht, daß die Systemanwender nur zu den Funktionen Zugang haben, die sie für ihre Aufgabenerfüllung benötigen.

Die Zugriffsrechte der verschiedenen Benutzerklassen werden jedoch nur auf Anwendungsebene und nicht auf Betriebssystemebene unterschieden. So werden auf UNIX-Ebene sämtlichen Benutzern umfangreiche Lese-/Schreib-Rechte auf ISmed-Dateien eingeräumt. Diese Situation ist vertretbar, solange sichergestellt wird, daß keine weiteren Anwendungen auf dem System installiert werden und kein Benutzer auf Betriebssystemebene gelangt (z. B. bei Systemzusammenbrüchen).

Bevor das ISmed-System beim MDK Hamburg in den Realbetrieb übergehen kann, müssen noch zusätzliche Maßnahmen realisiert werden. Der MDK Hamburg beabsichtigt, die erforderlichen Maßnahmen noch innerhalb des Probebetriebes umzusetzen.

21.7 Vernetzung des Universitätskrankenhauses Eppendorf (UKE)

Welchen Stellenwert die hamburgische Verwaltung dem Ausbau der Kommunikationsinfrastruktur einräumt (vgl. 11. TB, 3.1.2 und IuK-Datenschutzbericht), zeigt sich sehr deutlich am Beispiel der geplanten Vernetzung des gesamten UKE-Geländes: Dort wird zur Zeit ein grundlegendes Netzkonzept erarbeitet, das so ausgelegt ist, daß maximal in 13.000 Räumen insgesamt ca. 20.000 Rechneranschlüsse für den Haustechnik-, Forschungs-, Medizin- und Verwaltungsbereich verlegt werden können. Auch wenn der endgültige Ausbau des geplanten Netzes nicht zuletzt von der Bewilligung entsprechender Haushaltsmittel abhängig ist und bis zur Jahrtausendwende nur mit dem Anschluß von ca. 1.500 bis 2.000 Endgeräten zu rechnen ist, verdeutlicht das Beispiel die Grenzen einer datenschutzgemäßen Bewertung derart weitgehender DV-technischer Veränderungen.

Die frühzeitige Beteiligung des Hamburgischen Datenschutzbeauftragten hat zwar dazu beigetragen, daß ein Netzwerk konzipiert wurde, das sowohl datensicherungstechnischen Mindestanforderungen als auch Konzepten einer strukturierten Verkabelung gerecht wird. Es bleiben aber datenschutzrechtliche Probleme.

Positiv ist, daß für die Bereiche Haustechnik, Forschung sowie Verwaltung und Medizin drei physikalisch getrennte Subnetze installiert werden, die nur im Einzelfall miteinander gekoppelt werden. Für den Verwaltungs- und medizinischen Bereich sind keine physikalisch getrennten Subnetze vorgesehen, sondern lediglich Abgrenzungen durch sogenannte Router, da zwischen beiden Bereichen ein erheblicher Datenaustausch erwartet wird. Im integrierten Medizin- und Verwaltungsnetz werden als weitere Sicherungsmaßnahme filternde Sternkoppler eingesetzt, wie sie der Hamburgische Datenschutzbeauftragte bei der Übermittlung sensibler personenbezogener Daten für erforderlich hält. Darüber hinaus werden bei der gebäudeexternen Verkabelung abhörsichere Lichtwellenleiter sowie gebäudeintern Twisted-Pair-Kabel verwendet (vgl. 3.3).

Trotz aller technischer Sicherheitsmaßnahmen ist das geplante UKE-Netzwerk dennoch datenschutzrechtlich äußerst problematisch, da es keine verfahrensorientierte Verkabelung einzelner UKE-Bereiche, sondern eine flächendeckende Kommunikationsinfrastruktur darstellt, die den potentiellen Datentransport zwischen allen Einrichtungen wie Kliniken, Operationszentren, Laboratorien, Materialverwaltung, Rechenzentrum und Verwaltung unterstützen soll.

Welche Anwendungen demnächst über ein solches Netz konkret abgewickelt werden sollen, ist noch nicht abschließend entschieden. Es existiert bereits ein

recht umfangreiches Sollkonzept, das jedoch noch der internen Abstimmung und weiterer Gespräche mit dem Hamburgischen Datenschutzbeauftragten bedarf.

Insgesamt bringt die geplante flächendeckende Infrastruktur gravierende Datenschutzrisiken für jeden einzelnen Patienten mit sich. Während bei traditioneller Datenverarbeitung in abgeschlossenen Subnetzen der Datenmißbrauch in der Regel auf Einzelfälle beschränkt bleibt, werden bei einer flächendeckenden Vernetzung einer unerlaubten regelmäßigen Funktions- und Datenintegration keine unbedingt sicheren technischen Grenzen gesetzt.

Es kann zudem nur sehr schwer nachvollzogen werden, welche Krankenhausbereiche Daten untereinander austauschen. Zwar ist dies für den betroffenen Bürger bereits heute kaum mehr transparent. Dennoch wird diese Tendenz durch eine flächendeckende Vernetzung noch verstärkt.

Die mangelnde Systemtransparenz schränkt nicht nur die Rechte der Betroffenen ein, sondern hat auch Konsequenzen für die Kontrollmöglichkeiten des Hamburgischen Datenschutzbeauftragten. Diese sind nicht zuletzt im Krankenhaus deshalb bedeutsam, weil die betroffenen Patienten datenschutzrechtlichen Aspekten einen wesentlich geringeren Stellenwert als ihren gesundheitlichen Probleme einräumen und von daher institutionellen Kontrollen weitgehend vertrauen müssen.

21.8 Prüfung des Hygienischen Instituts

Durch die Senatsdrucksache über die IuK-Planung in den verschiedenen Behörden erhielten wir 1992 Kenntnis davon, daß im Hygienischen Institut ein automatisiertes Labordatensystem eingerichtet werden soll. Auf eine entsprechende Nachfrage unsererseits wurde uns das Konzept zunächst schriftlich vorgestellt. Dies nahmen wir zum Anlaß für eine ausführliche Prüfung vor Ort.

Vor einer Untersuchung der Datensicherheit des technischen Systems war die Frage zu stellen, ob es im Hygienischen Institut überhaupt einer personenbezogenen Datenverarbeitung bedarf. Denn in aller Regel werden in dem Institut nur Analyseaufträge anderer Stellen ausgeführt, also keine Kontakte zu den Probanden und Patienten selbst aufgenommen.

21.8.1 Anonymisierung von Analyseaufträgen

In einem ausführlichen Gespräch mit der Institutsleitung im August 1993 machten wir zunächst deutlich, daß der Datenschutz epidemiologische und Langzeitforschungen nicht behindern will. Dazu ist jedoch die Erfassung und Speicherung des Namens des Probanden nicht zwingend erforderlich. Vielmehr vermag grundsätzlich auch ein sogenanntes Strukturcode-Verfahren die Zuordnung verschiedener Untersuchungen zu derselben betroffenen Person sicherzustellen: Wird der Code z.B. jeweils gebildet durch den dritten Buchstaben des Vornamens, den zweiten Buchstaben des Nachnamens, die Gesamtzahl

der Buchstaben des Nachnamens und die Quersumme des Geburtsdatums, so ergibt sich ein für eine Identifikation geeigneter Einweg-Code, der eine Rückentschlüsselung nicht zuläßt.

Die Leitung des Hygienischen Instituts begründete demgegenüber die namensbezogene Speicherung von Analyseaufträgen und -ergebnissen mit sehr verschiedenen Fallkonstellationen – etwa einer familienbezogenen Infektionssuche oder der Probeneinsendung durch verschiedene, vorher nicht bekannte Einsender. Auch die Analyse der Proben von Krankenhauspatienten kann aufgrund der Einwilligung im Behandlungsvertrag namensbezogen erfolgen.

Besonderen Wert auf eine anonymisierte Verarbeitung legten wir dagegen bei den täglichen Massenverfahren. So ist bei Analysen auf seuchengesetzlicher Grundlage, die in großem Umfang (z.B. 60.000 Stuhluntersuchungen im Jahr) von den Gesundheitsämtern veranlaßt werden, die Einführung eines Strukturcodeverfahrens durchaus möglich. Dasselbe gilt für ca. 10.000 Hepatitisuntersuchungen bei Strafgefangenen.

Das Hygienische Institut fordert hierfür allerdings ein EDV-gestütztes Auftragsverfahren, um Fehler bei der Schlüsselbildung zu vermeiden. Dem schlossen sich die Behörde für Arbeit, Gesundheit und Soziales und das Senatsamt für Bezirksangelegenheiten an.

Schon heute werden die meisten Aufträge für eine HIV-Untersuchung bereits von den Einsendern anonymisiert. Da dies jedoch nicht mit einem Strukturcode erfolgt, beklagt das Hygienische Institut, daß eine Zuordnung späterer Untersuchungsbefunde zu früheren Analysen bei derselben Person und damit eine epidemiologische Forschung auf diesem wichtigen Gebiet nicht möglich ist.

Auch die Proben der Asylbewerber und die Analyseergebnisse werden zwischen dem Gesundheitsamt Altona und dem Hygienischen Institut anonymisiert übermittelt. Das Verfahren wurde mit uns im einzelnen festgelegt und trägt dem Datenschutz der betroffenen Ausländer Rechnung.

21.8.2 Netzsicherheit

Das Netz des Hygienischen Instituts besteht insgesamt aus zwei UNIX-Servern sowie zahlreichen Terminals und Personalcomputern. Als Netzwerk- und Transportprotokoll werden TCP/IP, zur Rechner-Kommunikation die UNIX-Dienste rlogin, FTP und TELNET eingesetzt. Das sowohl von der Medizinaluntersuchungsanstalt (MUA), der Chemischen und Lebensmitteluntersuchungsanstalt (CLUA) als auch von der Verwaltung genutzte Netz erfüllt weitgehend die bereits in Abschnitt 3.3 ausführlicher dargestellten Datensicherheits-Mindeststandards.

Das Netz ist eine Mischung aus Stern- und Bustopologie: Während die beiden File-Server sowie die Konsole über einen Bus mit vier Verteilern verbunden

sind, stellen die Verteiler wiederum einen Netzknoten für ein sternförmiges Subnetz auf der Basis von Ethernet 10 Base T dar. Zwischen den Verteilern und den File-Servern sind Glasfaserkabel verlegt. Sämtliche Terminals und Personalcomputer sind über Twisted-Pair-Kabel mit einem der vier Verteiler verbunden.

Die Verteiler wirken jedoch nicht als Filter, so daß die versendeten Datensegmente zum Zeitpunkt der Übertragung auf dem gesamten Netz vorhanden sind und von sämtlichen Benutzern durchaus mitgelesen werden können. Dies war zum Zeitpunkt der Prüfung insofern problematisch, als die Struktur der vier Subnetze vorrangig nicht auf funktionale Einheiten ausgerichtet ist, sondern den vier Brandabschnitten des Hauses entspricht. Besonders kritisch erwies sich die Situation an einem der Verteiler, über den MUA-, CLUA- und Verwaltungs-PC gemeinsam geschaltet waren.

Um wirksam zu verhindern, daß personenbezogene Daten des von der MUA genutzten File-Servers von Mitarbeitern anderer Abteilungen beim Transport über das Übertragungsmedium mitgelesen werden können, wurden zunächst sämtliche MUA-PC auf gesonderte Verteiler geschaltet. Diese Sofortmaßnahme erforderte lediglich einen zusätzlichen Verteiler im Netz. Um bei künftigen hausinternen Umzügen auch weiterhin flexibel zu bleiben, will das Hygienische Institut mit dem Verteiler-Hersteller Kontakt aufnehmen und prüfen, inwieweit bei neuen Anschaffungen filternde Sternkoppler einsetzbar sind. Damit könnte auf eine Verschlüsselung der über das Netz übertragenen Daten verzichtet werden.

21.8.3 Sicherheit der UNIX-Server

Die Sicherheit der beiden UNIX-File-Server war zum Zeitpunkt der Prüfung nicht ausreichend. Zum einen war lediglich eine für derart sensible Anwendungen unangemessene Standard-UNIX-Version im Einsatz, die weder aussagefähige Systemprotokolle erstellt, noch die Möglichkeit bietet, wichtige Sicherheitsobjekte, wie beispielsweise die Paßworttabelle, zusätzlich zu schützen. Durch den Wechsel auf eine Sicherheitsversion von UNIX ist diese Schwachstelle inzwischen behoben worden.

Zum anderen waren die beiden UNIX-File-Server so administriert, daß zahlreiche Benutzer unnötigerweise Zugriff auf das Betriebssystem hatten. Mittlerweile besitzen lediglich die beiden Systemverwalter Shell-Berechtigung.

Darüber hinaus wurde vom Hygienischen Institut zugesichert, personenbezogene Daten auf nicht mehr benötigten Datenträgern mit einem starken Magneten physikalisch zu löschen. Sicherungskopien des MUA-Rechners werden künftig ohnehin nur verschlüsselt auf externen Datenträgern gespeichert.

21.8.4 PC-Sicherheit

Während die Sicherheit der im Einsatz befindlichen MS-DOS-Rechner mit veränderter BIOS-Version durch das Sperren von Diskettenlaufwerk, serieller und

paralleler Schnittstelle ausreichend war, erwies sich die Datensicherheit der eingesetzten Apple-Rechner aufgrund fehlender Sicherheitssoftware als unzureichend. So konnte jeder Benutzer Daten aus dem Netz heraus auf lokale Datenträger kopieren, ohne daß der Netzverwalter hiervon überhaupt Kenntnis erhielt.

Wir haben das Hygienische Institut aufgefordert, die Datensicherheit auf den Apple-Rechnern durch Einsatz zusätzlicher Sicherheitssysteme zu erhöhen. Falls auch auf den MS-DOS-Rechnern ein Zugriff auf das Diskettenlaufwerk erforderlich ist, sollte hier ebenfalls zusätzliche Sicherheitssoftware eingesetzt werden.

Ein weiteres, allerdings nicht PC-spezifisches Problem besteht darin, daß der PC-Benutzer bei einigen Fällen vier Paßwörter eingeben muß, bis er endlich auf Anwendungsebene gelangt. Durch zahlreiche Paßwörter wird der Zugriffsschutz jedoch nicht verbessert, sondern im Gegenteil eher aufgehoben: Welcher Benutzer ist schon in der Lage, sich mehrere Paßwörter zu merken, die zudem noch regelmäßig gewechselt werden sollen. Im Interesse einer verbesserten Zugriffskontrolle halten wir es statt dessen für notwendig, lediglich ein Paßwort nach dem Systemstart des PC abzufragen, das Paßwort nach erfolgter Autorisierung zu parametrisieren und an die anderen Ebenen weiterzureichen. Das Hygienische Institut will zur Realisierung dieses Vorschlags Kontakt mit dem Entwickler des Labordatensystems aufnehmen.

21.8.5 Fernwartung der Labordatensysteme

Die Wartung der Labordatensysteme erfolgt im Hygienischen Institut nicht vor Ort, sondern per Fernwartung mittels Modem. Zwar wird die Modemleitung durch den Systemverwalter des Hygienischen Instituts erst nach vorherigem Anruf des Wartungstechnikers freigegeben. Dennoch reicht diese Maßnahme allein nicht aus, um weitgehend ausschließen zu können, daß personenbezogene Daten über die Leitung übertragen und somit dem Wartungstechniker offenbart werden (vgl. 11. TB, 3.4).

Besonders problematisch wird Fernwartung, wenn dem Wartungstechniker Systemverwalterrechte eingeräumt werden, wie es beim Hygienischen Institut der Fall war. Mittlerweile werden an den Fernwartungstechniker jedoch keine privilegierten Zugriffsrechte mehr vergeben. Ebenso werden sämtliche Fernwartungsaktivitäten an der Systemkonsole überwacht, protokolliert und im Mißbrauchsfalle abgebrochen. Für die Modembenutzung wurde inzwischen eine Benutzerordnung erstellt.

21.9 Empfehlungen zur Schwangerenberatung nach dem § 218 StGB-Urteil

Das Urteil des Bundesverfassungsgerichts vom 28. Mai 1993 zum Schwangerschaftsabbruch enthält in seiner Übergangsregelung zur Schwangerenberatung mehrere datenschutzrechtlich relevante Vorgaben:

— „Die schwangere Frau kann auf ihren Wunsch gegenüber der sie beratenden Person anonym bleiben."

— Nach der Beratung „hat die Beratungsstelle der Frau auf Antrag . . . eine auf ihren Namen lautende . . . Bescheinigung auszustellen."

— „Die beratende Person hat in einer Weise, die keine Rückschlüsse auf die Identität der Beratenen erlaubt, in einem Protokoll das Alter, den Familienstand und die Staatsangehörigkeit der Beratenen, die Zahl ihrer Schwangerschaften, ihrer Kinder und früherer Schwangerschaftsabbrüche festzuhalten. Sie hat ferner . . . gegebenenfalls die zu ihm (dem Beratungsgespräch) hinzugezogenen weiteren Personen zu vermerken."

Eine Anfrage der Behörde für Arbeit, Gesundheit und Soziales nahmen wir zum Anlaß, zu diesen Anforderungen neun „Datenschutzgrundsätze für die Beratung der Schwangeren in einer anerkannten Beratungsstelle" zu entwickeln. Sie konkretisieren die notwendigen organisatorischen Maßnahmen und Verfahren in den Beratungsstellen. Sie enthalten folgende Kernelemente:

Um die geforderte Möglichkeit einer anonymen Beratung auch dann sicherzustellen, wenn die Schwangere eine namensbezogene Bescheinigung erhält oder konkrete Hilfe zur Wohnungssuche oder Kinderbetreuung in Anspruch nimmt, müssen die Aufgaben in der Beratungsstelle auf verschiedene Personen verteilt und voneinander getrennt werden. Zur Wahrung der Anonymität dürfen namensbezogene Unterlagen weder bei der Protokollierung noch bei der Ausstellung der Bescheinigung in der Beratungsstelle verbleiben. Bei einer anonymen Beratung dürfen im Protokoll auch nicht die Namen der hinzugezogenen weiteren Personen vermerkt werden.

Diese und weitere Datenschutzgrundsätze wurden den Datenschutzbeauftragten der anderen Bundesländer zur Kenntnis gegeben und in der Senatsdrucksache 93/1182 der Behörde für Arbeit, Gesundheit und Soziales sowie des Senatsamtes für die Gleichstellung berücksichtigt. Die Senatsdrucksache weist zu Recht darauf hin, daß unsere Grundsätze Maßstäbe für die Personalausstattung und die innere Organisation der Beratungsstellen setzen und auch als Kriterien für die staatliche Aufsicht relevant sind.

21.10 Rettungswesen

Aufgrund einer Anfrage des Datenschutzbeauftragten von Brandenburg sowie eines Schreibens des Gesamtpersonalrats des Landesbetriebs Krankenhäuser befaßten wir uns mit der Verwendung von Rettungsdienst- und Notarztprotokollen in Hamburg. Diese als Durchschreibsatz gestalteten Formulare enthalten neben den Personalien des Versicherten detaillierte Befund- und Diagnosedaten.

Im September klärten wir in einem Gespräch mit Vertretern der Feuerwehr und der Notarztzentrale im AK Altona, wie die Protokolle derzeit verwahrt werden und wie das zukünftige Verfahren aussehen soll:

Gegenwärtig erhält das den Patienten aufnehmende Krankenhaus das Original-Protokoll für die Krankenunterlagen. Die erste und meist auch die zweite Durchschrift verbleiben bei der Notarztwache. Der Notarzt selbst kann die zweite Durchschrift aber auch zur eigenen Dokumentation nutzen. Die Aufbewahrungsfrist beträgt wie bei den ärztlichen Behandlungsunterlagen 10 Jahre. Für den einen wie für den anderen Zweck ist eine namensbezogene Dokumentation erforderlich.

Geplant ist ein IuK-gestütztes Dokumentationsverfahren zur Qualitätssicherung im Rettungsdienst. Dezentral durch das Team der Notarztwache oder zentral durch eine besondere Erfassungsstelle soll der fachliche Inhalt der Protokolle automatisiert erfaßt und ausgewertet werden. Bei zentraler Erfassung kommt nur eine Übersendung von Protokollen ohne Patientennamen in Betracht. Bei der automatisierten Erfassung wird außer dem Geschlecht und dem Geburtsjahr des Patienten auf die Speicherung von personenbezogenen Daten des Patienten oder des Arztes verzichtet. Angesichts dieser weitgehenden Anonymisierung haben wir hiergegen keine datenschutzrechtlichen Bedenken geltend gemacht.

Zur „Ergebnisqualitäts-Sicherung" ist darüber hinaus an eine spätere Rückmeldung des behandelnden Krankenhauses an den Rettungsdienst gedacht, um Diagnostik und Behandlung beim Rettungsdiensteinsatz nachträglich überprüfen zu können. Auch hierfür sollen keine Patientennamen, sondern nur Einsatznummern verwandt werden. Eine zentrale Erfassungs- und Auswertungsstelle könnte so im Vergleich mit den anonymisierten Notarztprotokollen ohne Patienten- und Arztbezug Querschnittsprüfungen zur Qualitätssteigerung des Rettungsdienstes insgesamt durchführen.

Eine Rückmeldung an oder über den einzelnen Notarzt, der zum Vergleich das patientenbezogene Protokoll zur eigenen Kontrolle heranzieht, würde zusätzliche medizinische Daten über den Patienten offenbaren. Soweit diese ärztliche Selbstkontrolle jedoch für eine effektive Qualitätssicherung des Rettungsdienstes erforderlich ist, wird diese personenbezogene Verarbeitung von Krankenhausdaten durch § 5 des Hamburgischen Rettungsdienstgesetzes ausdrücklich zugelassen.

21.11 Datenschutz in Arztpraxen

Im 11. TB hatten wir zwei Aspekte des Patientendatenschutzes in Arztpraxen behandelt, die wir mit der Ärztekammer Hamburg und der Zahnärztekammer Hamburg erörterten: den Verbleib von Patientenunterlagen bei Auflösung und Verkauf einer Praxis (21.10) und die Übermittlung von Patientendaten an Verrechnungsstellen (21.11). Im vergangenen Jahr haben wir erstmals auch IuK-Systeme in Arztpraxen geprüft.

21.11.1 Prüfungen

In einer großen Gemeinschafts-Praxis mit umfangreicher Laborleistung auch für externe Auftraggeber stießen wir auf verschiedene Lücken in der Datensicherheit des Netzwerks. Ein Schwerpunkt der Erörterungen war die Definition der Zugriffsrechte und eine Trennung der Praxisbereiche Verwaltung, ärztliche Behandlung und Labor.

Ein weiteres Grundsatzproblem war die Einführung einer unterschiedlichen Kennung für die einzelnen Ärzte der Gemeinschaftspraxis. Nach der Berufsordnung muß dem Patienten auch bei gemeinschaftlicher Berufsausübung die freie Arztwahl gewährleistet werden. „Gemeinsame Patientendaten" aller Gemeinschafts-Ärzte bzw. der ungehinderte Zugriff auf die Daten von Patienten der Arzt-Kollegen ist nur über eine ausdrückliche Einwilligung des Patienten zulässig.

In einer kleineren Arztpraxis lernten wir in Anwesenheit von Vertretern des Herstellers vor allem die Funktionsweise einer verbreiteten Standard-Software für niedergelassene Ärzte kennen. Hier bildeten die Gewährleistung der Fälschungssicherheit, die Umsetzung des Auskunftsrechts der Patienten und die Löschung nach Ablauf der Dokumentationsfrist praxisübergreifende Erörterungspunkte.

Bei einem späteren Fachgespräch mit dem Systementwickler des Herstellers konnten wir insbesondere diese allgemeinen Themen vertiefen und datenschutzrechtliche und datensicherungstechnische Aspekte für die zukünftige Weiterentwicklung der Praxis-Software einbringen. Gerade solche Einflußnahme „an der Quelle" der von Arztpraxen angewandten Systeme halten wir zur Verstärkung des Datenschutzes bei niedergelassenen Ärzten für wichtig.

21.11.2 Leitfaden

Aus unserer bisherigen Kontroll- und Beratungspraxis als Aufsichtsbehörde für niedergelassene Ärzte entstand 1993 ein Leitfaden „Datenschutz in der Arztpraxis". Er richtet sich sowohl an Ärztinnen und Ärzte als auch an Patientinnen und Patienten und wird Anfang 1994 zur Verfügung stehen.

Der Leitfaden behandelt in übersichtlicher Kurzform die Anforderungen, die die ärztliche Schweigepflicht und der Datenschutz an die Praxisorganisation, die Führung der Patientenakte und die Praxis-EDV stellen. Ferner werden die den Patienten meist unbekannten gesetzlichen Vorschriften benannt, welche die Ärzte ohne Einwilligung der Patienten zu einer Übermittlung von Patientendaten an Dritte berechtigen. Schließlich spricht der Leitfaden typische Formen und spezifische Probleme von Schweigepflicht-Entbindungserklärungen an. Ein Überblick über Kontroll-Einrichtungen und Beschwerdestellen schließt das Heft ab.

Um zu vermeiden, daß der Nutzer des Leitfadens von Feststellungen des Hamburgischen Datenschutzbeauftragten ausgeht, die Auffassungen der Ärztekammer Hamburg oder der Kassenärztlichen Vereinigung Hamburg widersprechen, haben wir diese Institutionen vorab um ihre Stellungnahme gebeten. Soweit in wichtigen Fragen keine Einigung erzielt werden konnte, ist die abweichende Meinung der Kammer oder der Kassenärztlichen Vereinigung ausdrücklich vermerkt.

Wir hoffen, mit diesem Leitfaden hinsichtlich des Datenschutzes mehr Transparenz in die Arzt-Patienten-Beziehung zu bringen und zu einer erhöhten Sensibilität beizutragen. Gleichzeitig umschreibt das Heft die inhaltlichen Maßstäbe für unsere weitere Prüf- und Beratungstätigkeit auf diesem Gebiet.

Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

22. Werbewirtschaft

22.1 Postwurfsendungen

Während wir uns meistens mit Wurfsendungen der Wirtschaftswerbung beschäftigen, ging es im Berichtszeitraum um den Datenschutz bei Postwurfsendungen politischer Parteien. Weil dabei das Verhalten der Bundespost im Vordergrund stand, haben wir uns mit dem für die Post zuständigen Bundesbeauftragten für den Datenschutz abgestimmt.

Nach den im Jahre 1991 geänderten Ausführungsbestimmungen zur Postordnung sowie den neuen Allgemeinen Geschäftsbestimmungen der Deutschen Bundespost Postdienst sind die Postboten verpflichtet, einen am Briefkasten angebrachten Aufkleber „Keine Werbung" als Annahmeverweigerung zu beachten (11. TB, 22.1). Im Vorfeld der Bürgerschaftswahl vom 19. September 1993 erschienen Presseveröffentlichungen, wonach einzelne Postboten trotz eines solchen Aufklebers Postwurfsendungen von Parteien zugestellt hatten. Dies haben wir zum Anlaß genommen, die Öffentlichkeit noch einmal auf die Rechtslage aufmerksam zu machen. Die Deutsche Bundespost Postdienst hat eingeräumt, daß die in Hamburg bekanntgewordenen Fälle offensichtlich auf einem falschen Verhalten der Postboten im Einzelfall beruhten.

Dissens besteht mit dem Postdienst jedoch darüber, in welcher Form ein Postkunde gezielt Sendungen ablehnen kann. Wir vertreten die Auffassung, daß es möglich sein muß, mit Hilfe eines Aufklebers am Briefkasten auch einzelne oder bestimmte gleichartige Postwurfsendungen im voraus abzulehnen, z. B. konkret angegebener rechtsextremer Parteien. Der Postdienst will eine solche gezielte Ablehnung nur dann akzeptieren, wenn sie vom Postkunden persönlich an der Haustür ausgesprochen wird.

Wir können nicht erkennen, welcher rechtliche Unterschied zwischen einer mündlich bzw. persönlich vorgetragenen und einer schriftlichen – mittels eines Aufklebers deutlich gemachten – Annahmeverweigerung besteht. Mit dem allgemeinen Persönlichkeitsrecht ist es unvereinbar, wenn der Postbote Aufkleber auf Briefkästen mißachtet, mit denen gezielt die Annahme einzelner oder bestimmter gleichartiger Postwurfsendungen abgelehnt wird.

Der Bundesbeauftragte für den Datenschutz hat auf unseren Wunsch diese Problematik mit der Generaldirektion der Deutschen Bundespost Postdienst erörtert. Dabei wurde bekannt, daß der Postdienst zwar Überlegungen zu einer Änderung seiner Allgemeinen Geschäftsbestimmungen angestellt hat, insbesondere um die unerwünschte Mitwirkung an der Verbreitung ausländerfeindlicher und rechtsradikaler Propaganda zu vermeiden. Diese Überlegungen sind

dem Bundesministerium für Post und Telekommunikation auch vorgetragen worden, ohne daß sie bisher bereits zu konkreten Ergebnissen geführt haben.

Wir haben den Bundesbeauftragten für den Datenschutz gebeten, auch gegenüber dem Bundesministerium für Post und Telekommunikation darauf zu drängen, daß vom Postdienst differenzierte Empfängerwünsche bei nicht adressierten Werbesendungen in den Fällen berücksichtigt werden, in denen für den Zusteller die Absenderangabe zweifelsfrei erkennbar ist.

22.2 Adressierte Werbesendungen

Nach wie vor wenden sich zahlreiche Bürger an die Aufsichtsbehörde und beklagen sich darüber, daß sie immer wieder persönlich adressierte Werbezuschriften von Unternehmen erhalten, mit denen sie vorher noch nie etwas zu tun hatten. Dies bestätigt, daß die Novellierung des Bundesdatenschutzgesetzes im Jahre 1990 im Ergebnis nicht zu nennenswerten Einschränkungen der Werbewirtschaft im Umgang mit personenbezogenen Daten geführt hat (10. TB, 23).

Um sich gegen die Zusendung unerwünschter adressierter Werbesendungen zur Wehr setzen zu können, verbleibt den Betroffenen zunächst die Möglichkeit, gemäß § 28 Abs. 3 BDSG gegenüber der speichernden Stelle und gegenüber dem Datenempfänger seine Widerspruchsrechte gegen die Nutzung und Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- und Meinungsforschung geltend zu machen.

Daneben ist es häufig erfolgreicher, sich in die „Robinson-Liste" des Direktmarketing-Verbandes eintragen zu lassen. Dies ist ein Verzeichnis der Personen, die keine adressierte Werbung wünschen. Durch die Eintragung erreicht der Betroffene, daß jedenfalls die dem Verband angeschlossenen Unternehmen – das sind ca. 40 % der Firmen dieser Branche, die jedoch etwa 80 % der adressierten Werbesendungen verschicken – seine Adresse nicht mehr zu Werbezwecken nutzen. Die Aufnahme in die „Robinson-Liste" ist kostenlos und kann beantragt werden bei der DDV Robinson-Liste, Postfach 1401, 71243 Ditzingen.

Wegen des großen Interesses der Öffentlichkeit an dieser Thematik hat die Aufsichtsbehörde Hamburg gemeinsam mit den Aufsichtsbehörden in Bremen und Niedersachsen ein Merkblatt zum Adressenhandel herausgegeben. Jedem Bürger wird es auf Wunsch kostenlos zugesandt.

23. Schufa

23.1 Personenverwechslungen wegen unzureichender Identitätsprüfungen

Aufgrund von Eingaben wurden uns mehrere Fälle bekannt, in denen es bei Schufa-Meldungen über Eintragungen im Schuldnerverzeichnis bei Namens-

gleichheit zu Personenverwechslungen kam. Da die Eintragungen sensible Negativmerkmale über die Vermögensverhältnisse betreffen, können derartige Verwechslungen gravierende Folgen für den Betroffenen haben.

Der Grund für die Verwechslungen liegt in der Regel darin, daß die Geburtsdaten der Betroffenen nicht bekannt sind, da diese im Schuldnerverzeichnis nicht enthalten sind. Die Schufa beauskunftet derartige Eintragungen mit dem Hinweis auf ein absolutes Nutzungsverbot, wenn die Identität nicht eindeutig feststellbar ist. Außerdem ist der Vertragspartner in diesen Fällen verpflichtet, der Schufa das Ergebnis der Identitätsprüfung mitzuteilen. Wir haben dieses Verfahren bereits in der Vergangenheit gerügt (7. TB, 5.2.3).

Die Beauskunftung in diesen Fällen ist nach § 29 Abs. 2 BDSG unzulässig, da der Empfänger nur bei Personenidentität ein berechtigtes Interesse an der Kenntnis der Daten darlegen kann. Anderenfalls besteht ein überwiegendes schutzwürdiges Interesse des Betroffenen an dem Ausschluß der Übermittlung.

Die Verantwortung für die Beauskunftung liegt bei der Schufa. Eine Verlagerung dieser Verantwortung auf die Vertragspartner ist dem Betroffenen gegenüber nicht wirksam. Die Petenten haben wir darauf hingewiesen, daß sie gemäß § 8 BDSG einen Schadensersatzanspruch gegen die Schufa haben können, wenn ihnen durch die Beauskunftung Nachteile entstanden sind.

Die Schufa teilt unsere Auffassung nicht und hält die Beauskunftung unter Hinweis auf das Nutzungsverbot für zulässig. Zudem habe sie mit den Spitzenverbänden der Kreditwirtschaft die Vereinbarung getroffen, vor einer negativen Entscheidung des Kreditgebers aufgrund einer Schufa-Auskunft und davon abweichenden Angaben des Betroffenen ein Aufklärungsgespräch mit dem Kunden über die Schufa-Daten zu führen. So könnten negative Konsequenzen derartiger Verwechslungsfälle vermieden werden.

23.2 Überprüfung des berechtigten Interesses

Die Diskussion mit der Schufa über die Erhöhung der Stichproben, die zur Prüfung des berechtigten Interesses durchgeführt werden, wurde fortgeführt (vgl. 11. TB, 23.1). An Stelle einer festen Ein-Promille-Regelung wurde von den Aufsichtsbehörden der Schufa mehrheitlich eine Regelung vorgeschlagen, nach der sich die Zahl der Stichproben gestaffelt nach der Anzahl der monatlichen Auskünfte pro Schufa-Geschäftsstelle richten soll.

Die Aufsichtsbehörden sind der Auffassung, daß die Überprüfung der Richtigkeit der Datenbestände durch die Schufa keine Stichproben zur Überprüfung des berechtigten Interesses ersetzen kann. Dies gilt auch für Eigenauskünfte, die meist eingeholt werden, um zu erfahren, welche Daten überhaupt gespeichert sind. Bei Einmeldung zwischenzeitlich geschlossener Kreditverträge, die das berechtigte Interesse an der Anfrage letztlich bestätigen, besteht allerdings kaum ein Bedarf an Stichproben. Die Schufa hat eine Prüfung des Kompromißvorschlages zugesagt.

23.3 Adressierung von Bestätigungsschreiben

Durch eine Eingabe wurden wir darauf aufmerksam, daß die Schufa schriftliche Bestätigungsschreiben über telefonische Auskünfte an den Vertragspartner schickt, ohne einen berechtigten Empfänger im Kreditinstitut auf dem Umschlag näher anzugeben. In dem der Eingabe zugrunde liegenden Fall wurden 21 Bestätigungsschreiben zusammen in einem Umschlag adressiert an die Sparkasse . . ., Postfach . . ., Ort . . ., versandt. Da derartige Schreiben in der Postabteilung geöffnet und dann in den einzelnen Abteilungen verteilt werden, besteht die Gefahr, daß Mitarbeiter, die weder mit der Kontoführung betraut sind noch Kontrollfunktionen wahrnehmen, von den sehr sensiblen Daten Kenntnis nehmen können.

Wir halten dieses Verfahren unter organisatorischen Datensicherheitsaspekten für verbesserungsbedürftig (vgl. auch Adressierung bei Direktversicherungen, 24.7). Es wird nicht verkannt, daß die Bestätigungsschreiben nicht nur an die anfragenden Sachbearbeiter adressiert werden können, um Mißbrauchsfälle zu vermeiden. Der Zugriff auf personenbezogene Daten muß aber Beschränkungen unterworfen sein, die nach den Aufgaben der Abteilungen differenziert werden könnten. In Frage käme daher eine Adressierung an bestimmte dafür zuständige Abteilungen, die aufgrund des Geschäftsverkehrs mit der Schufa bereits bekannt sind oder ohne größeren Aufwand ermittelt werden können. So könnte so weit wie möglich sichergestellt werden, daß jeder Mitarbeiter nur Zugriff auf die Daten hat, die er zur Erfüllung seiner Aufgaben benötigt.

Die Schufa ist demgegenüber der Auffassung, daß eine solche Adressierung entbehrlich sei. Die Poststellen der Vertragspartner erhielten ohnehin sämtliche Post und würden dafür sorgen, daß die jeweiligen Schreiben nur denjenigen Personen ausgehändigt würden, die in der Angelegenheit Kenntnis nehmen dürften. Die Poststellen seien auch von den Vertragspartnern stets sorgfältig ausgewählt und ganz besonders auf das Datengeheimnis verpflichtet worden. Ein geringerer Grad an Datenschutz bzw. Datensicherheit gegenüber z. B. einer Direktzustellung an die Revisionsabteilung sei daher nicht erkennbar.

Wir werden anregen, die dargestellte Problematik zusammmen mit der Schufa im Kreis der Obersten Aufsichtsbehörden zu erörtern.

23.4 Recht auf eigene Darstellung

Auch im Bereich der Schufa sind Fälle denkbar, in denen ein Anspruch des Betroffenen auf eigene Darstellung zur Vermeidung von unvollständigen oder falschen Eindrücken erforderlich sein kann (vgl. 1.3). Die Schufa hat dazu erklärt, daß es bereits jetzt möglich sei, in bestimmten Fällen Eigendarstellungen der Kunden in den Schufa-Datenbestand aufzunehmen und zu beauskunften. Die Schufa halte für derartige Zwecke sog. „Segmenthinweise" vor, unter denen derartige Eigendarstellungen der Betroffenen in Kurzform aufgenommen werden könnten.

Wir werden dieser Thematik im Zusammenhang mit künftigen Eingaben besondere Aufmerksamkeit widmen, insbesondere wenn an sich richtige Angaben ohne Zusammenhang mit dem ursprünglichen Kontext wiedergegeben wurden und dadurch zu Mißverständnissen mit ggf. schädlichen Folgen für den Betroffenen führen können.

24. Versicherungswirtschaft

24.1 Automationsentwicklung

Im Bereich der Versicherungswirtschaft ist zu beobachten, daß sich die Einführung des phonetischen Strukturcode-Verfahrens (vgl. zuletzt 11. TB, 25.1) weiter verzögert. Nachdem zunächst die Umstellung aller zentralen Warn- und Hinweissysteme im Laufe des Jahres 1992 angekündigt worden war, konnte dieser Zeitplan nicht eingehalten werden.

Nach Abschluß der Testverfahren ist nunmehr die marktweite Umstellung des Hinweissystems auf dem Gebiet der Kraftfahrtversicherung im Laufe des Jahres 1993 erfolgt. In den übrigen Sparten soll die Umstellung nach Abschluß der derzeitigen Praxistests Anfang 1994 durchgeführt werden. Aus datenschutzrechtlicher Sicht ist die Verzögerung der Vereinheitlichung der zentralen Warn- und Hinweissysteme durch die aufwendigen Praxistests zu bedauern, zumal eine endgültige Umstellung auch erst nach einer gewissen Übergangsfrist erwartet werden kann.

24.2 Zentrale Registrierstelle Rechtsschutz

Aufgrund eines Urteils des Bundesgerichtshofs aus dem Jahre 1991 (vgl. 10. TB, 25.4) wurden die Allgemeinen Bedingungen für die Rechtsschutz-Versicherung (ARB) geändert (vgl. 11. TB, 25.2).

Aus diesem Anlaß mußten auch die Voraussetzungen, unter denen personenbezogene Daten in die Warndatei Zentrale Registrierstelle Rechtsschutz eingemeldet werden können, neu festgelegt werden. Zweck der Datei ist es, anderen Rechtsschutzversicherern bei der Bearbeitung eines Versicherungsantrages einen Hinweis darauf zu geben, ob die antragstellende Person möglicherweise ein besonderes Risiko darstellt.

Den zu versichernden Personen sollen die entsprechenden Kriterien durch das „Merkblatt zur Datenverarbeitung" bekannt gemacht werden. Die Unterzeichnung der Einwilligungserklärung in die Datenverarbeitung ist nur gültig, wenn die Betroffenen bei Beantragung einer Versicherung die Möglichkeit hatten, in zumutbarer Weise vom Inhalt dieses Merkblattes Kenntnis zu nehmen (vgl. auch 24.4.).

Der im 11. TB (25.2) abgedruckte Vorschlag zur Neuformulierung des Merkblattes in bezug auf die Zentrale Registrierstelle Rechtsschutz hat nach erneuten

Verhandlungen mit dem Bundesaufsichtsamt für das Versicherungswesen und dem HUK-Verband nunmehr folgende Endfassung erhalten:

„Rechtsschutzversicherer

- Vorzeitige Kündigungen und Kündigungen zum normalen Vertragsablauf durch den Versicherer nach mindestens 2 Versicherungsfällen innerhalb von 12 Monaten.
- Kündigungen zum normalen Vertragsablauf durch den Versicherer nach mindestens 3 Versicherungsfällen innerhalb von 36 Monaten.
- Vorzeitige Kündigungen und Kündigungen zum normalen Vertragsablauf bei konkret begründetem Verdacht einer betrügerischen Inanspruchnahme der Versicherung.

Zweck: Überprüfung der Angaben zu Vorversicherungen bei der Antragstellung."

Mit dieser Formulierung werden die Voraussetzungen für eine Eintragung in die Warndatei für den Versicherungskunden deutlich beschrieben. Insbesondere müssen die Verdachtsgründe der Versicherung für eine betrügerische Inanspruchnahme konkret begründet werden und damit beweisbar sein.

Diese Einmeldekriterien sollen in das neu zu fassende Merkblatt eingearbeitet werden. Obwohl dies noch nicht geschehen ist, hat der HUK-Verband seinen Mitgliedsunternehmen mitgeteilt, daß die neuen Meldegründe ab sofort gelten. Die Obersten Aufsichtsbehörden der Länder haben die Versicherungswirtschaft darauf hingewiesen, daß die Einwilligungserklärung von Versicherungsnehmern sich nur auf die ihnen bekannten Meldegründe beziehen kann. Bei Eingaben wird dies zu berücksichtigen sein.

24.3 Allfinanz-Konzepte

Die Erörterungen mit der Versicherungswirtschaft, wie die Einwilligungserklärung in die Übermittlung personenbezogener Daten im Bereich der Allfinanz-Konzepte datenschutzrechtlich unbedenklich ausgestaltet werden kann (vgl. 11. TB, 25.3), wurden im Berichtszeitraum intensiv fortgeführt.

Zunächst stellte sich der Gesamtverband der Deutschen Versicherungswirtschaft auf den Standpunkt, daß eine Änderung der von den Versicherungskunden einzuholenden Einwilligung in die Datenverarbeitung nicht erforderlich sei. Es reiche eine Neuformulierung des Merkblattes, aus dem dann klar hervorgehen solle, welche Daten an wen bei einer weitergehenden Beratung und Betreuung in finanziellen Dienstleistungen weitergegeben werden.

Diese Auffassung entspricht nicht dem Wortlaut der gebräuchlichen Einwilligungserklärung, die bei jedem Versicherungsantrag zu unterschreiben ist. Der Versicherte willigt damit lediglich in Datenübermittlungen zu genau festgelegten Zwecken ein, nicht aber in die Verwendung seiner Daten zur Werbung für

weitergehende Finanzdienstleistungen. Auch die gesetzlichen Übermittlungstatbestände nach dem Bundesdatenschutzgesetz rechtfertigen die Weitergabe der personenbezogenen Daten in keiner Weise. Unabhängig davon ist zu berücksichtigen, daß die Versicherungswirtschaft bisher nicht bereit war, auf die Forderungen der Obersten Aufsichtsbehörden der Länder nach einer obligatorischen Aushändigung des Merkblattes vor Beantragung eines Versicherungsvertrages einzugehen (vgl. 24.4). Damit wäre – neben dem Fehlen der rechtlich notwendigen Einwilligung – die Unkenntnis des Kunden über die Verwendung seiner Daten zu anderen Zwecken vorprogrammiert.

Im weiteren Verlauf der Gespräche ließ die Versicherungswirtschaft dann die Bereitschaft erkennen, jeweils von den zu versichernden Personen eine Einwilligung einzuholen und legte den Obersten Aufsichtsbehörden einen entsprechenden Entwurf vor, der noch überarbeitet wurde.

Darüber hinaus wurde deutlich, daß die Versicherungen nicht beabsichtigen, personenbezogene Daten an sämtliche mit der jeweiligen Versicherung kooperierende Unternehmen zu übermitteln. Vielmehr sollen lediglich die bei den Vermittlern ohnehin vorhandenen Daten zur Unterbreitung von Angeboten genutzt werden. Ausgeschlossen wurde, daß andere als die jeweiligen konkreten Vermittler eines Versicherungsvertrages personenbezogene Daten der Betroffenen erhalten. Dabei kann der Vermittler auch ein mit einer Versicherungsgesellschaft kooperierendes Unternehmen sein.

Ein Kritikpunkt an dem vorgelegten Entwurf war der fehlende unmißverständliche Hinweis darauf, daß die Versagung der Einwilligung in diesem Punkt keinen Einfluß auf den übrigen Vertrag hat und jederzeit widerrufen werden kann. Die Versicherungswirtschaft ist inzwischen bereit, einen derartigen Hinweis aufzunehmen. Gemäß der Absicht der Versicherungswirtschaft, nur dem jeweiligen Vermittler Daten weiterzugeben, dürfte es auch unschwer möglich sein, diesen im Zusammenhang mit der Einwilligungserklärung deutlich zu nennen. Dem Betroffenen würde damit erkennbar, daß es sich nicht nur um einzelne Personen, sondern auch um ein Unternehmen, wie etwa Banken oder Bausparkassen, handeln kann. Seitens der Versicherungswirtschaft wurde den Aufsichtsbehörden ein neuer Entwurf zugeleitet, der jedoch die Vorschläge der Aufsichtsbehörden weitgehend unberücksichtigt läßt. Begründet wurde dies auch mit den praktischen Schwierigkeiten, eine gesonderte Einwilligungserklärung in die gebräuchlichen Antragsformulare einzuarbeiten.

Zwar konnte bisher keine Einigung über die Notwendigkeit einer gesonderten Einwilligungserklärung neben der nach dem BDSG einzuholenden Erklärung erzielt werden. Es besteht jedoch Einvernehmen darüber, daß eine eindeutig unterscheidbare Einwilligungserklärung entwickelt werden soll.

Die Gespräche sollen im 1. Halbjahr 1994 abgeschlossen werden.

24.4 Merkblatt zur Datenverarbeitung

Die Versicherungswirtschaft hat bereits vor Jahren ein Merkblatt zur Datenverarbeitung erstellt, das den Versicherungskunden umfassende Hinweise zur Datenspeicherung, zur Datenübermittlung, zur Funktion der zentralen Hinweissysteme der Fachverbände und zu sonstigen Fragen der Datenverarbeitung durch die Versicherungsunternehmen liefert. Dieses Merkblatt gewinnt seine Bedeutung insbesondere durch den engen Zusammenhang mit der von jedem Kunden bei Abschluß eines Versicherungsvertrages zu unterzeichnenden Einwilligungserklärung. Nur bei genauer Durchsicht dieser ergänzenden Hinweise werden den Betroffenen auch alle Konsequenzen ihrer Unterschrift unter die Erklärung zur Datenverarbeitung deutlich.

Nach langen Diskussionen über die Frage der Aushändigung des Merkblattes bei jeder Beantragung eines Versicherungsvertrages konnte von den Aufsichtsbehörden seinerzeit jedoch lediglich ein Kompromiß erreicht werden (vgl. 7. TB, 5.4.2). Danach gilt die Einwilligung nur, wenn der Kunde die Möglichkeit hatte, in zumutbarer Weise vom Inhalt des vom Versicherer bereitgehaltenen Merkblattes zur Datenverarbeitung Kenntnis zu nehmen.

Die damalige Einigung muß vor dem Hintergrund der geänderten Rechtslage gesehen werden. Gemäß § 4 Abs. 2 des am 1. Juni 1991 in Kraft getretenen BDSG ist der Betroffene auf den Zweck der Speicherung und einer vorgesehenen Übermittlung hinzuweisen, sofern bei ihm eine Einwilligung eingeholt wird. Das bedeutet, daß ihm nicht nur die Möglichkeit zur Kenntnisnahme eröffnet, sondern das Merkblatt tatsächlich ausgehändigt werden muß.

Die Erfahrung mit der bisherigen Versicherungspraxis hat darüber hinaus deutlich gemacht, daß die Betroffenen längst nicht in jedem Fall eine Einsichtnahme verlangen, oft nicht einmal auf die Existenz eines solchen Merkblattes hingewiesen werden und daher Probleme bei der Verarbeitung ihrer Daten nicht voraussehen können. Eine Reihe von Eingaben bei den Obersten Aufsichtsbehörden läßt erkennen, daß diese Schwierigkeiten sich durch Aushändigung des Merkblattes vermeiden ließen.

Die Obersten Aufsichtsbehörden der Länder haben die Vertreter der Versicherungswirtschaft daher gebeten, sich unter Berücksichtigung der bisherigen Probleme aufgrund des dargestellten praktizierten Verfahrens erneut zu dieser Frage zu äußern und zu einem baldigen Ergebnis zu kommen. Der Gesamtverband der Deutschen Versicherungswirtschaft hat erklärt, daß mit der in Kürze zu erwartenden Änderung des Versicherungsaufsichtsgesetzes ohnehin im 1. Halbjahr 1994 über diese Frage abschließend entschieden werden soll.

24.5 Schweigepflicht-Entbindungsklauseln

Nachdem die Neufassung einer Reihe von Schweigepflicht-Entbindungsklauseln im Schadensfall abgeschlossen worden war (vgl. zuletzt 11. TB, 25.4), stand im Berichtszeitraum noch die Lösung der Frage aus, auf welche Weise

die betroffenen Ärzte und die übrigen mit der Heilbehandlung befaßten Personen von dem jeweiligen Wortlaut informiert werden (vgl. 11. TB, 25.4.4). Die genaue Kenntnis vom Umfang der Schweigepflicht-Entbindung dieser Personen ist nicht nur zur Wahrung der datenschutzrechtlichen Belange der betroffenen Patienten, sondern auch zur Vermeidung strafrechtlicher Konsequenzen z.B. für die Ärzte erforderlich.

Die Versicherungswirtschaft hat die Anregung der Aufsichtsbehörden aufgegriffen, die Ärzte und andere betroffene Stellen bei Einholung einer Auskunft über den Inhalt der neuen Schweigepflicht-Entbindung zu informieren. Zu diesem Zweck wird der aktuelle Text dieser Schweigepflicht-Entbindung bei Gesundheitsabfragen abgedruckt mit dem Hinweis, daß davon in dieser – eventuell eingeschränkten – Form Gebrauch gemacht wird. Sofern dennoch bei der betroffenen Stelle Zweifel an der Ermächtigung auftreten, wird ihr eine Durchschrift der unterzeichneten Erklärung übersandt.

Dieses Vorgehen bewahrt einerseits den Betroffenen vor zu weitgehenden Auskünften über seinen Gesundheitszustand und sichert andererseits die Ärzte und anderen Angehörigen von Heilberufen davor, unzulässigerweise Daten über ihre Patienten zu verbreiten.

24.6 Gruppenversicherungsverträge

Das bei einer Versicherungsgesellschaft aufgetretene Problem der Übermittlung des Geburtsjahres durch einen Verein im Rahmen von Gruppenversicherungsverträgen (vgl. 11. TB, 25.5) konnte im Berichtszeitraum gelöst werden.

Der Text im Avis-Schreiben an die jeweiligen Vereinsmitglieder erhält nunmehr folgenden Wortlaut:

> „Damit auch Sie die Gelegenheit erhalten, diese Vergünstigungen in Anspruch zu nehmen, teilen wir unserem Partner die hierfür erforderlichen Daten (üblicherweise Name, Anschrift, Geburtsjahr) mit. Ein Mitarbeiter der . . . wird Sie in den nächsten Tagen aufsuchen. Die Daten werden ausschließlich für den Gruppenversicherungsvertrag verwendet. Sollten Sie aber mit der Mitteilung an . . . nicht einverstanden sein oder einen Besuch nicht wünschen, so benachrichtigen Sie uns bitte unverzüglich."

Dieser Text wird künftig allen neuen Vereinsmitgliedern zusammen mit dem Aufnahmeformular der jeweiligen Vereinigung überreicht und darüber hinaus an die Vereinsmitglieder übersandt, die noch keine Einwilligungs-Erklärung in die Datenübermittlung erteilt haben (sog. Altfälle).

24.7 Adressierung bei Direktversicherung

Durch mehrere Eingaben bei der Aufsichtsbehörde Hamburg wurde im Berichtszeitraum ein Problem bei der Adressierung von Schreiben im Rahmen von Direktversicherungen deutlich.

In einem Fall wurde eine bereits seit Jahren bestehende Lebensversicherung mit Zustimmung von Arbeitgeber und Arbeitnehmer in eine Direktversicherung umgewandelt. Das Versicherungsunternehmen übersandte daraufhin Vertragsunterlagen an den Arbeitgeber der betroffenen Person, ohne eine genaue Adressierung vorzunehmen. Dadurch wurde es ermöglicht, daß bereits in der Poststelle des Unternehmens Kenntnis von sehr sensiblen Daten des Betroffenen genommen werden konnte. In einem anderen Fall ging es um die Umwandlung in eine Direktversicherung in Form einer Gehalts-Umwandlung.

Hieran ist deutlich geworden, daß der Umgang der Versicherungsunternehmen mit den personenbezogenen Daten der betroffenen Begünstigten wesentlich sensibler gestaltet werden muß. Zwar handelt es sich bei dem Vertragspartner jeweils um den Arbeitgeber; sensible Daten fallen jedoch nur über den Arbeitnehmer an.

Mit der Versicherungswirtschaft wurde die Frage erörtert, auf welche Weise die einzelnen Versicherungsunternehmen sicherstellen können, daß bei Direktversicherungen lediglich die bei dem Arbeitgeber mit der Angelegenheit befaßten Personen – in der Regel Personalsachbearbeiter – Kenntnis von den entsprechenden personenbezogenen Daten des Arbeitnehmers erhalten. Darüber hinaus war zu klären, ob bei dem Abschluß von Lebensversicherungen Gesundheitsdaten der Arbeitnehmer zur Kenntnis der vertragschließenden Arbeitgeber gebracht werden.

Die Versicherungswirtschaft hat dazu erklärt, daß der Schriftwechsel an die vom Arbeitgeber aufgegebene Anschriftsbezeichnung erfolgt. Um eine präzise Anschrift festzulegen, die ausschließt, daß entsprechende Schreiben in den allgemeinen Posteingang gelangen, wird der Verband der Lebensversicherer seine Mitgliedsunternehmen anschreiben. Neben dem Hinweis auf die besondere Bedeutung der genauen Anschriftsbezeichnung im Hinblick auf den Datenschutz wird der Vorschlag aufgenommen, eine bestimmte Stelle in der Adresse anzugeben.

Außerdem wurde von der Versicherungswirtschaft erläutert, daß beim Abschluß von Direktversicherungen in der überwiegenden Zahl der Fälle auf eine Gesundheitsprüfung und damit bereits auf die Erhebung entsprechender Daten verzichtet werde. Sollte dennoch eine Gesundheitsprüfung erfolgen, habe es der jeweilige Arbeitnehmer in der Hand, lediglich die Versicherung zu informieren und gegebenenfalls auf Versicherungsschutz zu verzichten. Lägen gesundheitliche Probleme bei dem Arbeitnehmer vor und komme es mit seinem Einverständnis dennoch zum Vertragsabschluß, erfahre der Arbeitgeber nur von der Erhebung eines Risikozuschlags.

24.8 Auskunftsstelle über den Versicherungsaußendienst (AVAD)

Zur Auskunftsstelle über den Versicherungsaußendienst e.V. (AVAD) ist zuletzt ausführlich im 6. TB (5.4.5) berichtet worden (vgl. auch 9. TB, 5.3.4). Mittlerweile

haben sich im AVAD-Auskunftsverkehr einige Neuerungen ergeben, die auch datenschutzrechtliche Belange berühren.

24.8.1 Online-Verfahren

Die teilweise auf ein Online-Verfahren umgestellte Auskunftserteilung und Einmeldung ist mit ihren Einzelheiten im Vorfeld der Einführung eingehend mit der Aufsichtsbehörde erörtert worden. Grundlage der Teilnahme eines Versicherungsunternehmens an der Online-Übermittlung ist jeweils ein mit der AVAD abgeschlossener Vertrag, der die auf beiden Seiten zu beachtenden Sicherheitsanforderungen enthält.

Dazu gehört auch die Vereinbarung eines Stichprobenverfahrens. Den am Online-Verfahren beteiligten Versicherungsunternehmen werden von der AVAD die durchgeführten automatisierten Abrufe stichprobenweise aufgelistet und zur Überprüfung zugestellt.

Auch der jeweilige betroffene Vermittler erhält Kenntnis davon, daß Auskünfte sowohl in schriftlicher Form als auch über EDV online möglich sind. Dem Vermittler ist das „Informationsblatt über den AVAD-Auskunftsverkehr" vom Versicherungsunternehmen vor dem Einholen der AVAD-Auskunft auszuhändigen.

24.8.2 Aufnahme des Merkmals Versicherungsfachmann/-frau

An dem eingerichteten Online-Verfahren nimmt auch das Berufsbildungswerk der Deutschen Versicherungswirtschaft e. V. teil, das das Merkmal „Versicherungsfachmann/Versicherungsfachfrau BWV" zu dem jeweiligen Datensatz meldet.

Die Aufsichtsbehörde hatte dagegen zunächst geltend gemacht, daß dieses Merkmal nicht mehr von dem satzungsgemäßen Zweck der AVAD, wonach nur vertrauenswürdige Personen im Versicherungs- und Bausparkassenaußendienst oder als Versicherungsmakler tätig sein sollen, gedeckt ist. Vielmehr handelt es sich lediglich um die Aufnahme einer Berufsqualifizierung, die die Betroffenen dem jeweiligen Versicherungsunternehmen von sich aus mitteilen würden, so daß die Meldung entbehrlich wäre. Darüber hinaus fehlte jegliche Information der Betroffenen über die Datenübermittlung.

Auf Vorschlag der AVAD erklärte sich das Berufsbildungswerk dann damit einverstanden, in den Anträgen zum Ablegen der entsprechenden Prüfung darauf hinzuweisen, daß die AVAD über die Berechtigung zum Führen des Titels „Versicherungsfachmann/-frau" informiert wird. Für die Aufsichtsbehörde bestand daher kein Anlaß mehr, datenschutzrechtliche Bedenken geltend zu machen.

24.8.3 Löschungsfristen

Neu aufgegriffen wurde seitens der Aufsichtsbehörde die Frage, nach welchen Fristen die Daten von der AVAD gelöscht werden. Gemäß § 35 Abs. 2 Nr. 4 BDSG sind personenbezogene Daten zu löschen, wenn sie geschäftsmäßig zum Zwecke der Übermittlung verarbeitet werden und eine Prüfung am Ende des fünften Kalenderjahres nach ihrer erstmaligen Speicherung ergibt, daß eine längerwährende Speicherung nicht erforderlich ist. Es zeigte sich, daß die Daten bei der AVAD auch länger als 5 Jahre erhalten blieben und eine regelmäßige Löschung nicht erfolgte. Lediglich hinsichtlich der Übermittlungen wurden Einschränkungen gemacht.

Nunmehr nimmt die AVAD in regelmäßigen Abständen – längstens vierteljährlich – eine automatisierte Überprüfung der Löschungsfristen vor. Es wurden bestimmte Kriterien festgelegt, nach denen die Überprüfung und Löschung vorzunehmen ist. Darüber hinaus wurde der Aufsichtsbehörde zugesichert, die Löschungsansprüche auch im Einzelfall, z.B. bei entsprechenden Beschwerden, individuell zu überprüfen.

24.8.4 Registrierung von Versicherungsvermittlern

Eine Empfehlung der EG-Kommission vom 18. Dezember 1991 über Versicherungsvermittler sieht vor, daß nur noch in ein Register eingetragene Personen, die bestimmten Anforderungen genügen, die Tätigkeit eines Versicherungsvermittlers aufnehmen und ausüben dürfen. Nach der Antwort der Bundesregierung auf eine Große Anfrage zum vorsorgenden Verbraucherschutz im europäischen Versicherungswesen vom 5. Februar 1993 wird geprüft, ob die AVAD mit dem Aufbau dieser Registrierung beauftragt werden soll.

Die Aufsichtsbehörde Hamburg wird bei einer etwaigen Einrichtung eines entsprechenden Registers beteiligt werden. Einigkeit besteht schon jetzt über die Erforderlichkeit einer strikten Trennung von der vorhandenen Auskunftsdatei der AVAD.

24.8.5 Recht auf eigene Darstellung

Angesichts der bei der Aufsichtsbehörde in den vergangenen Jahren eingegangenen Eingaben, die die AVAD betrafen, ergibt sich auch an dieser Stelle die Frage nach einem Recht des Betroffenen auf eigene Darstellung (vgl. 1.3). Das Berichtigungsrecht, das bei verkürzter Darstellung einer Verfälschung der Daten entgegenwirkt, mag zwar vielfach zur Durchsetzung berechtigter Interessen weiterhelfen. Denkbar bleiben jedoch Fälle, in denen lediglich ein Anspruch auf Hinzufügung einer eigenen Darstellung den Persönlichkeitsrechten der Betroffenen gerecht wird und einen falschen Eindruck vermeiden hilft. Abzuwarten bleibt, ob sich diese Fragestellung künftig an konkreten Eingaben festmachen läßt.

25. Handels- und Wirtschaftsauskunfteien

25.1 Ergebnis der Arbeitsgruppe Handelsauskunfteien

25.1.1 Grenzüberschreitender Datenverkehr

Die bereits im 10. TB (26.2) und 11. TB (26.1) dargestellte Diskussion über den grenzüberschreitenden Datenverkehr wurde mit der Arbeitsgruppe „Handelsauskunfteien" fortgeführt, der neben Vertretern der Obersten Aufsichtsbehörden auch Vertreter der Handelsauskunfteien angehören. Die Aufsichtsbehörden wiesen erneut auf die Notwendigkeit von vertraglichen Lösungskonzepten hin, um bei Übermittlung personenbezogener Daten ins Ausland eine Gefährdung der schutzwürdigen Belange der betroffenen Personen zu vermeiden. Die Verträge sollten die wesentlichen Datenschutzelemente enthalten wie Verwendungszweck der Daten, Auskunftsrechte der Betroffenen, Rechte auf Berichtigung, Sperrung und Löschung, Benachrichtigungspflicht, Verpflichtung zu Datensicherungsmaßnahmen und Schadensersatzverpflichtungen.

Art. 27 Abs. 1 des Entwurfs der EG-Datenschutzrichtlinie zeigt, daß derartige vertraglich vorgesehene Schutzvorkehrungen zwischen Datenexporteur und -importeur auch nach Erlaß der Richtlinie von Bedeutung sein werden. Danach kann der Datentransfer in ein Drittland ohne angemessenes Schutzniveau genehmigt werden, wenn geeignete vertragliche Datenschutzbestimmungen vorliegen.

Nach der derzeitigen Rechtslage richtet sich die Übermittlung personenbezogener Daten ins Ausland nach den §§ 28, 29 BDSG. Falls es nicht im Rahmen der Zweckbestimmung des jeweiligen Vertrages liegt, kann die Übermittlung in Länder mit schwächerem oder gar fehlendem Datenschutz nach hiesigen Vorschriften unzulässig sein, wenn wegen der mangelnden Datenschutzvorkehrungen Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.

Ungeachtet dieser Rechtslage und der Aktualität von Vertragslösungen vor dem Hintergrund des Richtlinienentwurfs blieben die Handelsauskunfteien leider bei ihrer bisher vertretenen Auffassung (vgl. 11. TB, 26.1). Eine Notwendigkeit für Vertragslösungen sehen sie nicht. Allerdings teilten die Handelsauskunfteien mit, daß in ihrem Bereich derzeit Überlegungen für Verhaltensregeln auf internationaler Ebene angestellt würden.

Diese Überlegungen sind zwar zu begrüßen. Es darf aber nicht außer acht gelassen werden, daß Verhaltensregeln nur ergänzende Datenschutz-Maßnahmen für bestimmte Bereiche sein können. Ein wirksamer Datenschutz besteht für die Betroffenen nur bei Vorliegen verbindlicher Regelungen, wie zivilrechtliche Verträge sie enthalten können.

25.1.2 Umfang der Stichprobenkontrollen

Erfreulicherweise erklärten sich die Handelsauskunfteien nun bereit, den bisherigen Umfang von Stichprobenkontrollen (vgl. 11. TB, 26.2) von 1 auf 2 Promille zu erhöhen. Unabhängig von diesem Satz sollen pro Auskunftsstelle mindestens 12 gleichmäßig auf das Kalenderjahr verteilte Kontrollen pro Jahr durchgeführt werden.

25.1.3 Erweiterter Auskunftsanspruch

Ein weiterer Schwerpunkt der mit den Handelsauskunfteien geführten Diskussion lag in der Auslegung von § 34 Abs. 2 Satz 2 BDSG. Nach dieser Vorschrift kann der Betroffene von Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Auskunftserteilung speichern, Auskunft über Herkunft und Empfänger nur verlangen, wenn er begründete Zweifel an der Richtigkeit der Daten geltend macht. Nach Ansicht der Aufsichtsbehörden besteht der Anspruch auf Auskunft über Herkunft und Empfänger schon dann, wenn von mehreren in einer Auskunft enthaltenen Daten nur bei einem Datum von dem Betroffenen Angaben zur Unrichtigkeit gemacht werden. Ob es sich dabei um ein „wichtiges" oder „unwichtiges" Datum handelt oder auch nur um einen Schreibfehler, ist nach dem Wortlaut der Vorschrift unerheblich. So kann auch ein Schreibfehler beim Geburtsdatum den Auskunftsanspruch begründen.

Die Handelsauskunfteien vertraten bisher die Auffassung, daß der Auskunftsanspruch nicht bei jeder Unrichtigkeit bestehe, sondern voraussetze, daß das Persönlichkeitsrecht des Betroffenen durch die unrichtigen Daten beeinträchtigt werde. Die Unrichtigkeit müßte geeignet sein, die inhaltliche Aussage des Datensatzes insgesamt abzuändern und damit der Wirtschaftsauskunft eine andere Qualität zu geben. Sonst könnten durch die Auskunft erhebliche Geschäftszwecke von Informanten und Auskunftsempfängern gefährdet werden.

In der letzten Sitzung der Arbeitsgruppe konnte mit den Handelsauskunfteien nun Übereinstimmung darüber erzielt werden, daß grundsätzlich ein Auskunftsanspruch besteht, wenn von mehreren in einer Auskunft enthaltenen Daten lediglich in Bezug auf ein vergleichsweise unwesentlich erscheinendes Datum von dem Betroffenen Angaben zur Unrichtigkeit gemacht werden. Die Handelsauskunfteien räumten ein, daß der Wortlaut des § 34 Abs. 2 Satz 2 BDSG ihre bisher vertretene Auffassung nicht rechtfertige. Allerdings halten sie die Vorschrift für zu weitgehend.

Einigkeit bestand ferner in dem Punkt, daß ein bloßes Bestreiten der Richtigkeit der Daten zur Geltendmachung des Anspruchs nicht ausreicht. Zwar muß der Betroffene die richtigen Daten der speichernden Stelle nicht preisgeben. Er muß aber Angaben machen, aus denen sich tatsächliche Anhaltspunkte für eine mögliche Unrichtigkeit ergeben.

25.1.4 Telefonisches Auskunftsverfahren

Zwischen den Obersten Aufsichtsbehörden der Länder und den Handelsauskunfteien wurde auch das Verfahren bei Erteilung telefonischer Auskünfte erörtert. Zur Vermeidung von Mißbrauchsfällen halten die Aufsichtsbehörden mindestens die Erfassung des anfragenden Mitarbeiters eines Unternehmens im Auskunftsprotokoll für erforderlich. Auch sollten telefonische Auskünfte durch die Auskunftei schriftlich gegenüber dem Empfänger mit Angabe des anfragenden Mitarbeiters bestätigt werden. Die Handelsauskunfteien sagten eine Überprüfung zu.

25.2. Prüfung des Auskunftsverfahrens einer Handelsauskunftei

25.2.1 Inhalt von Auskünften

Im Berichtszeitraum gingen bei der Aufsichtsbehörde zahlreiche Eingaben ein, in denen die Petenten sich über den Inhalt von Auskünften einer großen Handelsauskunftei beschwerten. In den sog. „Konzeptauskünften", die den Betroffenen auf Anfrage nach § 34 BDSG übersandt wurden, finden sich neben der Adresse und dem Geburtsdatum häufig Formulierungen wie „in diesem Zusammenhang ließ sich nicht einwandfrei klären, wovon der Betroffene zur Zeit seinen Lebensunterhalt bestreitet" oder „ob es sich um die Liegenschaft des Betroffenen handelt, konnte nicht zweifelsfrei geklärt werden" oder „welcher Tätigkeit er nachgeht, war nicht eindeutig zu ermitteln".

Bei dem Empfänger einer solchen Auskunft kann durch derartige Formulierungen der Eindruck erweckt werden, der Lebenswandel des Betroffenen sei nicht einwandfrei oder der Betroffene versuche zu verschleiern, wovon er seinen Lebensunterhalt bestreitet. Die Auskunft läßt unrichtige Rückschlüsse auf persönliche und sachliche Verhältnisse des Betroffenen zu und greift damit ganz erheblich in sein Persönlichkeitsrecht ein. Eine Speicherung und Übermittlung derartiger Angaben verstößt gegen § 29 BDSG, da ein überwiegendes schutzwürdiges Interesse des Betroffenen an deren Ausschluß besteht.

In einem Gespräch erklärte sich die Handelsauskunftei bereit, keine derart vagen Formulierungen in den Auskünften mehr zu verwenden. Bei Nichtvorliegen von konkreten Informationen über Privatpersonen werden künftig Formulierungen gebraucht wie „Angaben zur Berufsausbildung liegen nicht vor", „der Genannte ist wirtschaftlich nicht in Erscheinung getreten" oder „die Zahlungsweise ist nicht zu beanstanden".

25.2.2 Auskunft über Herkunft und Empfänger der Daten

Im Gegensatz zu dem in der Arbeitsgruppe Handelsauskunfteien erzielten Einvernehmen über die Voraussetzungen des Auskunftsanspruchs nach § 34 Abs. 2 Satz 2 BDSG ist die geprüfte Handelsauskunftei grundsätzlich nicht bereit, den erweiterten Auskunftsanspruch bei Vorliegen begründeter Zweifel

an den in der Auskunft enthaltenen Daten zu akzeptieren. Nur dann, wenn durch ein unrichtiges Datum ein wirtschaftlicher Schaden des Betroffenen eintreten kann, besteht nach Ansicht der Auskunftei der Anspruch des Betroffenen nach § 34 Abs. 2 Satz 2 BDSG. Dies könne allenfalls bei Negativmerkmalen, wie z. B. Abgabe der eidesstattlichen Versicherung oder Haftanordnung, vorliegen. In den übrigen Fällen (z. B. Schreibfehler, falsche Beschreibung der ausgeübten Tätigkeiten) ist die Handelsauskunftei nur bei Vorliegen eines entsprechenden gerichtlichen Urteils zur Auskunft über Herkunft und Empfänger bereit.

Wir bedauern die Haltung der Handelsauskunftei. Die Auskunftsverweigerung verstößt gegen die Vorschrift des § 34 Abs. 2 Satz 2 BDSG. Zudem läßt sie Zweifel an der Sinnhaftigkeit von Arbeitsgruppen wie der Arbeitsgruppe „Handelsauskunfteien" zu, wenn die darin erzielten Ergebnisse von einzelnen Handelsauskunfteien angezweifelt werden. Da die Auskunftsverweigerung auch keine Ordnungswidrigkeit ist, bleibt dem Betroffenen nur die zivilrechtliche Klage auf Auskunft.

25.2.3 Zeitpunkt des Benachrichtigungsschreibens

Nach § 33 Abs. 1 Satz 2 BDSG ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. Wann die Benachrichtigung zu erfolgen hat, sagt die Vorschrift nicht. Die Kommentierungen zu § 33 BDSG sprechen aber von einer „angemessenen" Frist oder „unverzüglichen" Bekanntgabe. Um Nachteile für den Betroffenen durch evtl. unrichtig übermittelte Daten zu verhindern, sollte regelmäßig innerhalb von 2 bis 3 Wochen nach der Übermittlung die Benachrichtigung des Betroffenen durch die Auskunftei erfolgen. Dabei kann auf betriebliche Erfordernisse, etwa eine Versendung mit anderweitiger Post in absehbarer Zeit, Rücksicht genommen werden.

Die von uns überprüfte Handelsauskunftei fertigte aus organisatorischen Gründen alle 6 Wochen bis 3 Monate schubweise Benachrichtigungsschreiben an die Betroffenen. Auf unseren Einwand hin, daß diese Frist zu lang sei, sagte sie eine Überprüfung zu, ob künftig eine kurzfristige Benachrichtigung möglich sei.

25.2.4 Dauer der Speicherung des berechtigten Interesses

Nach § 29 Abs. 2 Satz 3 BDSG sind bei der Übermittlung personenbezogener Daten die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Über die Dauer der Aufzeichnungen enthält das Gesetz keine Angaben. Derzeit werden bei der Handelsauskunftei Angaben über den Anfragenden (Name, berechtigtes Interesse, Tag der Beauskunftung) nur noch 6 Monate beim Datensatz des Betroffenen gespeichert. Kopien über die Auskunftsempfänger und deren berechtigtes Interesse werden allerdings zusätzlich 1 1/4

Jahr lang in einem gesicherten Raum verwahrt. Bei Kenntnis des genauen Auskunftsdatums kann die Handelsauskunftei so nachvollziehen, wer aus welchem Grund angefragt hat.

Gegen dieses Aufbewahrungsverfahren spricht, daß für den Betroffenen der Tag der Auskunftserteilung gerade nicht mehr nachvollziehbar ist, wenn er nur 6 Monate im Datenbestand gespeichert wird. Die Aufzeichnungsfrist von 6 Monaten ist viel zu kurz, um eine wirksame Datenschutzkontrolle möglich zu machen. Hierbei ist auch zu berücksichtigen, daß das Benachrichtigungsschreiben nach § 33 BDSG manchmal erst 3 Monate nach dem Auskunftsersuchen erfolgt. Überlegt der Betroffene dann noch ein paar Wochen, ob er von seinen Kontrollmöglichkeiten Gebrauch machen will, kann es schon zu spät sein, da entsprechende Hinweise im Datenbestand gelöscht sind. Ein Jahr muß daher das Minimum für die Speicherung des Auskunftsersuchens sein.

25.2.5 Nachmeldungen

Nachmeldungen, die Negativdaten (Eintragungen im Schuldnerverzeichnis) betreffen, werden von der Handelsauskunftei ohne weitere konkrete Anfrage 6 Monate nach der ersten Auskunft erteilt. Bedenken gegen das Nachmeldeverfahren bestehen nach § 29 Abs. 1 Nr. 1a BDSG. Danach ist die Übermittlung von personenbezogenen Daten nur zulässig, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat.

Dieses berechtigte Interesse ist aber im Einzelfall zu überprüfen und nicht generell anzunehmen. Es kann nicht einfach davon ausgegangen werden, daß ein solches berechtigtes Interesse bei Anbahnung von Geschäftsbeziehungen auch nach 6 Monaten noch zwingend besteht. Selbst wenn sich in vielen Fällen die Vertragsabwicklung über einen längeren Zeitraum hinziehen kann, folgt darauf nicht unmittelbar in jedem Fall ein berechtigtes Interesse. Viele Geschäftsbeziehungen werden auch nicht auf Dauer angelegt und bestehen nach 6 Monaten bereits nicht mehr. Wir haben der Handelsauskunftei unsere Auffassung mitgeteilt. Ob eine Änderung des Verfahrens erfolgt, bleibt abzuwarten.

25.2.6 Recht auf eigene Darstellung

Im Zusammenhang mit einer Eingabe im Berichtszeitraum stellte sich die Frage, ob auch im Bereich der Tätigkeit der Handelsauskunfteien die Regelung eines Rechts auf eigene Darstellung (1.3) wünschenswert und erforderlich wäre. Der Eingabe lag folgender Sachverhalt zugrunde:

Ein Petent, Komplementär einer KG, beschwerte sich darüber, daß in der Auskunft über die KG auch ein Hinweis über die gegen ihn erfolgte Haftanordnung zur Abgabe der eidesstattlichen Versicherung enthalten war. Der Haftanordnung lag eine geringfügige Gerichtskostenforderung aus einem Familienrechtsstreit zugrunde, deren Begleichung er aus persönlichen Gründen ablehnte und die auf die Bonität des Unternehmens keinen Einfluß hatte. Ohne

Kenntnis dieser Umstände mußten Auskunftsempfänger davon ausgehen , daß die Haftanordnung gegen den Komplementär von erheblicher Bedeutung für die Bonität des Unternehmens war. Der Kontextverlust konnte zu Fehlinterpretationen führen, zumal der Bonitätsindex für das Unternehmen auf die höchstmögliche Kennziffer geändert und somit das Risiko für Kreditgeber als besonders hoch bewertet wurde. In Absprache mit dem Petenten haben wir daher die Handelsauskunftei gebeten, ihren Auskünften eine Ergänzung hinzuzufügen, daß die Eintragung im Schuldnerverzeichnis die Bonität des Unternehmens nicht betreffe. Die Auskunftei hat dem entsprochen.

Ein gesetzlicher Anspruch auf eine derartige Ergänzung durch die Auskunftei besteht dann, wenn das in der Auskunft enthaltene Datum über die Eintragung im Schuldnerverzeichnis, das für sich genommen nicht unrichtig war, zu einer Fehleinschätzung mit unrichtigen Schlußfolgerungen führt. Diese Form des Berichtigungsanspruchs ist im Rahmen der Auslegung des § 35 BDSG anerkannt. Eine andere Frage ist es, ob der Betroffene in Fällen von Kontextverlust – mit oder ohne Unrichtigkeiten im datenschutzrechtlichen Sinn – die Speicherung seiner eigenen Darstellung bei den Daten der Auskunftei verlangen kann. Dies würde einerseits den Interessen des Petenten entsprechen und andererseits den Interessen der Auskunftsempfänger nicht entgegenstehen. Wir werden weiter beobachten, ob – unabhängig von diesem Einzelfall – im Bereich der Tätigkeit der Auskunfteien ein Bedarf für eine gesetzliche Regelung des Rechts auf eigene Darstellung besteht.

26. Kreditwirtschaft

26.1 Euroscheck-Chip-Karte

Nach Presseberichten will das deutsche Kreditgewerbe spätestens bis Ende 1994 die Euroscheck-Karte mit einem multifunktionalen Computer-Chip ausstatten. Damit soll dem bargeldlosen kartengestützten Zahlungsverkehr zum Durchbruch verholfen werden. Nach den Überlegungen des Kreditgewerbes soll die mit dem Chip ausgestattete Euroscheck-Karte sowohl als Telefon-Wertkarte als auch als Kleingeldbörse für bestimmte Bereiche, u.a. den öffentlichen Nahverkehr, genutzt werden können.

Bereits seit Mitte 1993 wird die Eurocard mit integriertem Telekomchip, die bereits von einigen Banken angeboten wird, genutzt. Mit dieser Karte läßt sich unbegrenzt telefonieren. Die Telekom erstellt einmal monatlich unter der individuellen Referenznummer des Chips eine Abrechnung, die sie an die Gesellschaft für Zahlungssysteme weiterleitet. Dort wird die Verbindung zwischen der Referenznummer und dem Kunden hergestellt und dessen Kreditkarten-Konto mit dem entsprechenden Rechnungsbetrag belastet.

Wegen der Bedeutung der neuen Zahlungssysteme und dem dadurch möglichen Überwachungspotential durch gezieltes Auswerten von personenbezoge-

nen Daten haben wir den Bundesverband Deutscher Banken, der derzeit den Vorsitz im Zentralen Kreditausschuß hat, schon frühzeitig um Informationen zu den Chipkarten gebeten. Gerade im Vorfeld derartiger Vorhaben sollten die rechtlichen und technischen Aspekte ausreichend erörtert werden, um Mißbrauchsmöglichkeiten zu vermeiden. Wir haben auch ein Informationsgespräch zwischen Vertretern des Zentralen Kreditausschusses und den Obersten Aufsichtsbehörden vorgeschlagen, um zu verhindern, daß erst im nachhinein eine datenschutzrechtliche Begutachtung durch die Aufsichtsbehörden vorgenommen werden kann.

Der Bundesverband Deutscher Banken hat nun mitgeteilt, daß es derzeit noch keinen Beschluß des Zentralen Kreditausschusses gebe, die Euroscheck-Karte mit einem Computer-Chip auszustatten. Es sei noch offen, ob ein multifunktionaler Chip der Kreditwirtschaft auch an Kartentelefonen der Telekom eingesetzt werden könne. Wegen des Stadiums der Konzeptionierung könnten noch keine konkreten Aussagen zu Datenströmen getroffen werden. Erst wenn konkretere Planungen vorlägen, könnten die Aufsichtsbehörden umfassend unterrichtet werden.

Der Zentrale Kreditausschuß hat aber zu den Datenwegen bei der Eurocard mit integriertem Telefonchip ausführlich Stellung genommen. Wir werden eine datenschutzrechtliche Begutachtung dieses Zahlungsverfahrens durch die Obersten Aufsichtsbehörden anregen.

Im übrigen begrüßen wir die Bereitschaft der Kreditwirtschaft, die Aufsichtsbehörden in naher Zukunft über die mit dem Einsatz des geplanten Multifunktionschips verbundene Datenverarbeitung zu informieren. Eine Einflußnahme auf die Ausgestaltung des Zahlungssystems ist auch hier durch vorbeugenden Datenschutz geboten und nicht erst durch Nachbesserungen, die bei dem dann bereits eingeführten System schwierig durchzuführen sein werden.

26.2 Schlichtung von Kundenbeschwerden im deutschen Bankgewerbe

Der Bundesverband Deutscher Banken hat im Juni wegen der zunehmenden Auseinandersetzungen zwischen Banken und ihren Kunden ein Schlichtungsverfahren zur Beilegung von Meinungsverschiedenheiten eingeführt (vgl. im einzelnen zu dem Verfahren Hoeren, NJW 1992, 2727 ff). Nach Angaben der Bundesverbandes haben sich bisher bis auf ganz wenige Ausnahmen alle privaten Banken dem Verfahren angeschlossen.

Das Schlichtungsverfahren ist zulässig bei Beschwerden privater Verbraucher. Die Beschwerden sind zunächst an die Kundenbeschwerdestelle zu richten, die beim Bundesverband Deutscher Banken (Mohrenstr. 35–41, 50670 Köln) und beim Verband Deutscher Hypothekenbanken (Holbeinstr. 17, 53175 Bonn) bestehen. Dort erfolgt eine Vorprüfung und anschließend die Weiterleitung der Beschwerdeschrift an die betroffene Bank. Diese erhält eine Frist von einem Monat zur Stellungnahme. Reagiert die Bank nicht, legt die Kundenbeschwerdestelle dem Ombudsmann das Schreiben des Kunden vor. Der Ombudsmann entscheidet die Streitlage aufgrund der ihm vorliegenden Unterlagen. Er kann die Parteien auch zu schriftlichen oder mündlichen Ergänzungen auffordern. Derzeitiger Ombudsmann ist Dr. Leo Parsch, ehemaliger Präsident des Bayerischen Verfassungsgerichtshofs.

Der abschließende Schlichtungsspruch ist nur für die Bank bindend, sofern der Streitwert unterhalb des Höchstbetrags für vermögensrechtliche Klagen vor den Amtsgerichten liegt. Der Beschwerdeführer kann in jedem Fall die ordentlichen Gerichte anrufen.

Es bleibt abzuwarten, ob das Schlichtungsverfahren von Verbrauchern und Banken akzeptiert wird und welche Bedeutung es erlangt.

27. Kartengestützte Zahlungsverfahren

27.1 Fahrkartenverkauf beim Hamburger Verkehrsverbund (HVV) mit Euroscheck-Karte

Die Aufsichtsbehörde hat im Berichtszeitraum erst durch Presseveröffentlichungen davon erfahren, daß der HVV ein bargeldloses Zahlungssystem beim Fahrkartenverkauf einführen will. Wir haben daraufhin das Unternehmen gebeten, uns die Einzelheiten des Vorhabens näher zu erläutern. Diese Gespräche sind aus unserer Sicht konstruktiv verlaufen und haben mittlerweile folgenden Sachstand erreicht:

Der HVV beabsichtigt, zum Bezahlen des Fahrpreises den Einsatz der Euroscheck-Karte (EC-Karte) vorzusehen und dabei zahlreiche personenbezogene Daten zu erheben und weiter zu verarbeiten. Dabei soll ein Datensatz automatisiert gespeichert werden, der die EC-Kartennummer mit Bankleitzahl des Fahrgastes sowie Datum, Uhrzeit, Automatennummer und Preisstufe der jeweiligen Fahrten enthält. Der HVV will über einen bestimmten Zeitraum oder bis zu einem bestimmten Höchstbetrag diese Daten sammeln und die aufsummierten Fahrpreise dann in einer Summe vom Bankkonto des jeweiligen Fahrgastes abbuchen. Dann gäbe es den „gläsernen" Fahrgast, an dessen Daten über das Fahrverhalten auch andere Stellen wie Polizei, Finanzamt und Arbeitgeber interessiert wären.

Gegen ein solches Fahrkartensystem, das genaue Informationen über das Fahrverhalten der Fahrgäste für längere Zeit vorhält, bietet das Bundesdatenschutzgesetz keine Hilfe, weil diese Fahrgeldabrechnung in den Allgemeinen Geschäftsbedingungen des HVV und damit für den Beförderungsvertrag wirksam geregelt wäre. Jedoch ist gerade bei öffentlichen Unternehmen – wie dem HVV – jeweils zu prüfen, ob nicht datenschutzfreundlichere Lösungen möglich sind.

Die Aufsichtsbehörde hat in den Gesprächen mit dem HVV auf mögliche Alternativen hingewiesen, die es erlauben, im automatisierten Verfahren bargeldlos

die öffentlichen Verkehrsmittel benutzen zu können, ohne Angaben über die eigene Person machen zu müssen. Im Mittelpunkt unserer Überlegungen stand dabei ein Pilotprojekt in Kiel, das sich dort unter dem Motto „Busfahren mit Telefonkarte" in der Erprobung befindet. Dabei kann mit Hilfe einer Telefonkarte der Telekom, die keinerlei personenbezogene Daten enthält, ein Fahrschein erworben werden. Ein solches datenschutzfreundliches Verfahren hat den Vorteil, daß es auch bundesweit eingesetzt werden kann.

Der HVV favorisiert allerdings weiterhin die Verwendung der EC-Karte, weil dieses Kartensystem in der Bevölkerung am weitesten verbreitet und akzeptiert sei. Wir stehen einer solchen Lösung nicht grundsätzlich ablehnend gegenüber, meinen jedoch, daß erst die Einführung der EC-Karte mit einem zusätzlichen Chip für Guthaben abgewartet werden soll. Dann ist es möglich, daß die Fahrkostenpreise von einem auf dem Chip gespeicherten Guthaben ohne Personenbezug hinsichtlich der vorgenommenen Fahrten abgezogen werden. Es ist nach unserer Kenntnis auch möglich, ein Guthaben auf dem Chip jeweils zu erneuern; seit kurzem soll dies sogar telefonisch möglich sein. Ein solches Verfahren wäre also zugleich anwender- und datenschutzfreundlich.

Wir haben deshalb den HVV gebeten, eine endgültige Systemauswahl erst zu treffen, wenn die Auswertung des Kieler Pilotprojektes mit der Telefonkarte sowie die Prüfung einer Nutzung der EC-Karte als Wertkarte vorliegt. Deshalb betrachten wir das zur Zeit vom HVV vorgesehene Verfahren allenfalls als Test.

Schon jetzt hat sich der HVV bereit erklärt, den Zugriff auf die Daten, die auf dem Kontoauszug wiedergegeben sind, besser abzusichern. Zunächst war beabsichtigt, dem Kunden unter einer Service-Telefonnummer entweder per Sprachausgabe (Computer) oder auf Wunsch von einem personalbedienten Arbeitsplatz Auskunft über seine einzelnen Fahrscheinkäufe zu erteilen. Hierzu wäre lediglich die Nennung seiner auf dem Kontoauszug angegebenen Rechnungsnummer erforderlich gewesen. Dann hätten auch Dritte wie z.B. Familienangehörige bei Kenntnis des Kontoauszugs telefonisch Einzelheiten über die Fahrten erfahren können. Aufgrund unserer Bedenken will der HVV nunmehr als Kriterium zur Identitätsprüfung zusätzlich die Kartennummer heranziehen.

28. Auftragsdatenverarbeitung

Gemäß § 11 Abs. 1 BDSG ist der Auftraggeber auch dann für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich, wenn personenbezogene Daten im Auftrag durch andere Stellen verarbeitet oder genutzt werden.

Durch solche Auftragsverhältnisse werden Möglichkeiten geschaffen, ohne Prüfung der strengen Übermittlungsvoraussetzungen und der Einhaltung weiterer Pflichten – wie etwa der Benachrichtigung des Betroffenen – personenbezogene Daten an andere weiterzugeben. Hierin liegt der Grund für die besondere, über den eigenen Bereich hinausgehende Verantwortung des Auftraggebers, die sich in den Regelungen des § 11 BDSG ausdrückt. Da die eigentlich von entsprechenden Auslagerungen Betroffenen davon in der Regel nichts erfahren, muß die Aufsichtsbehörde ein besonderes Augenmerk auf die strikte Einhaltung der schriftlichen Auftragserteilung richten. Bei unseren Prüfungen im Rahmen der Überwachung nach § 38 BDSG sind wir vermehrt auf Probleme bei den Auftragsverhältnissen und den an sie gestellten gesetzlichen Anforderungen gestoßen. Nach § 11 BDSG hat der Auftraggeber folgende Vorgaben zu beachten:

- seine weiter bestehende Verantwortung für die Einhaltung der Vorschriften des BDSG und anderer datenschutzrechtlicher Vorschriften
- sorgfältige Auswahl des Auftragnehmers
- schriftlicher Auftrag unter
  a) Festlegung der technischen und organisatorischen Maßnahmen nach § 9 BDSG
  b) Bezeichnung etwaiger Unterauftragsverhältnisse
- konkrete Weisungen zur Datenverarbeitung an den Auftragnehmer
- Wahrnehmung seiner Kontrollpflicht.

Wir stellten bei unseren Prüfungen fest, daß vielfach der schriftliche Auftrag nicht vorlag. Wenn ein schriftlicher Vertrag abgeschlossen war, wurden die technischen und organisatorischen Maßnahmen oder etwaige Unterauftragsverhältnisse häufig nicht festgelegt. Der Auftraggeber beschränkte sich in seinen Weisungen auf die Wiederholung des Gesetzestextes, verwies auf die gesetzlichen Bestimmungen oder berief sich auf eigene datenschutzrechtliche Grundsätze, die nicht Bestandteil des Vertrages waren oder dazu gemacht wurden. Soweit sich Auftragnehmer eines Subunternehmers bedienten, hatte der Auftraggeber in einigen Fällen hiervon keine Kenntnis.

Da die Tätigkeit der Auftragsdatenverarbeitung als Dienstleistung angeboten wird, entwickeln diese Unternehmen oft auch die Verträge. Dies kann dazu führen, daß der Auftraggeber seine Verantwortung, sein Weisungs- und Kontrollrecht nicht mehr vollständig wahrnimmt und die Vertragsgestaltung dem Auftragnehmer überläßt, was nicht dem Gedanken des § 11 BDSG entspricht.

28.1 Akten- und Datenträgervernichtung

Das Problem der fehlenden oder unzureichenden schriftlichen Aufträge wird besonders deutlich im Bereich Akten- und Datenträgervernichtung, insbesondere bei Selbstanlieferern, die teilweise nur einmalig Material vernichten lassen wollen oder nur Kleinstmengen haben. In diesen Fällen werden oft lediglich Lieferscheine und Vernichtungszertifikate ausgestellt.

Auch bei langjährigen Kunden ist es in dieser Dienstleistungsbranche vielfach üblich, aufgrund eines telefonischen Auftrages tätig zu werden. Viele Unternehmen sind jedoch dazu übergegangen, schriftliche Verträge abzuschließen.

In einem Fall haben wir den Auftragnehmer gebeten, mit allen Auftraggebern einen schriftlichen Vertrag, der den Anforderungen des § 11 BDSG genügt, abzuschließen. Auf entsprechende Schreiben des Auftragnehmers reagierten jedoch nicht alle Auftraggeber. Die Aufsichtsbehörde erwägt nun, sich direkt an die Auftraggeber zu wenden, weil sie gegen die gesetzliche Pflicht nach § 11 Abs. 2 Satz 2 BDSG verstoßen, den Auftrag schriftlich zu erteilen.

Im Berichtszeitraum haben wir fast sämtliche Akten- und Datenträgervernichtungsunternehmen geprüft, die zum Register der Aufsichtsbehörde nach § 32 BDSG gemeldet sind. Soweit dabei das Fehlen eines schriftlichen Auftrages oder nicht ausreichende entsprechende Regelungen festgestellt wurden, ist dies im Prüfbericht bemängelt worden.

28.2 Transport von Datenmüll

Im Bereich der Akten- und Datenträgervernichtung sind uns zwei Fälle bekannt geworden, in denen die Auftraggeber lediglich einen Transporteur für das zu vernichtende Material beauftragten, obwohl ein Unternehmen sogar mit der Dienstleistung „Aktenvernichtung" wirbt. Diese Transporteure fahren das Material zum Aktenvernichtungsunternehmen und erhalten ein entsprechendes Zertifikat, das nicht an den Kunden weitergegeben wird.

Der Auftraggeber ist nicht einmal darüber informiert, daß diese Betriebe lediglich den Transport durchführen. Hätten die Auftraggeber einen schriftlichen Auftrag gemäß den Anforderungen des § 11 BDSG erteilt, wäre ihnen aufgefallen, daß der Auftrag gar nicht die Aktenvernichtung umfaßt. Da die Auftraggeber selbst für die Aktenvernichtung verantwortlich sind, sind die Verträge entsprechend auszugestalten.

29. Register nach § 32 BDSG und Prüftätigkeit

29.1 Register und Meldepflicht

Die Aufsichtsbehörde führt nach § 38 Abs. 2 BDSG ein Register der Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der personenbezogenen oder der anonymisierten Übermittlung speichern oder im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen. Diese Stellen unterliegen nach § 32 BDSG der Meldepflicht. Derzeit sind zu diesem Register 239 Unternehmen gemeldet. Unterteilt nach der Art der meldepflichtigen Tätigkeit ergibt sich folgendes Bild:

Speicherung zum Zwecke der Übermittlung

Auskunfteien/Warndienste	13
Direktmarketing/Adreßhändler	13

Speicherung zum Zwecke der anonymisierten Übermittlung

Markt- und Meinungsforschung	39

Auftragsdatenverarbeitung

Servicerechenzentren	26
Akten- und Datenträgervernichter	13
Mikroverfilmer	7
Datenerfasser	34
Mailboxen	3
sonstige Auftragsdatenverarbeitung	91

Eine Vielzahl von Unternehmen, die bislang nicht zum Register gemeldet waren, sind angeschrieben und um Prüfung der Meldepflicht und ggfs. Anmeldung gebeten worden. Dabei haben zahlreiche Informations- und Beratungsgespräche stattgefunden.

Wir haben mit Umstellungsarbeiten hinsichtlich einer Automatisierung des Registers und Aktualisierungsarbeiten zu den inhaltlichen Angaben im Register im Berichtszeitraum begonnen. In vielen Fällen wurden Verstöße gegen die Meldepflicht festgestellt. Dennoch wurde bisher davon abgesehen, Ordnungswidrigkeitenverfahren einzuleiten, weil die betroffenen Unternehmen die Meldungen umgehend nachgeholt haben.

29.2 Prüfungen

Der folgenden Übersicht sind die Zahlen der Überprüfungen vor Ort im Berichtszeitraum zu entnehmen:

Auskunfteien/Warndienste	3
Direktmarketing/Adreßhändler	5
Markt- und Meinungsforschung	2
Akten- und Datenträgervernichter	6
Servicerechenzentren	5
Mikroverfilmer	2
sonstige Auftragsdatenverarbeitung	6
gesamt	29

Folgende wesentliche Mängel wurden am häufigsten festgestellt:

— mangelhafte Zugangskontrolle

— keine ausreichende Funktionstrennung bei den Mitarbeitern innerhalb des Betriebes

— kein ausreichender Paßwortschutz

— Mängel in der Datenträgerkontrolle

— fehlende schriftliche Weisungen der Auftraggeber (siehe 28.)

— nicht mehr aktuelle Registermeldungen.

In zahlreichen Fällen bezogen sich die betrieblichen Hinweise zum Datenschutz auf das alte Bundesdatenschutzgesetz.

Die geprüften Stellen waren freiwillig bereit, festgestellte Mängel zu beheben. Bußgeldverfahren wurden deshalb nicht eingeleitet.

Darüber hinaus wurde eine Vielzahl von Unternehmen vor Ort aufgrund von Beschwerden oder anderen Anlässen, z.B. Presseveröffentlichungen, geprüft.

30. Arbeitnehmerdatenschutz

30.1 Psychologische Tests bei Auswahlverfahren

Im 11. TB (29.1) berichteten wir von rechtswidrigen „Bewerber-Psycho-Tests" der Firma U-Man International Hamburg, die in der Presse wiederholt Erwähnung gefunden hatte. Nach unserer Erkenntnis befindet sich diese Firma in der Liquidation, so daß kein weiterer Handlungsbedarf entstand.

Bei einem anderen Unternehmen hatten wir im Berichtszeitraum Gelegenheit, uns mit rechtmäßigen psychologischen Auswahlverfahren zu befassen. Eine Eingabe betraf das psychologische Auswahlverfahren einer Forschungsanstalt. Das Institut führt unter anderem im Auftrage von Fluggesellschaften das Auswahlverfahren für Pilotenbewerber oder auch für Fluglotsen durch. Die Auswahluntersuchungen beziehen sich auf zwei Bereiche, den Leistungs- und den Persönlichkeitsbereich.

Im Leistungsbereich werden Merkmale wie etwa Raumvorstellung, Merkfähigkeit (auditiv/visuell), Englisch-Kenntnisse usw. untersucht. Der Persönlichkeitsbereich untergliedert sich in Leistungsbereitschaft, interpersonales Verhalten (Kooperationsbereitschaft) und emotionale Stabilität (Belastungsfähigkeit). Erkenntnisquellen sind jeweils gezielte Fragen, psychologische Tests und psychologische Gespräche.

Wesentliche Beachtung findet, wie der Betroffene sich in vergleichbaren Situationen außerhalb der Berufstätigkeit verhalten hat. Fragen etwa nach einer Vereinstätigkeit des Betroffenen dienen dazu, mögliche Erkenntnisse über dessen Kooperationsbereitschaft zu erlangen. Gänzlich ausgenommen vom Testverfahren bleiben datenschutzrechtlich besonders sensible Bereiche wie politische Anschauungen bzw. eine etwaige Parteizugehörigkeit, religiöse Anschauungen und das Sexualleben.

Nach einem umfassenden Informationsgespräch bei dem Institut haben wir insgesamt den Eindruck gewonnen, daß das Auswahlverfahren auf die Berufsbilder abgestimmt ist und sich im Rahmen der von der Rechtsprechung entwickelten Grundsätze zum Fragerecht des Arbeitgebers bewegt. Die Komplexität des Verfahrens ist durch die vergleichsweise hohen Anforderungen an diese Berufe bedingt.

Ausdrücklich wurde von uns begrüßt, daß die erhobenen Daten nicht an den Auftraggeber übermittelt werden. Über die Auswahl entscheidet vielmehr eine Auswahlkommission, die sich aus Vertretern der Forschungsanstalt und des

Auftraggebers zusammensetzt. Nach der Entscheidungsfindung werden die Unterlagen zum Teil vernichtet, zum Teil verbleiben sie – insbesondere aus Gründen der Testnormierung und der Validierung – bei der Forschungsanstalt.

30.2 Arbeitsschutzrahmengesetz

Im Zuge der Umsetzung der sog. Rahmenrichtlinie zum Arbeitsschutz (Richtlinie 89/391/EWG des Rates vom 12. Juni 1989 über die Durchführung von Maßnahmen zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Arbeitnehmer bei der Arbeit) hatte der Bundesminister für Arbeit und Sozialordnung im Dezember 1992 den Entwurf eines Arbeitsschutzrahmengesetzes vorgelegt. Die Behörde für Arbeit, Gesundheit und Soziales (BAGS) hat in diesem Zusammenhang einen eigenen Entwurf eines Arbeitsschutzgesetzbuches, Erstes Buch „Allgemeiner Teil", erarbeitet und diesen im Juni 1993 dem Hamburgischen Datenschutzbeauftragten zur Abstimmung vorgelegt. Zum Entwurf der BAGS haben wir ausführlich Stellung bezogen. Anfang November 1993 erreichte uns der überarbeitete Bundesgesetzentwurf in der Fassung vom 22. Oktober 1993.

Bei aller Unterschiedlichkeit im einzelnen regeln die Entwürfe detailliert den Gesundheitsschutz der Beschäftigten am Arbeitsplatz. Aus datenschutzrechtlicher Sicht kommt der vorgesehenen Einführung genomanalytischer Untersuchungen besondere Bedeutung zu.

Der Bundesgesetzentwurf (in der Fassung des Referentenentwurfs vom 22. Dezember 1992) sah hierzu vor, daß nach Aufklärung und mit Einwilligung des betroffenen Arbeitnehmers im Rahmen von Vorsorgeuntersuchungen „genomanalytische Untersuchungen" zulässig sind, wenn durch sie „bestimmte ererbte Veranlagungen für Erkrankungen, die durch bestimmte Arbeitsbedingungen entstehen können," ermittelt werden. Darüber hinaus sollten genomanalytische Untersuchungen bei Erstuntersuchungen durch Verordnung zugelassen werden können. Dagegen durften bei Vorsorgeuntersuchungen Genomanalysen, „die der bloßen Aufdeckung der Erbanlagen der untersuchten Person dienen", nicht durchgeführt werden.

Im neuen Entwurf wurden die Voraussetzungen im Sinne des Datenschutzes verschärft: Genomanalytische Untersuchungen sind erst zulässig, wenn nach gesicherten Erkenntnissen der Arbeitsmedizin eine schwere bleibende Schädigung möglich ist, der Arbeitnehmer umfassend über die Gefahren, den Untersuchungsablauf, die Verwendung der Ergebnisse und die Notwendigkeit seiner Einwilligung aufgeklärt ist und schriftlich einwilligt. DNA-Analysen dürfen nur noch durchgeführt werden, soweit sie zusätzlich durch Gesetz ausdrücklich zugelassen sind. Für die Anwendung anderer Verfahren in Vorsorge- und Erstuntersuchungen bedarf es einer zusätzlichen Rechtsvorschrift. Ausdrücklich ist auch aufgenommen worden, daß nur die Verfahren angewendet werden dürfen, die die geringstmögliche Überschußinformation liefern.

In unserer kritischen Stellungnahme zu diesen Plänen haben wir uns leiten lassen von einem Beschluß der Datenschutzbeauftragten schon aus dem Jahre 1989. Die grundsätzlich ablehnende Auffassung des Hamburgischen Datenschutzbeauftragten gegenüber Genomanalysen im Arbeitverhältnis wurde bereits im 8. TB, 3.11.1.2 ausführlich wiedergegeben (vgl. auch 7. TB, 4.14.3).

Der jetzt vorliegende Referentenentwurf des Bundes berücksichtigt zwar die Entschließung der Datenschutzbeauftragten, wonach Genomanalysen im Arbeitsverhältnis wegen der Zweifel an der Freiwilligkeit von Einwilligungen nur aufgrund gesetzlicher Regelungen zulässig sein sollen. Hierauf darf sich der Schutz aber nicht beschränken; wir sind nach wie vor der Auffassung, daß es einer Zulassung von Genomanalysen im Arbeitsverhältnis überhaupt nicht bedarf, daß andererseits die Risiken für den Betroffenen bei einer Zulassung unverhältnismäßig hoch sind:

So können arbeitsmedizinische Tests zu Wirkungen von Risikostoffen durchaus ohne einen Namensbezug, etwa durch ein Strukturcode-Verfahren, durchgeführt werden. Zum Schutz des Arbeitnehmers kann sich dieser selbst – privat – einer Genomanalyse unterziehen. Dazu müßte ihm der Arbeitgeber allerdings die in Betracht kommenden Risikostoffe benennen.

Auch eine gesetzlich zulässige, vom Arbeitgeber veranlaßte Genomanalyse durch den Betriebsarzt würde das „Recht auf Nichtwissen" des Arbeitnehmers verletzen. Obwohl der Eintritt einer diagnostizierten Erbkrankheit zumindest hinsichtlich des Zeitpunkts völlig ungewiß ist, kann diese Offenbarung auch das private Leben des Betroffenen tiefgreifend verändern. Der Arbeitgeber kann sich durch die Nichteinstellung oder Entlassung des Betroffenen einseitig und auf Kosten des Arbeitnehmers vom Risiko des Krankheitseintritts und möglicherweise faktisch auch von objektiven Arbeitsschutzmaßnahmen entlasten. Aus denselben Gründen muß auch die Überlassung von privat angefertigten Genomanalysen ausdrücklich ausgeschlossen werden.

Alle diese Gründe gebieten nach unserer Auffassung, Genomanalysen im Arbeitsverhältnis prinzipiell abzulehnen, um den Anfängen zu wehren.

Geschäftsverteilung (Stand: 1. Dezember 1993)

Der Hamburgische Datenschutzbeauftragte
Baumwall 7, 20459 Hamburg

Tel.: 040/3504-2044
BN: 9.41-2044
Fax: 040/3504-2372

			Durchwahl
Dienststellenleiter:	Dr. Hans-Hermann Schrader	D	-2044-
Stellvertreter:	Peter Schaar		-2231-
Vorzimmer:	Eva-Maria Reupke		-2045-

D 1 – Geschäftsstelle

			Durchwahl
Leiter:	Gunnar Hansen	D 1	-2223-
Sachbearbeiterin:	Annelies Franke	D 10	-2063-
Mitarbeiterinnen:	Eva-Maria Reupke	D 11	-2045-
	Irene Heinsohn	D 12	-2047-

D 1: Allgemeine Verwaltungsangelegenheiten
Tätigkeitsberichte
Konferenz der Datenschutzbeauftragten
Öffentlichkeitsarbeit
Geheimschutzangelegenheiten

D 10: Systemverwaltung (mit D 32)
Bibliothek
Register nach § 24 HmbDSG
Bearbeitung von Eingaben
Verwaltung von Senats-/Bürgerschaftsdrucksachen

D 11: Vorzimmerdienst
Textverarbeitung
Eingabenverwaltung

D 12: PC-Textverarbeitung
Registratur
Postverteilung

D 2 – Referat

			Durchwahl
Leiter:	Matthias Burba	D 2-1	-2046-
	Ulrich Werner	D 2-2	-2581-
Sachbearbeiter:	Gunnar Hansen	D 21	-2223-

D 2-1: Grundsatzfragen des Datenschutzes
Novellierung der Datenschutzgesetze
Parlamentsangelegenheiten
Verfassungsschutz
Justiz
Staatsanwaltschaft
Strafvollzug
Ausbildungsleiter für die Juristenausbildung

D 2-2: Polizei und Feuerwehr
Meldewesen
Ausländerwesen
Personenstandswesen
Straßenverkehrsverwaltung
Verkehrsordnungswidrigkeiten

D 21: Bau-, Vermessungs- und Wohnungswesen
Eingabenbearbeitung im Referatsbereich ohne Polizei, Justizverwaltung und Staatsanwaltschaft

D 3 – Referat

			Durchwahl
Leiter:	Peter Schaar	D 3	–2231–
Referent:	Uwe Schläger	D 30	–2564–
Referent:	Ulrich Kühn	D 31	–2564–
Sachbearbeiter:	Dietmar Nadler	D 32	–2236–

D 3: Grundsatzfragen der IuK-Technik und -Organisation
Telekommunikation
Online-Datenbanken
technische Assistenz für die Bereiche
— Polizei/Meldewesen
— Verfassungsschutz
— Justiz
— Wissenschaft und Forschung
— Kultur
— nicht-öffentlicher Bereich
datenschutzrechtliche Betreuung der Bereiche
— Statistik
— Wahlen
— Medien
— Natur- und Umweltschutz

D 30: LAN
MS-DOS
Host-PC-Kopplung
Electronic-Cash
technische Assistenz für die Bereiche
— Sozialwesen/PROSA
— Gesundheitswesen
— Archivwesen
datenschutzrechtliche Betreuung des Bereichs Stadtentwicklung

D 31: Überwachungstechniken
UNIX
technische Assistenz für die Bereiche
— Schulwesen
— Senatsamt für Bezirksangelegenheiten
— Wirtschaftsverwaltung

D 32: Richtlinien zur Datensicherung und Datenverarbeitung
Systemverwaltung (mit D 10)
IuK-Gesamtplan
Speichertechnik
BS 2000
MVS
technische Assistenz für die Bereiche
— Bauwesen
— Personalwesen
— Bürgerschaft
datenschutzrechtliche Betreuung der Bereiche
— Finanz-, Steuer- und Rechnungswesen
— Organisationswesen

D 4 – Referat

			Durchwahl
Leiter:	Dr. Hans-Joachim Menzel	D 4	–2558–
Sachbearbeiter:	Achim Kruppke	D 41	–2563–

D 4: Gesundheitswesen mit medizinischer Forschung (öffentlicher und nicht-öffentlicher Bereich)
Kultur

D 41: Arbeits- und Sozialwesen

D 5 – Referat

			Durchwahl
Leiterin:	Verena Scheffler-Ritters	D 5	–2562–
Sachbearbeiter:	Achim Kruppke	D 51	–2563–

D 5: Arbeitnehmer-Datenschutz
(öffentlicher und nicht-öffentlicher Bereich)
Archivwesen
Wirtschaft und Landwirtschaft
Wissenschaft und Forschung

D 51: Schulwesen

D 6 – Referat

			Durchwahl
Leiterinnen:	Helga Naujok	D 6-1	–2556–
	Elisabeth Duhr	D 6-2	–2541–
Referent:	Detlef Malessa	D 60	–2089–
Sachbearbeiterin:	Evelyn Seiffert-Rosenboom	D 61	–2468–

Aufsichtsbehörde nach § 38 Bundesdatenschutzgesetz

D 6-1: Versicherungswirtschaft einschließlich Vorsitz im Arbeitskreis Versicherungswirtschaft der Aufsichtsbehörden
Allfinanz-Gruppen
Handel, Industrie
Düsseldorfer Kreis der Aufsichtsbehörden

D 6-2: Auskunfteien, Wirtschafts- und Handelsauskunfteien
SCHUFA
Kreditwirtschaft
Internationaler Datenverkehr im öffentlichen und nicht-öffentlichen Bereich, insbesondere Datenschutzrecht der Europäischen Gemeinschaften

D 60: Auftragsdatenverarbeitung
Versandhandel
Werbung und Adreßhandel
Bauen und Wohnen, insbesondere Mietangelegenheiten
Transport und Verkehr einschließlich HVV
Freie Berufe und gewerbliche Dienstleistungen
Sonstige Rechtsfragen zum Datenschutz in der Wirtschaft

D 61: Markt- und Meinungsforschung
Datenbankbetreiber und Netzanbieter
Bildschirmtext und Mailboxen
Allgemeine Beratung von betrieblichen Datenschutzbeauftragten
Grundsätzliche Fragen zum Register nach § 32 BDSG
Akten- und Datenträgervernichtung

Stichwortverzeichnis

Abkürzungen

AG-Kripo	Arbeitsgruppe Kriminalpolizei der Innenministerkonferenz
AGJWG	Ausführungsgesetz zum Jugendwohlfahrtsgesetz
AGKJHG	Ausführungsgesetz zum Kinder- und Jugendhilfegesetz
AK	Allgemeines Krankenhaus
AO	Abgabenordnung
AOÄG	Gesetz zur Änderung der Abgabenordnung und anderer Rechtsvorschriften
APIS	Arbeitsdatei PIOS „Innere Sicherheit"
APOK	Arbeitsdatei PIOS „Organisierte Kriminalität"
APR	Arbeitsdatei PIOS „Rauschgift"
ARB	Allgemeine Bedingungen für die Rechtsschutzversicherung
ARD	Arbeitsgemeinschaft der Rundfunkanstalten Deutschlands
AuslG	Ausländergesetz
AVAD	Auskunftsstelle über den Versicherungsaußendienst e.V.
BAGS	Behörde für Arbeit, Gesundheit und Soziales
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
BfI	Behörde für Inneres
BGS	Bundesgrenzschutz
BIS	Bodeninformationssystem
BHH	Betreuungsgesellschaft für den Hamburger Hauptbahnhof GmbH
BKK	Betriebskrankenkasse
BRat	Bundesrat
BSHG	Bundessozialhilfegesetz
BSJB	Behörde für Schule, Jugend und Berufsbildung
Btm	Betäubungsmittel
Btx	Bildschirmtext
BVerfGE	Bundesverfassungsgerichtsentscheidung
BVerfSchG	Bundesverfassungsschutzgesetz
BVSt	Besoldungs- und Versorgungsstelle
BZRG	Bundeszentralregistergesetz
COMVOR	Projekt „Computerunterstützte Vorgangsbearbeitung" bei der Polizei
D1,D2	digitale Mobilfunknetze
DB	Deutsche Bundesbahn
DDV	Deutscher Direktwerbe- und Direktmarketing Verband
DNA	Desoxyribonucleinsäure
DV	Datenverarbeitung
DVU	Deutsche Volksunion
EC-Karte	Euroscheck-Karte
EDV	Elektronische Datenverarbeitung

EDU	European Drug Unit – Europäische Drogenzentralstelle
EG	Europäische Gemeinschaft
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
EIS	Europäisches Informationssystem der Polizei
Europol	Zentrales Europäisches Kriminalamt
FIS	Flächenbezogenes Informationssystem
FKPG	Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms
GBG	geschlossene Benutzergruppe
GG	Grundgesetz
GwG	Geldwäschegesetz
HdlStatG	Gesetz über die Statistik im Handel und Gastgewerbe (Handelsstatistikgesetz)
HGV	Hamburger Gesellschaft für Beteiligungsverwaltung
HHA	Hamburger Hochbahn Aktiengesellschaft
HmbBG	Hamburgisches Beamtengesetz
HmbDSG	Hamburgisches Datenschutzgesetz
HmbMG	Hamburgisches Meldegesetz
HmbMedienG	Hamburgisches Mediengesetz
HmbMeldeDÜV	Hamburgische Verordnung über regelmäßige Datenübermittlungen aus dem Melderegister
HmbPersVG	Hamburgisches Personalvertretungsgesetz
HmbStatG	Hamburgisches Statistikgesetz
HmbVermG	Hamburgisches Vermessungsgesetz
HUIS	Hamburger Umweltinformationssystem
HVV	Hamburger Verkehrsverbund
ID	individuelle Kennung eines Gerätes (z. B. Computers) oder eines Benutzers
INPOL	Informationssystem der Polizei (bundesweit)
ISDN	Integrated Services Digital Network — Integriertes digitales Kommunikationssystem
ISmed	Informationssystem für die MDK-Beratungsstellen
IuK	Informations- und Kommunikationstechnik
JVA	Justizvollzugsanstalt
KAN	Kriminalaktennachweis in INPOL
KORA	Koordinationsstelle zur Bekämpfung der offenen Rauschgiftszene in St. Georg
KPMD-S	kriminalpolizeilicher Meldedienst in Staatsschutzsachen
KpS	kriminalpolizeiliche Sammlung
LAN	Local Area Network – lokales Netzwerk
LBK	Landesbetrieb Krankenhäuser
LIT	Landesamt für Informationstechnik
LVA	Landesversicherungsanstalt
MALENA	Projekt „Maschinenlesbares Narkoseprotokoll"
MDK	Medizinischer Dienst der Krankenversicherungen

MiStra	Anordnung über Mitteilungen in Strafsachen
MittVw	Mitteilungen für die Verwaltung
MobiDik	Projekt „Mobile Datenerfassung im Krankenhaus"
MODACOM	Mobile Datenkommunikation – Dienst der Deutschen Bundespost – TELEKOM –
MRRG	Melderechtsrahmengesetz
MTA	Medizinisch-Technischer Assistent
NADIS	Nachrichtendienstliches Informationssystem
NDR	Norddeutscher Rundfunk
NJW	Neue Juristische Wochenschrift
OK	organisierte Kriminalität
OLG	Oberlandesgericht
OrgKG	Gesetz zur Bekämpfung der organisierten Kriminalität
PAULA	Projekt „Automation des Ausländer- und Asylwesens"
Pay per View	Form von Pay TV, bei der für jede empfangene Sendung gezahlt wird
Pay TV	entgeltpflichtiges Fernsehen
PÄD	Personalärztlicher Dienst
PC	Personalcomputer
PHW	personenbezogener Hinweis in polizeilichen Dateien
PIK	Projekt „Pflegedienst im Krankenhaus"
PIOS	Personen, Institutionen, Objekte, Sachen – Dateityp in INPOL
POLAS	Polizeiliches Auskunftssystem (Hamburg)
PolDVG	Gesetz über die Datenverarbeitung der Polizei
PROJUGA	Projekt Jugendamts-Automation
PROPERS	Projekt Personalwesen
PROSA	Projekt Sozialhilfe-Automation
PStG	Personenstandsgesetz
PULS	Projekt „Pflegedienstunterstützung für die LBK-Stationen"
Quasic	Projekt „Qualitätssicherung in der Chirurgie"
RAK	Referatsarbeitskartei des Landesamtes für Verfassungsschutz
SÄD	Schulärztlicher Dienst
SED	Sozialistische Einheitspartei Deutschlands
SfB	Senatsamt für Bezirksangelegenheiten
SfV	Senatsamt für den Verwaltungsdienst
SGB-IV	Sozialgesetzbuch/Viertes Buch
SGB-VI	Sozialgesetzbuch/Sechstes Buch
SGB-X	Sozialgesetzbuch/Zehntes Buch
SINIX	herstellerspezifische Variante des Betriebssystems UNIX
SOG	Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung
SOS	Studentenoperationssystem

StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrszulassungsordnung
SVA	Sozialversicherungsausweis
TB	Tätigkeitsbericht
TK-RL	Telekommunikationsrichtlinie
UIG	Umweltinformationsgesetz
UNIX	Betriebssystem für Mehrplatz-Computersysteme
WAN	Wide Area Network – behördenübergreifendes Netzwerk
WoBindG	Wohnungsbindungsgesetz
WEG	Wohnungseigentumsgesetz
ZDF	Zweites Deutsches Fernsehen