BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG

Drucksache 14/1016

14. Wahlperiode

16. 01. 92

Der Hamburgische Datenschutzbeauftragte

An die
Frau Präsidentin der Bürgerschaft

Betr.: Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

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

Dem Senat leite ich den Tätigkeitsbericht gleichzeitig zu.

Dr. Schrader

* Verteilt nur an die Abgeordneten der Bürgerschaft

Bürgerschaftsdrucksachen — außer Senatsvorlagen — sind zu beziehen bei:
Druckerei Warlenberg & Söhne GmbH, Theodorstraße 41 w, 2000 Hamburg 50, Telefon 89 39 45

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

vorgelegt im Januar 1992
(Redaktionsschluß: 6. Dezember 1991)
Dr. Hans-Hermann Schrader

herausgegeben vom Hamburgischen Datenschutzbeauftragten
Baumwall 7 · 2000 Hamburg 11 · Tel. 35 02 39 45

Druck: Lütcke & Wulf, Hamburg

INHALTSVERZEICHNIS

Vorwort

Nachdem mich die Bürgerschaft am 16. Januar 1991 auf Vorschlag des Senats zum neuen Hamburgischen Datenschutzbeauftragten für sechs Jahre gewählt hatte, habe ich mein Amt am 1. Februar 1991 angetreten. Den 10. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten lege ich hiermit zugleich als meinen ersten Bericht vor.

Dieser Bericht schließt an den 9. Tätigkeitsbericht an, der von dem damals amtierenden Hamburgischen Datenschutzbeauftragten Manfred Krause am 19. November 1990 dem Senat und der Bürgerschaft vorgelegt worden war. Danach war Herr Krause weiter für die Arbeit des Hamburgischen Datenschutzbeauftragten und seiner Mitarbeiter bis zu meinem Dienstantritt verantwortlich. Bei der Übernahme der Dienstgeschäfte kam mir seine langjährige Erfahrung im Datenschutz zugute. Für seinen Rat und seine Unterstützung danke ich ihm besonders.

Der neue Tätigkeitsbericht erscheint in einer geänderten äußeren Form. Durch das Buchformat, das zunehmend auch bei den Tätigkeitsberichten der anderen Landesdatenschutzbeauftragten verwendet wird, soll eine häufigere Benutzung dieser handlichen Ausgabe in der Praxis gefördert werden. Dazu dient auch die erstmalige Aufnahme eines Stichwortverzeichnisses am Ende des Berichts. Die äußere Aufmachung entspricht der 1991 begonnenen Schriftenreihe „Hamburger Datenschutzhefte".

Grundlage der Tätigkeit während des gesamten Berichtszeitraums ist das neue Hamburgische Datenschutzgesetz (HmbDSG), das am 1. August 1990 in Kraft getreten ist (siehe dazu 1.2.1). Zu den wesentlichen Arbeitsgrundlagen der Dienststelle, die auch für den nicht-öffentlichen Bereich zuständig ist, gehört außerdem das neue Bundesdatenschutzgesetz (BDSG), das am 1. Juni 1991 in Kraft getreten ist (siehe dazu 1.3).

Grundsatz für mein Datenschutzverständnis hinsichtlich der Stellung des Bürgers ist: „Soviel Freiheit wie möglich und soviel Bindung wie nötig." Entgegen der immer noch weit verbreiteten Auffassung, daß der Staat und die Wirtschaft im Interesse ihrer Handlungsfähigkeit über möglichst viele persönliche Daten verfügen sollten, gilt der Grundgedanke von Prof. Simitis: „Eine demokratische Gesellschaft sollte immer weniger wissen wollen, als sie wissen könnte."

Für die neunziger Jahre mit den neuen Risiken durch zunehmende Datenvernetzung könnten auf diese Weise die Datenschutzprobleme und ihre Lösungsansätze auf den Punkt gebracht werden. Die informationelle Selbstbestimmung des Bürgers kann sich nur bei einer informationellen Selbstbeschränkung von Verwaltung und Wirtschaft entfalten.

Die dafür geeigneten Instrumentarien sind in der Datenschutzgesetzgebung und -praxis verstärkt auszuarbeiten. Dazu wird insbesondere eine weitere Entwicklung des – vom Bundesverfassungsgericht wiederholt behandelten – Grundrechtschutzes durch Verfahren gehören, wobei sich Vorabprüfungen und begleitende Korrekturen neben der häufig zu späten Beanstandung positiv für den Datenschutz auswirken könnten.

Auf diese Fragen geht der vorliegende Tätigkeitsbericht ein. Eine angemessene Umsetzung kann nur erreicht werden, wenn Bürgerschaft, Senat, Verwaltung, Wirtschaft, die Medien und vor allem die Bürger selbst diese aktuellen Anliegen des Datenschutzes aufgreifen und sich zu eigen machen.

1. Zur Lage des Datenschutzes

1.1 Schwerpunkte Automationsvorhaben, Gesundheitsdaten, Personaldaten

Im Vordergrund der aktuellen Entwicklung steht die Ausweitung der automatisierten Datenverarbeitung. Bisherige manuelle Verfahren werden vielfach automatisiert. Bestehende automatisierte Verfahren werden integriert und zu flächendeckenden Anwendungen ausgebaut. Einzelplatzanlagen werden miteinander vernetzt, und zugleich werden zunehmend Telekommunikationsdienste eingesetzt.

Dies bedeutet nicht nur wesentliche quantitative, sondern auch erhebliche qualitative Veränderungen bei der Datenverarbeitung. Dabei stellt sich die grundsätzliche Frage, inwieweit die Regelungsinstrumente des Datenschutzrechts noch geeignet sind, diesem Automatisierungsprozeß und seinen Risiken Rechnung zu tragen.

Der Umgang mit modernen Informationsprozessen wird nicht nur durch die fachlichen Anforderungen in den einzelnen Bereichen der Verwaltung bestimmt, sondern gerade auch durch die zunehmende flächendeckende Automatisierung. Aus der damit verbundenen Möglichkeit, inhaltlich sensible Daten weit mehr als bisher in der Verwaltung und darüber hinaus technisch leicht austauschen zu können, ergeben sich neue Gefährdungen.

Die damit zusammenhängenden Fragen zur automatisierten Datenverarbeitung werden in Abschnitt 3 dieses Berichts grundsätzlich dargestellt. In den nachfolgenden Abschnitten über einzelne Bereiche werden jeweils an erster Stelle die Automationsvorhaben und deren Probleme behandelt. Damit wird dieser Schwerpunkt des Tätigkeitsberichts durchgängig hervorgehoben.

Als weitere Schwerpunkte sind – gemäß der Ankündigung bei meinem Dienstantritt – der Schutz der Gesundheitsdaten und der Schutz der Personaldaten behandelt worden. Darauf wird an den jeweiligen Stellen in diesem Bericht eingegangen, beginnend bei 1.5 hinsichtlich der Zusammenarbeit mit der Verwaltung.

1.2 Hamburgisches Datenschutzrecht

1.2.1 Hamburgisches Datenschutzgesetz

Zum neuen Hamburgischen Datenschutzgesetz gibt es schon jetzt Änderungsbedarf, weil die verschiedenen Verweisungen auf das bisherige Bundesdatenschutzgesetz nunmehr an das neue Bundesdatenschutzgesetz anzupassen sind. Außerdem haben sich bei der Anwendung des neuen Hamburgischen Datenschutzgesetzes einige klarstellungsbedürftige Punkte ergeben, z.B. hinsichtlich des Anwendungsbereichs für sog. öffentliche Unternehmen und der Meldepflicht zum Dateiregister für die Landesbetriebe.

Im Vergleich zu anderen neueren Landesdatenschutzgesetzen bietet es sich ferner an, einzelne Verbesserungen aufzugreifen. Dazu einige Beispiele: Die Maßnahmen der Datensicherung sollen sich nach dem jeweiligen Stand der Technik richten. Die Unterrichtung von Betroffenen bei Datenschutzverstößen soll geregelt werden.

Zur Rechtsstellung des Hamburgischen Datenschutzbeauftragten ist eine Ergänzung der bisherigen Regelung sachgerecht, mit der – wie in anderen Landesdatenschutzgesetzen – seine Funktion als Dienstvorgesetzter eindeutig festgelegt und eine Vertreterregelung eingefügt wird. Im übrigen soll die Regelung zur Rechtsaufsicht über den Hamburgischen Datenschutzbeauftragten nun endgültig entfallen, nachdem es eine solche Bestimmung in keinem anderen Landesdatenschutzgesetz mehr gibt. Schließlich könnte das Verfahren bei einer Beanstandung in verschiedenen Punkten klarer geregelt werden. Die Vorschläge zur Änderung des Hamburgischen Datenschutzgesetzes habe ich der Justizbehörde in mehreren Schreiben mitgeteilt.

1.2.2 Weitere gesetzliche Regelungen

Im Anschluß an das Volkszählungsurteil des Bundesverfassungsgerichts vom Dezember 1983 sind außer dem Hamburgischen Datenschutzgesetz mehrere hamburgische Gesetze im Jahre 1991 verabschiedet worden, die Rechtsgrundlagen für den Datenschutz enthalten. Hervorzuheben ist dabei das Hamburgische Gesetz zur Änderung des Gesetzes zum Schutz der öffentlichen Sicherheit und Ordnung und zur Sicherung des Datenschutzes bei der Polizei vom 2. Mai 1991. Neben der Änderung des SOG ist damit zugleich im neuen Gesetz über die Datenverarbeitung der Polizei erstmals im einzelnen geregelt, welche Befugnisse der Polizei bei der Datenverarbeitung zustehen.

Zu den schwerwiegenden datenschutzrechtlichen Problemen des neuen Polizeirechts kann auf die ausführliche Darstellung in den letzten beiden Tätigkeitsberichten verwiesen werden (8. TB., 3.8.1; 9. TB., 4.12.1). In der Schlußphase der Gesetzgebung konnten Verbesserungen nur noch begrenzt verwirklicht werden. Immerhin wurde im Gesetz klargestellt, daß die Behörde für Inneres mit ihren verschiedenen Bereichen außer der Polizei bei einem automatisierten Datenabruf nicht einfach als nur eine öffentliche Stelle gilt. Vielmehr sind die besonderen Schutzvorkehrungen nach dem Hamburgischen Datenschutzgesetz für den Datenabruf auch zwischen verschiedenen Stellen der Behörde für Inneres – z.B. zwischen Polizei und Verfassungsschutz – einzuhalten.

Mit der erreichten Rechtsklarheit in dem neuen Polizeirecht sind andererseits erhebliche Ausweitungen der polizeilichen Befugnisse gegenüber dem Bürger verbunden. Hier bestehen dieselben vielfältigen Probleme, die zusammen mit dem Gesetzentwurf des Bundes zur Bekämpfung der organisierten Kriminalität (OrgKG) erörtert werden. In beiden Fällen wird von den Datenschutzbeauftragten darauf hingewirkt werden, daß die Durchführung des neuen Polizeirechts verfassungskonform und restriktiv erfolgt. Insbesondere wird darauf geachtet

werden müssen, daß über die teilweise offen formulierten Begriffe der Zugriff auf die Daten der Bürger nicht noch weiter ausgedehnt wird. Die Problematik im einzelnen wird nachfolgend im Zusammenhang mit dem Entwurf des OrgKG behandelt (siehe 19.1.1).

Gemäß dem Bundesverfassungsgerichtsurteil von 1983 zum informationellen Selbstbestimmungsrecht sind zunehmend bereichsspezifische Regelungen zum Datenschutz von der Bürgerschaft getroffen worden. Sie sind insbesondere im Hamburgischen Archivgesetz vom 21. Januar 1991, im Hamburgischen Statistikgesetz vom 19. März 1991 und im Hamburgischen Krankenhausgesetz vom 17. April 1991 enthalten.

Im Rundfunkgesamtstaatsvertrag vom 31. August 1991 wird der Datenschutz teilweise erstmals festgelegt und teilweise fortgeschrieben für den privaten Rundfunk, das ZDF, die Rundfunkgebühren und den Bildschirmtext. Im neuen NDR-Staatsvertrag sind unter meiner Beteiligung die bisherigen Regelungen des Hamburgischen Datenschutzgesetzes übernommen und bereichsspezifisch fortentwickelt worden. Die neuen Datenschutzbestimmungen im ZDF- und im NDR- Staatsvertrag stimmen dabei sinnvollerweise weitgehend überein.

Weitere wesentliche Gesetzesvorhaben, wie die Neufassung des Hamburgischen Meldegesetzes, sind in Vorbereitung. Angekündigt, aber dem Senat noch nicht vorgelegt sind die bereichsspezifischen Gesetzentwürfe insbesondere im Schulbereich und für den hamburgischen Verfassungsschutz. Eine rechtzeitige Beteiligung des Hamburgischen Datenschutzbeauftragten über diese Gesetzesvorhaben ist gemäß den früheren Ersuchen der Bürgerschaft Voraussetzung dafür, daß die datenschutzrechtlichen Anforderungen sachgerecht berücksichtigt werden.

1.3 Neues Bundesdatenschutzgesetz

Das am 1. Juni 1991 in Kraft getretene Bundesdatenschutzgesetz ist Rechtsgrundlage für die Tätigkeit des Hamburgischen Datenschutzbeauftragten als Aufsichtsbehörde im nicht-öffentlichen Bereich. Die Novellierung hat zwar aus Sicht der Aufsichtsbehörde einige Verbesserungen gebracht. Der Datenschutz bleibt aber im nicht-öffentlichen Bereich deutlich hinter dem Datenschutz im öffentlichen Bereich zurück.

Das neue Bundesdatenschutzgesetz konkretisiert als Schutzziel nunmehr das Persönlichkeitsrecht. Der sachliche Anwendungsbereich wurde auf die Erhebung und Nutzung personenbezogener Daten ausgedehnt. Zur Verbesserung betriebsinterner Kontrollmechanismen wurde die Stellung des betrieblichen Datenschutzbeauftragten gestärkt. Seine Abberufung durch die nicht-öffentliche Stelle ist nur unter den Voraussetzungen für eine außerordentliche Kündigung – z. B. wegen vorsätzlich schlechter Arbeitsleistung – zulässig. Ihm sind von der speichernden Stelle im erforderlichen Umfang persönliche und sächliche Mittel sowie die Dateiübersicht zur Verfügung zu stellen. Die Straftatbe-

stände bei unbefugtem Umgang mit personenbezogenen Daten wurden erweitert. Beispielsweise sind jetzt die unbefugte Speicherung und die erschlichene Übermittlung strafbar.

Im Gegensatz zu den Regelungen für den öffentlichen Bereich wurde die Datenerhebung im nicht-öffentlichen Bereich aber nur ungenügend einbezogen und die Datenverarbeitung in Akten grundsätzlich gar nicht erfaßt. Die Aussage im Bundesdatenschutzgesetz, daß die Datenerhebung „nach Treu und Glauben und auf rechtmäßige Weise" erfolgen muß, ist zwar zutreffend; hier hätten jedoch nähere Anforderungen festgelegt werden sollen, wie dies vergleichbar für den öffentlichen Bereich geschehen ist. Die Unterscheidung zwischen Datenschutz in Dateien und in Akten führt außerdem dazu, daß die wenig sinnvolle und praktisch schwierige Abgrenzung zwischen diesen Bereichen beibehalten werden muß.

Bei der neu aufgenommenen Zweckbindung übermittelter Daten bleibt der Gesetzeswortlaut hinter den Einschränkungen in der Datenschutzkonvention des Europarats zurück, die durch die Ratifizierung im Jahr 1985 in der Bundesrepublik Deutschland verbindliches Recht wurde (Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 – Konvention 108 –). Durch die weitreichenden Ausnahmen von der Zweckbindung erscheinen Zweckänderungen in gleicher Weise möglich wie bei der Verarbeitung und Nutzung ohne vorangegangene Übermittlung.

Verbesserungen für die Aufsichtsbehörde liegen andererseits darin, daß sie zu einer Überprüfung bereits berechtigt ist, wenn bei einer Datenverarbeitung für eigene Zwecke hinreichende Anhaltspunkte für Datenschutzverstöße vorliegen; einer ausdrücklichen Beschwerde eines Betroffenen bedarf es nicht mehr. Anhand ihrer Prüfungsergebnisse kann sie dann Maßnahmen zur Beseitigung technischer und organisatorischer Mängel anordnen und sogar den Einsatz einzelner Verfahren untersagen. Sie kann die Abberufung eines betrieblichen Datenschutzbeauftragten verlangen, wenn dieser nicht über die erforderliche Fachkunde und Zuverlässigkeit verfügt.

Voraussetzung dafür ist allerdings, daß die Unternehmen gemäß ihrer gesetzlichen Verpflichtung – bei mindestens 5 Arbeitnehmern für automatisierte Datenverarbeitung oder mindestens 20 Arbeitnehmern für nicht-automatisierte Datenverarbeitung – einen betrieblichen Datenschutzbeauftragten bestellen. Bei über 80.000 Betrieben in Hamburg müßte es eigentlich einige Tausend betriebliche Datenschutzbeauftragte geben. Da dies bisher nicht bekannt ist, spricht viel dafür, daß zahlreiche Betriebe dieser gesetzlichen Verpflichtung noch nicht nachgekommen sind, obwohl dies eine Ordnungswidrigkeit ist.

Wie bereits im letzten Tätigkeitsbericht hervorgehoben wurde, greift das Gesetz mit der Regelung in § 24 Abs. 6 BDSG in die Kontrollbefugnisse der Landesdatenschutzbeauftragten ein. Eine derartige Regelung ist mit der verfassungsrechtlichen Kompetenzverteilung zwischen Bund und Ländern unvereinbar (9. TB., 1.2). Ich habe daher die Justizbehörde gebeten, in Abstimmung mit den anderen Ländern die Durchführung eines Normenkontrollverfahrens vor dem Bundesverfassungsgericht zu klären.

Die nordwestdeutschen Landesdatenschutzbeauftragten haben am 3. Juni 1991 eine gemeinsame Erklärung gegen den Eingriff in die Rechte der Landesdatenschutzbeauftragten abgegeben, die der Justizbehörde zur Kenntnis gegeben wurde. Auf der Datenschutzkonferenz am 26./27. September 1991 bestand zwischen den Landesdatenschutzbeauftragten Einvernehmen, daß dem Bund die Kompetenz fehlt, die Kontrollrechte der Landesdatenschutzbeauftragten durch § 24 Abs. 6 BDSG einzuschränken.

Im Hinblick darauf, daß nach § 24 Abs. 2 BDSG die Betroffenen in allgemeiner Form über das ihnen zustehende Widerspruchsrecht zu unterrichten sind, haben sich außerdem die Bundes- und Landesdatenschutzbeauftragten auf dieser Konferenz darüber verständigt, nach welchen Grundsätzen sie bei der Anwendung und Auslegung dieser Vorschriften verfahren werden. Diese Grundsätze sollen – soweit erforderlich – in einer Bekanntmachung im Amtlichen Anzeiger zum Widerspruchsrecht der hamburgischen Beschäftigten im Öffentlichen Dienst wiedergegeben werden.

1.4 Verhältnis zum Bürger

1.4.1 Öffentlichkeitsarbeit

Die gesamte Tätigkeit des Hamburgischen Datenschutzbeauftragten und der Mitarbeiter steht im Dienste des Bürgers. In § 1 HmbDSG wird die „Aufgabe des Datenschutzes" damit umschrieben, „das Recht des einzelnen zu schützen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen".

Für die Tätigkeit des Datenschutzbeauftragten ist es daher wichtig, dem Bürger wesentliche Themen ständig zu vermitteln und ihm damit die Wahrung seiner Rechte zu erleichtern. Erste Voraussetzung ist dafür, daß der Bürger seine Rechte kennt. Die Broschüre „Das neue Datenschutzrecht" war dazu als Informationsschrift über das neue Hamburgische Datenschutzgesetz und das neue Bundesdatenschutzgesetz gemeinsam mit der Justizbehörde vorbereitet worden (9. TB., 1.1). Für ein breiteres Verständnis bei den Bürgern genügen allerdings die abstrakten Gesetzestexte nicht. Deshalb wurden in diese Broschüre ausführliche Erläuterungen zum Hamburgischen Datenschutzgesetz mit der ergänzten amtlichen Begründung aufgenommen.

Zur Unterrichtung der Bürger sind nicht nur Informationen über das Datenschutzrecht notwendig, sondern gerade auch Berichte über die technische Entwicklung. Entsprechend dem Schwerpunkt Automationsvorhaben ist daher am 30. September 1991 als zweite Broschüre in der Reihe der Hamburger Datenschutzhefte eine Informationsschrift „Datenschutzkonzept für PC – Einzelplatzsysteme, Lokale Netze, PC-Host-Kopplung – " veröffentlicht worden.

Damit wird der gesetzlichen Aufgabe des Hamburgischen Datenschutzbeauftragten Rechnung getragen, Empfehlungen zur Verbesserung des Datenschutzes zu geben und zu den Auswirkungen der Nutzung neuer Informations- und Kommunikationstechniken auf den Datenschutz Stellung zu nehmen. Das im letzten Tätigkeitsbericht vorgestellte Datensicherungskonzept bei Einzelplatz-PC (9. TB., 3.2) wurde in die vorliegende Broschüre aufgenommen. Ergänzend wurde auf die zunehmend wichtige Verknüpfung von PC zu Lokalen Netzen und auf den Anschluß von PC an Großrechner eingegangen.

Seit meinem Dienstantritt werden außerdem in Gesprächen, die vierteljährlich in der Dienststelle mit Vertretern von Presse und Rundfunk stattfinden, aktuelle Datenschutzfragen bekanntgemacht. Darüber hinaus wurden wiederholt bürgerrelevante Themen in Presseerklärungen an die Öffentlichkeit herangebracht. Dabei ging es zum Beispiel aus unterschiedlichen Anlässen mehrfach um den Telefondatenschutz, der die Bürger besonders berührt.

Zur Öffentlichkeitsarbeit gehört schließlich der Beginn einer Vortragsreihe über Datenschutzfragen, in der Referenten über aktuelle Datenschutzthemen jeweils zunächst ein internes Gespräch in der Dienststelle des Hamburgischen Datenschutzbeauftragten mit den Mitarbeitern führen und danach einen öffentlich zugänglichen Vortrag halten. Den Anfang machte ein Vortrag von Prof. Lutterbeck am 14. November 1991 über „Datenverarbeitung außer Kontrolle? – Perspektiven des Datenschutzrechts und der Datenschutztechnik –".

Von verschiedenen Seiten wurde ich gebeten, Vorträge zu Datenschutzfragen zu halten. Daraufhin habe ich mehrfach über das neue Bundesdatenschutzgesetz eingehend informiert und bei anderen Anlässen bereichsspezifische Datenschutzprobleme insbesondere zum Personaldaten- und Gesundheitsdatenschutz behandelt.

1.4.2 Eingaben

Täglich wenden sich Bürger mit schriftlichen Eingaben, mit telefonischen Anfragen und bei persönlichen Besuchen an die Dienststelle des Hamburgischen Datenschutzbeauftragten. Dies zeigt das Problembewußtsein für Datenschutzfragen in der Bevölkerung. Nach Abstimmung mit den beteiligten öffentlichen und nicht-öffentlichen Stellen wird jeweils versucht, in möglichst kurzer Zeit die Eingaben zu beantworten. Bis Ende November 1991 gingen 294 schriftliche Eingaben ein. Sie betrafen folgende Themen:

Öffentlicher Bereich	168
davon Sicherheitsbereich	45
Gesundheits- und Sozialbereich	47
übrige Bereiche	76
Nicht-öffentlicher Bereich	126
davon Versandhandel	6
Versicherungswirtschaft	28
Kreditwirtschaft	9
Werbung	5
Arbeitnehmer-Datenschutz	10
SCHUFA und Auskunfteien	18
Gesundheitswesen	9
Sonstige	41

Zusätzlich wurden ab April 1991 im zweimonatigen Abstand Bürgergespräche in der Dienststelle des Hamburgischen Datenschutzbeauftragten angeboten und öffentlich bekanntgegeben. Damit sollte Bürgern sowie Vertretern von Gruppen und Organisationen die Möglichkeit gegeben werden, in Einzelgesprächen ihre Sorgen und Vorschläge einzubringen. Die Themen bei den ersten beiden Bürgergesprächen waren der Datenschutz im Gesundheitsbereich und dann der Datenschutz für Arbeitnehmer. Die folgenden Gespräche bezogen sich einerseits auf den Datenschutz in der Verwaltung und andererseits auf den Datenschutz in der Wirtschaft.

Bisher ist die Resonanz auf dieses zusätzliche Angebot verhältnismäßig gering geblieben. Dies erklärt sich vermutlich daraus, daß die Bürger nicht auf feste Termine für ihre Anliegen warten wollen, sondern jeweils nach Bedarf unmittelbar ihre datenschutzrechtlichen Probleme mitteilen. Gleichwohl soll auch dieses Angebot – allerdings ohne Themenvorgabe – als Bürgersprechstunde zu Datenschutzfragen fortgeführt werden.

1.5 Zusammenarbeit mit der Verwaltung

Zu Beginn meiner Tätigkeit hatte ich betont, daß es mir im Zusammenwirken mit den Behörden um einen konstruktiven Datenschutz geht. Dem informationellen Selbstbestimmungsrecht des Bürgers dient es am meisten, wenn in seinem Interesse Fortschritte bei der Durchsetzung des Datenschutzes zusammen mit den Behörden erreicht werden und Beanstandungen auf unvermeidbare Fälle begrenzt bleiben.

In einem ersten Rundschreiben vom März 1991 an die Senatsämter und Fachbehörden zur Zusammenarbeit mit dem Hamburgischen Datenschutzbeauftragten wies ich darauf hin, daß Voraussetzung für meine Aufgabenwahrnehmung eine frühzeitige und umfassende Unterrichtung durch die Behörden in allen datenschutzrelevanten Angelegenheiten ist. Dazu erinnerte ich an die Beschlußlage gemäß den Ersuchen der Bürgerschaft, den Beschlüssen des Senats und den Ergebnissen der Staatsrätebesprechungen, die eine derartige frühzeitige und umfassende Unterrichtung gewährleisten sollen.

In diesem Sinne habe ich mich insbesondere dafür eingesetzt, daß künftig formale Beanstandungen nur deshalb, weil Behörden nicht rechtzeitig zu anhängigen Datenschutzfragen Stellung genommen haben, möglichst vermieden werden. Es ist erfreulicherweise gelungen, in mehreren Fällen durch direkte Gespräche mit den Behördenleitungen die Abgabe noch ausstehender Stel-

lungnahmen und Entwürfe zu erreichen. Zur zügigen Bearbeitung soll auch die ausdrückliche Aufforderung in meinem Rundschreiben beitragen, daß die Behörden ggf. durch qualifizierte Zwischenbescheide jedenfalls über den weiteren vorgesehenen Ablauf berichten.

Die Behörden haben wiederholt erwähnt, daß sie für die neuen Aufgaben im Datenschutz meistens keine personelle Verstärkung erhalten haben. Diesen Schwierigkeiten kann nur abgeholfen werden, wenn die Stellenanträge der Behörden im Datenschutzbereich künftig im erforderlichen Umfang berücksichtigt werden. Jedoch kann es nicht angehen, daß Behörden unter Hinweis auf ihre anderen Pflichtaufgaben die Beantwortung datenschutzrechtlicher Fragen immer wieder in Zwischenbescheiden zurückstellen. Der Datenschutz ist nun einmal eine gesetzlich festgelegte Aufgabe, die gerade wegen ihrer Grundrechtsrelevanz von den Behörden nicht nachrangig behandelt werden kann.

In einem weiteren Rundschreiben an die Senatsämter und Fachbehörden im August 1991 habe ich ergänzend darum gebeten, mir wichtige datenschutzrechtliche Vorhaben mit Regelungsbedarf durch Gesetz, Verordnung oder Anordnung sowie wichtige Einzelfälle bis Mitte September mitzuteilen. Diese Bitte ist zurückhaltend aufgenommen worden, weil befürchtet wurde, daß dies zu einer Ausforschung von Vorentwürfen der Behörden führen könnte. Ich habe daraufhin klargestellt, daß es mir lediglich im Sinne der Beschlußlage von Senat und Bürgerschaft um die Unterrichtung über mitteilungsreife Vorhaben geht. Dies entspricht meinem gesetzlich vorgegebenen Ansatz, möglichst rechtzeitig datenschutzrechtliche Fragen gemeinsam zu klären und nicht erst nachträglich mit oft größerem Aufwand bereits aufgetretene Mängel zu beseitigen.

Der frühzeitigen Beratung dient auch meine Mitwirkung in mehreren Projekten der Verwaltung. Intensive Beratungen ermöglichten es mir, offene Fragen im Projekt Sozialhilfe-Automation (PROSA) und im Projekt Personalwesen – mit dem Ziel einer weitgehenden Automatisierung der Personalverwaltung – zeitgerecht zu klären. Positiv haben sich auch die Beratungen im Projekt COMVOR – über computerunterstützte Vorgangsbearbeitung bei der Polizei – ausgewirkt. Dies sind Beispiele für eine sachgerechte Zusammenarbeit der Behörden mit dem Hamburgischen Datenschutzbeauftragten.

In weiteren Projekten und Arbeitsgruppen der Verwaltung wirken die jeweils zuständigen Mitarbeiter mit. Zu erwähnen sind hier das Projekt Automation Ausländerwesen, das Bildschirm-Dialogverfahren für die Bearbeitung von Verkehrsordnungswidrigkeiten (OWID), das Projekt Automation Kraftfahrzeug-Zulassungswesen (PAKZU), das Projekt Automation Standesämter (PASTA), das Projekt Kassen- und Rechnungswesenautomation (PROKURA), der Statistische Landesausschuß und weitere Lenkungsgruppen im Statistik-Bereich, die Projektgruppe DVZ-Verlagerung sowie mehrere Arbeitskreise und Arbeitsgruppen im IuK-Bereich.

Gegenüber der Verwaltung habe ich im Bereich der Gesundheitsdaten mit Nachdruck dafür gesorgt, daß die seit längerem angekündigte Dienstanweisung für das Universitätskrankenhaus Eppendorf bis Mitte 1991 endlich fertiggestellt wurde. Mit der Behörde für Arbeit, Gesundheit und Soziales wurden die offenen Punkte – insbesondere die überfällige Dienstanweisung für den Landesbetrieb Krankenhäuser – eingehend erörtert.

Zum Themenbereich Personaldaten ist vor allem auf die Mitarbeit in der Lenkungsgruppe des bereits erwähnten Projekts Personalwesen hinzuweisen. Nach intensiven Vorarbeiten faßten außerdem die Datenschutzbeauftragten des Bundes und der Länder Ende September 1991 eine ausführliche Entschließung zum „Datenschutz im Recht des öffentlichen Dienstes", die ich dem Senatsamt für den Verwaltungsdienst zugeleitet habe.

Insgesamt hat sich nach meinem bisherigen Eindruck die Bereitschaft der Verwaltung zur Zusammenarbeit verbessert. Mehrfach wurde deutlich, daß die Verwaltung selbst daran interessiert ist, bei datenschutzrechtlich schwierigen Vorhaben frühzeitig eine Klärung zu erreichen. Die Vertretbarkeit solcher Vorhaben nach außen und damit auch die Akzeptanz gegenüber dem Bürger kann auf diese Weise nach eigener Einschätzung der Verwaltung stärker abgesichert werden. In Einzelfällen erfolgte allerdings die Abstimmung bei Senatsdrucksachenentwürfen nicht rechtzeitig.

Schwerwiegende datenschutzrechtliche Verstöße habe ich Ende September 1991 bei dem Fehlbelegungsabgabe-Verfahren der Mietenausgleichszentrale als einer Abteilung der Hamburgischen Wohnungsbaukreditanstalt beanstandet (siehe 12.1). In einem langwierigen Verfahren mußte vorher mit Unterstützung des Senats und der beteiligten Behörden erst einmal durchgesetzt werden, daß die datenschutzrechtliche Prüfung in diesem Bereich überhaupt durchgeführt werden konnte.

Meine grundsätzliche Einstellung werde ich beibehalten: Gerade für den Datenschutz ist Vorbeugen besser als Heilen, weil die möglichst frühe und konstruktive Klärung datenschutzrechtlicher Fragen allen Beteiligten zugute kommt.

1.6 Verbindung zu den neuen Ländern

Die deutsche Einheit führte auch im Datenschutz zu grundlegenden Änderungen. An der Konferenz der Datenschutzbeauftragten des Bundes und der Länder nahmen die Vertreter der neuen Länder zunächst als Gäste teil. Im Einigungsvertrag ist festgelegt, daß das Bundesdatenschutzgesetz mit bestimmten Maßgaben auch für den öffentlichen Bereich der neuen Länder gilt, bis dort Landesdatenschutzgesetze verabschiedet sind. Bis zu einer eigenen Datenschutzkontrolle, längstens bis zum 31. Dezember 1991, übt der Bundesbeauftragte für den Datenschutz die Kontrolle für die neuen Länder aus.

Den für den Datenschutz in Mecklenburg-Vorpommern zuständigen Kollegen habe ich frühzeitig mit Informationen und Materialien unterstützt. Bereits im

April 1991 wurden bei einem Besuch der Dienststelle des Hamburgischen Datenschutzbeauftragten in Schwerin mit ihm Gespräche geführt. Im September und Oktober 1991 habe ich mich an Datenschutzseminaren in Schwerin beteiligt.

1.7 Europäisches Datenschutzrecht

Im Hinblick auf die Vollendung des EG-Binnenmarktes bis zum 1. Januar 1993 hat die Kommission der Europäischen Gemeinschaften am 27. Juli 1990 einen „Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" vorgelegt.

Die für eine fristgerechte Annahme der Richtlinie durch den Rat und die fristgerechte Umsetzung in nationale Rechtsvorschriften verbleibende Zeit ist für eine vorherige Diskussion des Entwurfs durch die Mitgliedsstaaten sehr knapp. Die Datenschutzbeauftragten des Bundes und der Länder haben auf der Sonderkonferenz am 29. Januar 1991 eine Stellungnahme beschlossen und auf ihrer Konferenz am 26./27. September 1991 bekräftigt, daß sie eine datenschutzgerechte Richtlinie auf möglichst hohem Niveau gemäß dem Entwurf der EG-Kommission grundsätzlich befürworten. Die Stellungnahme des Rechtsausschusses des Europäischen Parlaments wird um die Jahreswende 1991/92 erwartet.

Der Binnenmarkt wird einen zwischenstaatlichen Austausch personenbezogener Daten, insbesondere im nicht-öffentlichen Bereich, in erheblichem Umfang mit sich bringen. Das Datenschutzniveau in den Mitgliedsstaaten ist allerdings sehr unterschiedlich (vgl. bereits 8. TB, 4.5.5). Die Vereinbarung sogenannter „Vertragsmodelle", wonach bei Datenübermittlung in Staaten ohne Datenschutzgesetze oder in Länder mit niedrigem Datenschutzniveau der dortige Datenempfänger vertraglich durch die deutsche übermittelnde Stelle auf die Einhaltung des deutschen Datenschutzrechts verpflichtet wird, erscheint insbesondere im Hinblick auf fehlende Kontrollrechte unzureichend (vgl. 9. TB, 5.2.1.1 und 5.4.2) und allenfalls als Übergangslösung vertretbar.

Von deutscher Seite wird die Einbeziehung der Datenerhebung in den Anwendungsbereich der Richtlinie angestrebt. Dies sieht auch die Stellungnahme des Wirtschafts- und Sozialausschusses der EG vom 24. April 1991 vor. Der Beschluß der Datenschutzbeauftragten vom 29. Januar 1991 fordert, daß der Datenschutz, jedenfalls im Bereich der öffentlichen Verwaltung, für alle Unterlagen mit personenbezogenen Daten gelten muß, mithin auch für Akten.

Aus unserer Sicht ist es ferner wünschenswert, daß in Art. 9 des Entwurfs eine Benachrichtigungspflicht bereits im Zeitpunkt der erstmaligen Speicherung und nicht erst bei erstmaliger Übermittlung oder Ermöglichung des Datenabrufs vorgesehen wird.

Der Beschluß der Datenschutzbeauftragten vom 29. Januar 1991 fordert außerdem eine strikte Zweckbindung für die Verwendung und Weitergabe persönlicher Daten anstelle der in Art. 16 Nr. 1 Bst. b des Entwurfs vorgesehenen bloßen Vereinbarkeit der Zwecke der Erhebung, Speicherung und Übermittlung.

Hinsichtlich der Regelung des Richtlinienentwurfs über den Datenexport in Drittländer in Art. 24 des Kommissionsentwurfs bedauern die Datenschutzbeauftragten in ihrer Stellungnahme, daß für die Zulässigkeit der Datenübermittlung ein lediglich angemessenes Schutzniveau des Drittlandes vorgesehen ist. Sie erwarten, daß in dem Empfängerland ein dem EG-Standard gleichwertiges Datenschutzniveau bestehen muß. Die gleiche Kritik übt auch der Wirtschafts- und Sozialausschuß in seiner Stellungnahme. Es dürfte zudem nicht mit den nationalen Kompetenzen der Mitgliedsstaaten vereinbar sein, wenn die Kommission gemäß Art. 25 des Entwurfs die Erteilung einer ausnahmsweisen Erlaubnis eines Datenexports untersagen darf.

Der Richtlinienentwurf sieht in Art. 2 Bst. f und Art. 26 vor, daß in jedem Mitgliedsstaat eine unabhängige Kontrollbehörde mit Untersuchungs- und Eingriffsbefugnissen eingerichtet wird. Von deutscher Seite wird eine flexiblere Regelung angestrebt, weil zum einen nach dem BDSG und den Landesdatenschutzgesetzen bereits Kontrollbehörden bestehen und für eine Änderung dieser bewährten Praxis kein Anlaß besteht. Zum anderen ist die Aufnahme des Gebots der Unabhängigkeit der Datenschutzkontrollbehörde hinsichtlich des nicht-öffentlichen Bereichs nach unserem Rechtssystem nicht möglich, weil im Bereich der Eingriffsverwaltung das Prinzip der parlamentarischen Verantwortlichkeit gilt.

Die Datenschutzbeauftragten begrüßen in ihrem Beschluß vom 29. Januar 1991, daß der Entwurf versucht, den Datenschutz in der EG auf einem möglichst hohen Niveau zu harmonisieren. Bei der Diskussion des Richtlinienentwurfs auf EG-Ebene sollte von deutscher Seite besonders darauf hingewirkt werden, daß der Standard des vorgelegten Entwurfs nicht abgesenkt wird. Seitens einiger Mitgliedsstaaten sind Bestrebungen erkennbar, die in der Richtlinie vorgesehenen Rahmenbestimmungen auf wenige Grundsätze zu beschränken und Einzelheiten dem nationalen Gesetzgeber zu überlassen. Einige Mitgliedsstaaten wenden sich ferner gegen die Unterscheidung zwischen öffentlichem und nicht-öffentlichem Bereich datenverarbeitender Stellen.

2. Entwicklung der Dienststelle

2.1 Personelle Ausstattung

Nach den personellen Veränderungen im Jahre 1990 (9. TB., 2.1) haben weitere Mitarbeiter, die hier zum Teil langjährig für den Datenschutz tätig waren, neue Aufgaben in der Verwaltung und in der Justiz übernommen. Während sie dort zum Verständnis für den Datenschutz beitragen, setzen sich die neuen Mitarbeiter nach kurzer Einarbeitungszeit aktiv für die Belange des Datenschutzes ein.

An dieser Stelle ist auf die derzeitige ungenügende Vertreterregelung im Hamburgischen Datenschutzgesetz hinzuweisen. Als Mitte 1990 die Bestellung eines Vertreters anstand, sind zwischen dem Ausscheiden des früheren Hamburgischen Datenschutzbeauftragten und der Senatsentscheidung über die Vertreterbestellung immerhin 3 Wochen vergangen. In diesem Zeitraum war es zumindest rechtlich zweifelhaft, ob der bis dahin nur dienststelleninterne Vertreter datenschutzrechtliche Entscheidungen treffen konnte, die vom Gesetz dem Hamburgischen Datenschutzbeauftragten persönlich vorbehalten sind. Der Hamburgische Datenschutzbeauftragte muß nach seinem gesetzlichen Auftrag stets handlungsfähig sein, so daß eine gesetzliche Vertreterregelung wie in anderen Landesdatenschutzgesetzen geboten ist.

2.2 Geschäftsverteilung

In der Dienststelle des Hamburgischen Datenschutzbeauftragten wurde die Geschäftsverteilung aktualisiert. Um den Ansprechpartnern im öffentlichen und im nicht-öffentlichen Bereich den unmittelbaren Kontakt mit den zuständigen Mitarbeitern in der Dienststelle zu erleichtern, ist am Ende dieses Tätigkeitsberichts die Geschäftsverteilung im einzelnen wiedergegeben.

Hinsichtlich der Aufgabenverteilung und auch der Erreichbarkeit der Mitarbeiter ist zu berücksichtigen, daß sechs der 17 Mitarbeiter teilzeitbeschäftigt sind. Der Frauenanteil ist mit 40 % der Gesamtzahl der Mitarbeiter und zugleich 40 % der Mitarbeiter im höheren Dienst beispielhaft groß.

2.3 Aufgabenerweiterung

Durch die deutsche Einheit hat sich der Abstimmungsbedarf mit Einbeziehung der neuen Länder deutlich erhöht. Für die Dienststelle des Hamburgischen Datenschutzbeauftragten, der im öffentlichen Bereich den Vorsitz im Arbeitskreis Sicherheit und im nicht-öffentlichen Bereich in der Arbeitsgruppe Versicherungswirtschaft hat, wirkt sich dies besonders aus.

Eine erfolgversprechende Tätigkeit im Datenschutz ist nur bei ständiger Abstimmung zwischen den Datenschutzbeauftragten des Bundes und der Länder und den Aufsichtsbehörden im nicht-öffentlichen Bereich möglich. Der Arbeitskreis Sicherheit mit der Zuständigkeit insbesondere für die Datenschutzprobleme bei der Polizei hat mehrfach in Hamburg getagt und Entschließungen der Datenschutzbeauftragten vorbereitet. Die Arbeitsgruppe Versicherungswirtschaft ist mit den Auswirkungen auf alle Bürger gerade für Hamburg als wichtigsten Versicherungsplatz von Bedeutung. Die Mehrarbeit durch die deutsche Einheit soll ohne Stellenvermehrung mitgeleistet werden.

Die Aufgaben im nicht-öffentlichen Bereich können jedoch – erst recht nach der Aufgabenerweiterung durch das neue Bundesdatenschutzgesetz (9. TB., 2.2) – nicht angemessen erfüllt werden. Die Dienststelle verfügt bei insgesamt 13 Stellen bisher für den gesamten nicht-öffentlichen Bereich über 1 1/2 Stellen

im höheren Dienst und 1 1/2 Stellen im gehobenen Dienst. Damit ist sie außerstande, eine hinreichende Aufsicht in diesem Bereich mit über 80.000 Betrieben wahrzunehmen. Für 1992 ist deshalb an einer neuen Stelle Regierungsrat A 13 für diesen Bereich festgehalten worden. Nach eingehender Auseinandersetzung hinsichtlich der Aufgaben- und Bedarfssituation ist diese Stelle schließlich in den Stellenplanentwurf 1992 aufgenommen worden.

3. Automatisierte Datenverarbeitung

Die Informationstechnik entwickelt sich mit höherer Geschwindigkeit als „alte" Techniken. In den letzten 30 Jahren hat sie sowohl die Produktion als auch die Büroarbeit grundlegend verändert:

— Miniaturisierung: Während die Aufzeichnungsdichte und die Verarbeitungsgeschwindigkeit exponentiell zunehmen, werden die Speichermedien und DV-Anlagen immer kleiner. Neben und anstelle der papiermäßigen Aufzeichnung tritt die elektronische Speicherung von Daten.

— „Echtzeit"-Verarbeitung: Auf die jeweiligen aktuellen Datenbestände kann praktisch ohne zeitliche Verzögerung zugegriffen werden.

— Daten- und Funktionsintegration: Datenbestände, ihre Relationen und die Methoden ihrer Auswertung werden in integrierten Systemen zusammengefaßt und können multifunktional erschlossen und miteinander verknüpft werden.

— Vernetzung: Lokale Netzwerke und Telekommunikationsdienste ermöglichen den Zugriff auf Daten unabhängig vom Ort der Speicherung.

— Neue Erfassungssysteme: Neben die konventionelle Datenerfassung mittels Tastatur treten optische und akustische Verfahren der Datenerhebung.

— Künstliche Intelligenz: Datenverarbeitung beschränkt sich nicht mehr auf Dateien, die nach bestimmten Merkmalen geordnet sind. „Intelligente" Systeme erleichtern zunehmend die Überwachung des gesprochenen Wortes, die Bildauswertung und die inhaltliche Erschließung unstrukturierter Informationen.

Inzwischen ist unbestritten, daß die Sammlung und Verteilung von Informationen von entscheidender Bedeutung für die Funktionsweise und Leistungsfähigkeit von Unternehmen und Verwaltungen ist. Die Technisierung des Informationsflusses wirkt sich nicht allein auf die Effizienz der jeweiligen Organisation aus; sie verändert auch ihre internen Strukturen und ihre Außenbeziehungen. So wird in weiten Bereichen die Arbeitsteilung zwischen EDV-Spezialisten und Benutzern in Frage gestellt.

Diese Entwicklung läuft zur Zeit mit großer Intensität in der Büroautomation und hat entsprechende Folgen für den Datenschutz.

Büroautomation war ursprünglich reine Textverarbeitung. Angesichts der hohen Kosten wurden automatisierte Textsysteme zunächst in zentralen

Schreibbüros installiert. Durch funktionalere Textverarbeitungsprogramme wurde es bald möglich, Adressen zu verwalten und Anschriften automatisiert in Texte einzufügen. Zudem verdrängten Allzweck-Computer zunehmend die nur für Zwecke der Textverarbeitung tauglichen Systeme. Die gleichzeitig stark sinkenden Computerpreise machten es möglich, auch die Sachbearbeiter selbst mit entsprechenden „persönlichen Computern" (PC) auszustatten und ihnen damit nicht nur die Textverarbeitung am Arbeitsplatz, sondern auch (mittels Standardsoftware) eigene Datenverarbeitung zu ermöglichen.

Mit der lokalen Vernetzung dieser Systeme und ihrer Anbindung an Großrechner (vgl. 3.5) sowie ihrer Einbindung in Telekommunikationsnetze (z.B. ISDN) wachsen die zunächst inselhaft betriebenen Anwendungen zu komplexen und nur noch schwer steuerbaren Strukturen zusammen.

3.1 Risiken der Automatisierung

Automatisierte Datenverarbeitung stärkt die Steuerungskapazität und zugleich die Kontrollfunktionen von Großorganisationen. Solche Machtverschiebungen lassen sich bereits heute im Bereich etwa des Verhältnisses zwischen Verwaltungen und Bürgern, Arbeitgebern und Arbeitnehmern feststellen.

Die Risiken moderner Informationssysteme bestehen darin, daß eines oder mehrere ihrer Elemente (Daten oder Programme) oder Relationen (Umweltbeziehungen, Multifunktionalität) oder sogar das System als Ganzes vielfach „gefahrgeneigt" sein können. Diese Gefahren ergeben sich tendenziell daraus, daß mit der Datenverarbeitung das Verhalten der Bürger insgesamt oder z. B. der Beschäftigten immer transparenter wird.

„Gefahrgeneigt" wird die Ausgestaltung der Datenverarbeitung dabei immer dann, wenn sie die Freiheit des Betroffenen verringert, sich für ein bestimmtes Verhalten in der einen oder anderen Richtung zu entscheiden. Diese Freiheitsbeschränkung wird von der jeweiligen Großorganisation, die für die Datenverarbeitung verantwortlich ist, oftmals in Kauf genommen, ohne daß vermeidbare Mängel abgestellt werden:

— So hebt der Einsatz optischer Speicherungstechniken bei der Archivierung von Aktenmaterial die Datenverarbeitung auf eine neue Stufe. Zum einen wird dem „Zwang des knappen Raumes" zur Löschung der Datenbestände entgangen; das Eigeninteresse der Verwaltung an der Reduktion der Aktenmenge tritt in den Hintergrund. Zum anderen ist der Datenbestand nunmehr automatisiert auszuwerten; aus den Akten sind Dateien geworden. Erweiterte Auswertungs- und Verknüpfungsmöglichkeiten erleichtern die Zweckdurchbrechung und greifen mithin in das informationelle Selbstbestimmungsrecht ein. So könnten Daten der Telefonkunden, die aus herkömmlichen Telefonbüchern in elektronische, auf CD-ROM geführte Teilnehmerverzeichnisse übernommen wurden, als bundesweite Adreßregister gebraucht werden (vgl. 4.4), ohne daß melderechtliche Restriktionen beachtet würden.

— Die bei der Digitalisierung der Telekommunikation (vor allem im ISDN) entstehenden Verbindungsdaten ermöglichen es nachzuvollziehen, wer wann mit wem telefoniert hat; diese „Kommunikationsspuren" lassen sich automatisiert auswerten und zu Profilen verdichten (vgl. 4).

— Mit der Elektronisierung des Zahlungsverkehrs wird das Verbraucherverhalten zunehmend kontrollierbar; jede Abhebung von Bargeld beim Bankautomaten, jede Zahlung mittels Scheckkarte im EC-Cash und jede Benutzung von Kreditkarten führen an verschiedenen Stellen zur Speicherung von auswertbaren und verknüpfbaren Daten.

— Vorgangsverwaltungssysteme, die auch zur Wiederauffindung der jeweiligen Akten bestimmt sind, halten die vielfältigen Kontakte zwischen Verwaltung und Bürger fest. Diese Systeme führen – insbesondere wenn sie miteinander vernetzt sind – zu schwer überschaubaren Auswertungsmöglichkeiten. Sie bergen in sich das Risiko, daß die Einschränkungen bei der jeweiligen Verwaltungstätigkeit mit den dafür geltenden Zugriffsbegrenzungen und Löschungsfristen umgangen werden könnten.

— Der Einsatz von Computertechnik am Arbeitsplatz führt – schon aus Datenschutzgründen – zu umfangreichen Protokollierungen der Benutzeraktivitäten. Diese Systemprotokolle unterliegen selbst erheblichen Mißbrauchsrisiken.

Das Datenschutzrecht versucht, den technischen Herausforderungen zu begegnen, indem es materielle Zulässigkeitsanforderungen für die Datenverarbeitung aufstellt. Technische und organisatorische Maßnahmen (Datensicherung) sollen diese Anforderungen flankieren (§ 8 HmbDSG, § 9 BDSG). Angesichts der beschriebenen technischen Entwicklungen und der damit verbundenen Risiken ist zu fragen, ob dieser Ansatz erweitert werden muß.

3.2 Defizite des herkömmlichen Datenschutzrechts

Will man die Struktur des bisherigen Datenschutzrechts beschreiben, so muß man differenzieren zwischen den Datenschutzgesetzen der ersten Generation, insbesondere also dem BDSG von 1977 und den Landesdatenschutzgesetzen der Phase zwischen 1970 und 1980 einerseits sowie den Datenschutzgesetzen der zweiten Generation, insbesondere also dem BDSG von Ende 1990 und den neueren Landesdatenschutzgesetzen Hessens, Bremens, Nordrhein-Westfalens, Berlins und Hamburgs andererseits.

Bestimmend für die Datenschutzgesetze der ersten Generation war das Konzept der Verhinderung von Mißbrauch. Demgegenüber sind die Gesetze der zweiten Generation stärker von einem Konzept der Gebrauchssteuerung gekennzeichnet. Diese Gebrauchssteuerung ist insbesondere dokumentiert in den Merkmalen

— Transparenz des Informationsverhaltens,

— Beschreibbarkeit der Erforderlichkeit,

— Verbot der Zweckänderung.

Als Beispiel für das Kriterium „Transparenz des Informationsverhaltens" sei genannt die Erhebungsregelung in § 12 HmbDSG, wonach die direkte Befragung des Betroffenen ausdrücklichen Vorrang vor der Informationsermittlung bei dritten Personen und Stellen hat. Zum anderen wird das Prinzip der Transparenz dokumentiert durch verbesserte Ansprüche auf Auskunft, Akteneinsicht, Benachrichtigung über die automatische Verarbeitung von Daten, die Beschreibung des Verarbeitungsrahmens für einzelne Dateien und schließlich die umfassende und rechtzeitige Unterrichtung des Hamburgischen Datenschutzbeauftragten über alle Verfahrensentwicklungen.

Die Kriterien „Beschreibbarkeit der Erforderlichkeit" und „Verbot der Zweckänderung" werden insbesondere durch eine deutliche Betonung des Zweckbindungsgesichtspunktes (§ 13 HmbDSG) dokumentiert. Nur die Daten dürfen verarbeitet werden, die allgemein zur Erfüllung der jeweiligen behördlichen Aufgabe erforderlich sind und außerdem im Hinblick auf den jeweils konkret verfolgten Zweck erforderlich sind. Darüber hinaus ist der Bürger, dem bestimmte Informationen abverlangt werden, über deren Erhebungszweck aufzuklären. Schließlich ist bei Verarbeitung der Angaben in automatisierten Dateien vor deren Errichtung der Verarbeitungszweck zu definieren.

3.3 Lösungsansätze

3.3.1 Rechtliche Regelungen

Obgleich Verbesserungen zweifelsohne feststellbar sind, ist die Grundstruktur der rechtlichen Regelungen einschließlich der bis heute vorherrschenden Kontrolle bereits geschehener Verstöße aber nicht ausreichend, um eine effiziente Steuerung der Risiken für den Datenschutz zu gewährleisten.

Rechtliche Regelungen zur Informationstechnik müssen künftig wesentlich stärker technik- und verfahrensbezogen ausgerichtet werden. Es reicht nicht mehr aus, nur die zulässige bzw. unzulässige Nutzung informationstechnischer Systeme zu normieren; die Rechtsvorschriften müssen auch technische Vorgaben zur Erfüllung und Konkretisierung eben dieser Vorgaben enthalten sowie verfahrensmäßig deren Vorprüfung und Nachbesserung vorsehen.

Dieser Ansatz ergibt sich im wesentlichen daraus, daß Gefährdungen durch informationstechnische Systeme nicht allein durch ihre unangemessene Nutzung auftreten können. Vielmehr können sie ebenso sehr oder in noch größerem Maße durch eine falsche Modellierung bzw. eine fehlerhafte Programmierung die verarbeiteten Daten selbst und damit auch den Datenschutz beeinträchtigen. Daraus ist die Konsequenz zu ziehen, daß die in Rechtsnormen enthaltenen Anforderungen auch für die verschiedenen Phasen der Entwicklung informationstechnischer Produkte festgelegt werden müssen.

Eine prinzipielle Schwierigkeit rechtlicher Techniksteuerung, insbesondere auch im Bereich der Informationstechnik, ergibt sich aus dem Widerspruch, daß Rechtsnormen (Gesetze) auf Beständigkeit angelegt sind, während sich der zu regelnde Bereich der Technik sehr dynamisch weiterentwickelt. Von daher läuft jede Technik regelnde Rechtsvorschrift Gefahr, durch die schnelle Veränderung der technischen Konfiguration zu veralten und damit die Grundlagen ihrer Wirksamkeit zu verlieren.

Da es nur in engen Grenzen möglich ist, die künftige technische Entwicklung zu prognostizieren, müssen rechtliche Instrumente im Bereich der Informationstechnik zwei Anforderungen erfüllen:

— Sie müssen so flexibel angelegt sein, daß eine ständige Anpassung an die sich verändernde Technik möglich ist und

— Möglichkeiten zur Nachbesserung enthalten, so daß neue technische Entwicklungen, die zum Zeitpunkt der Verabschiedung der gesetzlichen Regelungen noch nicht absehbar waren, aufgenommen werden können.

Angesichts des hohen Tempos der informationstechnischen Entwicklung dürfte wichtigste Voraussetzung jeder Technikgestaltung in diesem Bereich sein, daß für die Analyse und Bewertung von Technikfolgen, insbesondere aber auch für die Entwicklung von Gestaltungskonzepten, Zeit gewonnen wird. Dieser Zeitgewinn wird realistischerweise nicht in der Form erfolgen können, daß zur Einführung anstehende Systeme gestoppt oder storniert werden. Realistisch dürfte nur sein, daß Systeme, die als riskant eingeschätzt werden, eine zeitlich bemessene Versuchs- und Irrtumsphase zu durchlaufen haben.

Die Steuerung im Bereich der Informationstechnik sollte sinnvollerweise auf drei Ebenen vorgesehen werden: Der Ebene der Rechtsetzung, der Ebene der technischen Normungen und der Ebene der Zulassung technischer Systeme. Dieses Vorgehen ist erheblich wirksamer, als nachträgliche Kontrollen sein können.

Angesichts der Komplexität informationstechnischer Systeme sollte Technikgestaltung in erster Linie darauf zielen, Rahmenbedingungen für die Techniknutzung zu setzen. Wesentliches Element der Setzung von Rahmenbedingungen wäre dabei die Schaffung von Verfahren, in denen die Planung und Sozialverträglichkeitskontrolle informationstechnischer Systeme zu überprüfen und zu bewerten wäre.

Auf der Ebene der Rechtsetzung existiert das Gesetzgebungs- und Verordnungsverfahren. Hier geht es nicht so sehr um eine Etablierung eines neuen Verfahrens, sondern vielmehr um Modifikationen zum bisherigen Verfahren.

Die im Bereich der Gesetzgebung wichtigste Modifikation wird mit dem Begriff der Reflexivität bezeichnet, also der Möglichkeit des „Nachfassens" des Gesetzgebers, um der Dynamik technischer, insbesondere informationstechnischer Entwicklung als einem offenen, auf Selbstkorrektur angewiesenen Pro-

zeß mit Mitteln der Rechtsetzung adäquat antworten zu können. Diese Reflexivität von Gesetzgebung verlangt institutionelle Vorkehrungen, um die technische Entwicklung und ihre Auswirkungen beobachtbar und bewertbar zu machen.

3.3.2 Technikfolgenabschätzung

Ein bereits seit einiger Zeit bewährtes Mittel sind die Enquete-Kommissionen. Darüber hinaus wäre zu denken an verstärkte Technikfolgenabschätzung mit Verfahren, die zu einer öffentlichen Diskussion und politischen Bewertung der jeweiligen Zukunftsalternativen führen.

Auf der Ebene der Rechtsetzung würde ein Konzept der Reflexivität, d.h. also des Nachfassenkönnens durch den Gesetzgeber, nur Sinn geben, wenn die dafür zuständigen Institutionen entweder selbst zu einer jeweils geplanten Entscheidung mögliche Alternativen entwickeln oder wissenschaftlichen Sachverstand zur Ausarbeitung dieser Alternativen heranziehen.

Zur Umsetzung könnte eine sogenannte Validierungsstelle geschaffen werden, die in einem Zulassungsverfahren dafür sorgt, daß für die IuK-Systeme der jeweils festzulegende Mindeststandard an Sicherung und Schadensvorsorge gewährleistet ist. Dafür kommt insbesondere das einzurichtende Landesamt für Informationstechnik in Betracht.

Die Frage darf nach allem nicht mehr lauten: Wie soll das Recht auf veränderte Entwicklungen reagieren? Vielmehr muß umgekehrt gefragt werden: Wie sind technische Systeme zu gestalten, um der Verfassungsordnung zu entsprechen und die vorgesehenen Entwicklungsziele zu verwirklichen? Die Umsetzung dieses Postulats läuft auf Verfahrensmodelle hinaus. Kernpunkte einer solchen Verfahrensregelung, die sinnvollerweise durch (Rahmen-) Gesetz erfolgen müßte, sollten sein:

1. Definition von Voraussetzungen, unter denen informationstechnische Systeme eingeführt werden können, und
2. Definition eines Verfahrens, um die Einführungsvoraussetzungen im einzelnen prüfen und beurteilen zu können.

Die Struktur eines solchen Verfahrens könnte folgendermaßen skizziert werden: Bislang sind herkömmlich bei der Einführung informationstechnischer Systeme die Systemanalyse auf seiten des Betreibers/Dienstherrn und das Mitbestimmungsverfahren bekannt.

Systemanalysen müßten erweitert werden um die Komponente „Risikoanalyse", mit der die Risiken des geplanten informationstechnischen Systems kalkulierbar würden.

Gesetzestechnisch könnte dies so gestaltet werden, daß der Dienstherr/Betreiber bei der Planung verpflichtet wird, eine Risikostudie (ggf. unterstützt durch

externe Sachverständige) erarbeiten zu lassen. Die Beauftragung der Sachverständigen würde Einvernehmen zwischen Betreiber/Dienstherrn und den vom System Betroffenen bzw. ihren Repräsentanten (Personalrat) verlangen.

Die Ergebnisse einer entsprechenden Studie wären hinsichtlich ihrer Korrekturanforderungen nachvollziehbar von den zuständigen Stellen zu prüfen. Die festgestellten Mängel des vorgesehenen Verfahrens wären abzustellen. Die Mängelkontrolle könnte außerdem durch eine obligatorische Erprobungsphase verbessert werden, für die der Zeitraum und das begleitende und abschließende Prüfungsverfahren mit Benennung der Beteiligten festzulegen wären. Das Hamburgische Datenschutzgesetz wäre entsprechend zu ergänzen.

3.3.3 Vorgehenskonzepte

Durch methodische Instrumente wie Informationsstruktur- und Funktionsstrukturanalysen und die Organisation von größeren Automationsvorhaben in gestaffelten Projektorganisationen kann versucht werden, der gewachsenen Komplexität der Aufgaben Rechnung zu tragen und die in der Informationstechnik zweifellos vorhandenen Steuerungsreserven zu mobilisieren.

Die Hamburger Verwaltung hat sich für ein solches Vorgehenskonzept entschieden, um eine einheitliche und effiziente Durchführung von größeren ADV-Vorhaben zu gewährleisten. Es wäre ohne weiteres möglich, das vorgeschlagene Verfahren der Risikoanalyse und -beschränkung in dieses Vorgehenskonzept einzubeziehen. Dies könnte organisatorisch verknüpft werden mit dem im Rahmen der Neuordnung der Zuständigkeiten für die automatisierte Datenverarbeitung einzurichtenden Landesamt für Informationstechnik. Denkbar wäre es dabei auch, Risikoanalyse und -bewertung in den Prozeß der jährlichen Aufstellung behördenübergreifender IuK-Pläne einzubeziehen.

Diese Ansätze bedürfen weiterer Erörterung. Nach der Stellungnahme des Senats zu diesem Tätigkeitsbericht könnte die Thematik im zuständigen bürgerschaftlichen Ausschuß behandelt und mit einem bürgerschaftlichen Ersuchen vorangebracht werden.

3.4 Probleme der Projektorganisation

3.4.1 Zieldefinition

An ADV-Projekte werden vielfältige Anforderungen gestellt. Sie sollen unter Beachtung der rechtlichen, auch datenschutzrechtlichen Vorgaben

— Rationalisierungseffekte haben, also per Saldo zu Kosteneinsparungen führen, indem sie z.B. Doppelarbeiten vermeiden,

— die Umsetzung politischer Vorgaben erleichtern,

— Verwaltungsabläufe beschleunigen und flexibel gestalten,

— einen jederzeitigen Zugriff auf aktuelle Daten ermöglichen,

— Denk- und Rechenfehlern durch weitgehende Programmsteuerung beikommen,

— die Bürgerfreundlichkeit von Verwaltung erhöhen.

— die Kommunikationsfähigkeit mit einer zunehmend technisierten Umwelt sicherstellen,

— Führungsinformationen bereitstellen,

— die Arbeitsbedingungen der Mitarbeiter verbessern.

Je umfassender ein Projekt angelegt ist und je größer die von der Automatisierung betroffenen Bereiche der Verwaltung sind, desto schwieriger lassen sich die genannten, z.T. widersprüchlichen Zielsetzungen operationalisieren und in ein handhabbares Verfahren umsetzen und desto größer wird die Gefahr des Scheiterns.

3.4.2 DV-Projekte in der hamburgischen Verwaltung

Angesichts des erheblichen Rationalisierungs- und Automationsdrucks wurde in den letzten Jahren eine Anzahl größerer, „strategischer" ADV-Projekte begonnen, die (z.T. mit unterschiedlichen methodischen und technischen Ansätzen) die Verwaltungsarbeit automatisieren sollen.

Zwar wurde die Personalausstattung des IuK-Bereichs kontinuierlich ausgebaut; zwischen 1987 und 1991 wurden mehr als 160 neue Stellen für IuK-Personal geschaffen. Auch die für die Umsetzung bereitgestellten Investitions- und Sachmittel haben erheblich zugenommen. Diese Mittel sind jedoch nur zum Teil und sehr zögernd abgeflossen. Die nur schleppende Entwicklung des Mittelabflusses aus dem globalen IuK-Fonds ist als Indiz dafür zu werten, daß sich die Behörden erheblich mehr vorgenommen zu haben, als sie mit dem ihnen zur Verfügung stehenden Personal realisieren konnten.

Neben einer Vielzahl kleinerer Automationsvorhaben laufen zur Zeit in der Hamburger Verwaltung folgende „strategischen" Automationsprojekte:

— PROSA (Projekt Sozialhilfe-Automation, vgl. 6.1),

— COMVOR (Computerunterstützte Vorgangsbearbeitung bei der Polizei, vgl. 16.1),

— PROPERS (Projekt Personalwesen, vgl. 7.1),

— PAKZU (Projekt Automation des Kraftfahrzeug-Zulassungswesens),

— Automation des Ausländer- und Asylwesens (vgl.14.1),

— LAN-Projekt des Statistischen Landesamtes (vgl. 8.1.2).

Diesen Projekten ist gemeinsam, daß sie wesentliche Verwaltungsfunktionen für einen größeren Bereich automatisieren bzw. im Rahmen von Online-Verfahren unterstützen sollen. Bei der Projektbegleitung sind wir zu dem Eindruck

gelangt, daß die Komplexität der Aufgaben bei einigen Vorhaben zunächst unterschätzt wurde. Dies hat z.B. bei COMVOR dazu geführt, die zunächst äußerst ambitionierten Projektziele (zumindest zunächst) auf ein operationalisierbares Maß zurückzuschrauben.

Bei anderen Projekten – hier ist auf die geplante Automation des Ausländerwesens hinzuweisen – stellt sich die Frage, ob die gegenwärtige Rechtsgrundlage den geplanten Computereinsatz überhaupt trägt. Auch hier müssen die Projektziele noch einmal kritisch überprüft werden. Auf die jeweiligen konkreten Probleme der verschiedenen Projekte wird weiter unten näher eingegangen.

Grundsätzlich müssen Senat und Behörden sich aber fragen lassen, ob nicht statt neuer großer ADV-Vorhaben im Hinblick auf die Realisierungsaussichten überschaubare Teilvorhaben vorzuziehen wären, wie dies z.B. bei der Umsetzung des Projektes Personalwesen vorgesehen ist. Eine derartige Strukturierung würde sicher nicht nur dem Datenschutz, sondern auch insgesamt der Qualität der Ergebnisse für die Bürger und die Verwaltung zugute kommen.

3.5 Lokale Netze und PC-Großrechner-Kopplung

Im 9. TB (3.2) ist ein Datensicherungskonzept für Einzelplatz-PC dargestellt worden, das der Hamburgische Datenschutzbeauftragte seitdem bei seiner Beratungs- und Prüftätigkeit für den öffentlichen und nicht-öffentlichen Bereich zugrunde legt. Dieses Konzept ist im letzten Jahr durch Sicherungsmaßnahmen für Lokale Netze und PC-Großrechner-Kopplung vervollständigt worden.

Kernpunkt des Gesamtkonzeptes ist es, gemäß der gesetzlichen Regelung Maßnahmen zur Datensicherung anzugeben, die in einem angemessenen Verhältnis zur Schutzwürdigkeit der Daten stehen. Diesem Grundsatz folgend haben wir das Konzept differenziert ausgestaltet. Gemäß der unterschiedlichen Sensibilität der Daten wird mit dem vorliegenden Konzept zwischen vier Schutzstufen unterschieden. Damit soll gewährleistet werden, daß das Konzept nicht nur den rechtlichen Gegebenheiten, sondern auch der praktischen Durchführbarkeit entspricht.

Für die Datensicherung bei Personalcomputern liegt damit ein umfassendes Konzept vor, das als Grundlage unserer Beratungs- und Prüfungstätigkeit dient. Das Datenschutzkonzept für PC ist vom Hamburgischen Datenschutzbeauftragten im Oktober 1991 als Broschüre herausgegeben worden und wird daher an dieser Stelle nicht noch einmal dargestellt. Die Broschüre kann kostenlos bei uns bezogen werden.

3.6 Prüfung der Datenverarbeitungszentrale (DVZ)

Die Sachverhaltsermittlungen für die im Februar 1990 begonnene Prüfung der DVZ wurden im November 1990 abgeschlossen. Der vollständige Prüfbericht

ist im Februar 1991 versandt worden; das Senatsamt für den Verwaltungsdienst hat dazu im April Stellung genommen. Wie im letzten Tätigkeitsbericht (9. TB. 3.4) angekündigt, können die Prüfungsergebnisse nunmehr dargelegt werden.

3.6.1 Vorbemerkungen

Die automatisierte Datenverarbeitung im Rechenzentrum der Freien und Hansestadt Hamburg liegt in der Verantwortung unterschiedlicher Behörden. Während die der Finanzbehörde unterstellte DVZ die Aufgaben der maschinellen Durchführung von ADV-Verfahren der hamburgischen Verwaltung wahrnimmt (Datenerfassung, technische Vorbereitung, maschinelle Verarbeitung, Abstimmung und Belegbearbeitung, Formularnachbearbeitung und Versand, Datenträgertransport von und zu den Anwenderdienststellen), ist das Senatsamt für den Verwaltungsdienst – Organisationsamt – für die ADV-Gesamtplanung (methodische Vereinheitlichung, Maschinenplanung, die Organisation der technischen Einrichtungen, Datenbanken, Datenerfassung u.ä.) und die Systemprogrammierung zuständig. Den Fachbehörden obliegen Verfahrensentwicklung (Problemanalyse, Planung, Programmierung, Einführung) und -pflege (Änderung und Anpassung bestehender ADV-Verfahren). Darüber hinaus ist die Baubehörde – Fernmeldeabteilung – bei Fragen des Netzausbaus beteiligt.

In der DVZ werden eine Vielzahl automatisierter Verfahren verschiedener öffentlicher Stellen abgewickelt. Die Aufgaben der DVZ entsprechen dabei denjenigen des Auftragnehmers bei der Auftragsdatenverarbeitung, auch wenn die DVZ als Teil der hamburgischen Verwaltung nicht formell als Auftragnehmer i.S.v. § 3 HmbDSG anzusehen ist. Unter sinngemäßer Anwendung dieser Vorschrift darf die DVZ nur im Rahmen der ihr erteilten Aufträge tätig werden.

Die DVZ hat die erforderlichen Maßnahmen zur Datensicherung (§ 8 HmbDSG) für ihren Bereich zu ergreifen. Die fachliche Verantwortung für die Datenverarbeitung und für die verfahrensspezifischen Maßnahmen zur Datensicherung liegt bei den Auftraggebern, d.h. den für die rechtmäßige Erfüllung der jeweiligen Fachaufgabe zuständigen Stellen (speichernde Stellen i.S.v. § 4 Abs. 3 HmbDSG). Die hamburgischen Behörden haben jedoch, soweit sie keine eigenen Rechner betreiben, faktisch keine Möglichkeit, einen Auftragnehmer für die Durchführung ihrer automatisierten Verfahren „unter besonderer Berücksichtigung der Eignung der von ihm getroffenen Maßnahmen zur Datensicherung (§ 8) sorgfältig auszuwählen", wie es § 3 Abs. 1 Satz 2 HmbDSG vorschreibt, sondern sie sind auf die DVZ angewiesen.

Vor diesem Hintergrund ist die Datensicherheit in der DVZ von grundlegender Bedeutung für die Gewährleistung des Datenschutzes in der hamburgischen Verwaltung.

3.6.2 Prüfungsinhalte

Wie bei der Prüfung 1984/85 stand wieder die Sicherheit der Datenverarbeitung in der DVZ im Mittelpunkt, nicht die bei einzelnen automatisierten Verfahren zu treffenden und von den zuständigen Behörden zu verantwortenden Sicherungsmaßnahmen. Mit Sicherheit der Datenverarbeitung sind die gemäß § 8 HmbDSG zu treffenden Maßnahmen gemeint, die erforderlich sind, um den Schutz der in der DVZ verarbeiteten Daten zu gewährleisten, wobei sich die erforderlichen Schutzmaßnahmen an der Gefährdung der Daten zu orientieren haben. Schwerpunkt der Prüfung war die Frage, wie die in der DVZ eingesetzten sicherheitsrelevanten Softwareprodukte (Betriebssysteme, systemnahe Software, Sicherheitssoftware, der Sicherheit dienende Komponenten in Anwendungssoftware) zusammenwirken und inwieweit damit die gebotene Datensicherheit erreicht wird.

In der DVZ werden Großrechner der Hersteller IBM und Siemens unter den Betriebssystemen MVS und BS2000 betrieben. Für die Datenfernverarbeitung werden mehrere Datenübertragungsnetze (u.a. SNA und TRANSDATA) unterhalten. Angesichts der Vielfalt der eingesetzten Produkte haben wir uns auf folgende Komplexe beschränkt:

- Funktionsweise und Zusammenwirken der Produkte im IBM-Rechnerbereich:
  - Betriebssystem MVS,
    - Sicherungssoftware Top Secret Security,
    - Transaktionsmonitor COM-PLETE,
- Funktionsweise und Zusammenwirken der Produkte im Bereich der Siemens-Rechner:
  - Betriebssystem BS2000,
    - Transaktionsmonitor UTM,
- Funktionsweise und Zusammenwirken der Produkte der Software AG und deren Einbindung in die BS2000- und MVS-Umgebung:
  - PREDICT/CASE,
  - ADABAS SECURITY,
  - NATURAL SECURITY.

Die äußere Datensicherheit (z.B. das Zugangskontrollsystem der DVZ oder die physische Leitungssicherung) war nicht Gegenstand der Prüfung. Die Sachverhaltsermittlung erfolgte im wesentlichen in Form von „Expertengesprächen". Weil sich die Untersuchung überwiegend auf Systemsoftware und „Allgemeine Software" bezog, die vom Senatsamt für den Verwaltungsdienst bereitgestellt wurde und für die die dortigen Systemprogrammierer zuständig sind, nahmen fachkundige Vertreter des Organisationsamtes an den Gesprächen in der DVZ teil. Hieran schlossen sich verschiedene Prüfungen vor Ort in

der DVZ, im Organisationsamt und in einem Fall bei einer anwendenden Dienststelle an. Im Mittelpunkt dieser Termine stand die Ermittlung der tatsächlichen Administration des DVZ-Systems einschließlich der eingesetzten Sicherheitssoftware.

3.6.3 Bewertungsmaßstäbe

In der DVZ werden Daten von besonderer Schutzwürdigkeit verarbeitet, (z.B. Sozialdaten und polizeiliche Ermittlungsdaten). An die zu treffenden Sicherungsmaßnahmen sind daher hohe Ansprüche zu stellen. Dies bedeutet, daß

- der Systemzustand – insbesondere im Hinblick auf die ergriffenen Sicherheitsmaßnahmen und Sicherheitsverletzungen – revisionssicher dokumentiert wird,
- die Systembenutzung durch Unberechtigte verhindert wird,
- Verfahren, Datenbestände und Benutzer wirkungsvoll voneinander abgeschottet werden,
- Berechtigungsüberschreitungen verhindert und entsprechende Versuche dokumentiert und aufgeklärt werden,
- durch organisatorische Maßnahmen (vor allem eine sinnvolle und verbindliche Zuständigkeitsregelung und konsequente Funktionstrennung) mögliche Mißbrauchsfälle erschwert werden.

Den Ausgangspunkt der Bewertung der Systemsicherheit bilden die von den Betriebssystemen standardmäßig bereitgestellten Sicherheitsmechanismen. Im Zusammenspiel mit der übrigen eingesetzten Systemsoftware (einschließlich spezieller Sicherheitssoftware) ergibt sich ein maximal auf einem System erreichbares Sicherheitsniveau. Inwieweit dieses Niveau tatsächlich auch erreicht wird, hängt entscheidend von der jeweiligen Konfiguration und Administration ab.

Den genannten Maßstäben entsprechend haben wir aufgrund unserer Prüfungsfeststellungen Vorschläge und Forderungen zur Erhöhung der Sicherheit der Datenverarbeitung in der DVZ erarbeitet. Die Stellungnahme des Senatsamtes und die inzwischen vorgenommenen Verbesserungen sind in der Darstellung berücksichtigt.

3.6.4 Prüfungsergebnisse und Forderungen

Zusammenfassend haben unsere Feststellungen ergeben, daß in beiden Systemwelten erhebliche – zum Teil durch die unvollkommene Administration bedingte – Sicherheitsmängel bestanden haben. Da seitens des Organisationsamtes die von uns monierten Sicherheitsmängel in der DVZ im wesentlichen anerkannt wurden und entsprechende Abhilfe bereits geplant war bzw. zugesagt worden ist, haben wir von einer Beanstandung abgesehen.

Die derzeitigen verteilten Zuständigkeiten haben Abgrenzungsprobleme und einen hohen Koordinierungsaufwand zur Folge. Wir haben deshalb vorgeschlagen, Systemprogrammierung und maschinelle Durchführung der Datenverarbeitung einer einheitlichen Dienst- und Fachverantwortung zu unterstellen. Der Senat hat inzwischen die Einrichtung eines Landesamtes für Informationstechnik beschlossen. Hierin sollen zukünftig bisher vom Organisationsamt, der Datenverarbeitungszentrale und der Baubehörde – Abteilung Fernmeldetechnik – wahrgenommene Aufgaben personell und organisatorisch zusammengefaßt werden.

Wir haben feststellen müssen, daß kein grundlegendes, nachvollziehbares Sicherheitskonzept für die DVZ vorhanden ist. Es gibt lediglich für die eingesetzten Produkte mehr oder minder ausführliche Dokumentationen, in denen Datenschutz und Datensicherheitsprobleme z.T. nur unzureichend erörtert werden. Wir haben deshalb gefordert, ein solches Sicherheitskonzept zu erarbeiten. Daraus sollte hervorgehen, welche Anforderungen an die Systemsicherheit insgesamt gestellt werden und durch welche technischen und organisatorischen Maßnahmen diese Vorgaben realisiert werden. Der Auffassung des Organisationsamtes, ein durchgängiges Sicherungskonzept sei durchaus vorhanden, wenn auch nicht zusammenhängend dokumentiert, können wir zwar nicht folgen. Wir begrüßen aber die Zusage, die Ergebnisse grundlegender Sicherheitsuntersuchungen der eingesetzten DV-Systeme zu einem einheitlichen Sicherheitsprofil zusammenzuführen mit dem Ziel, das ordnungsgemäße Verhalten und die Funktionalitäten der DV-Systeme in der DVZ zu gewährleisten.

Die parallele Verwendung zweier Betriebssysteme mit unterschiedlicher Systemphilosophie und voneinander stark abweichenden Datenschutzmechanismen erschwert die Gewährleistung eines gleichmäßigen Schutzniveaus und hat zur Folge, daß nahezu sämtliche konzeptionellen Überlegungen und technischen Maßnahmen der Datensicherheit doppelt erfolgen müssen. Bei Beibehaltung unterschiedlicher Großrechnerbetriebssysteme sollte daher darauf hingewirkt werden, daß betriebssystemunabhängige Sicherheitsprodukte oder zumindest solche Produkte mit gleicher Sicherheitsphilosophie eingesetzt werden.

Das Senatsamt ist hier der Auffassung, daß Sicherheitssoftware an das zu schützende Betriebssystem genau angepaßt sein müßte, was bei den erheblichen Unterschieden in den jeweiligen Ansätzen zur Gewährleistung praktischer Sicherheit und bei der Komplexität der Anwendungen mit einem gemeinsamen Sicherheitsprodukt kaum möglich sei. Zumindest fände sich am Markt bisher kein Anbieter. Dem ist entgegenzuhalten, daß es sehr wohl Sicherheitssoftware gibt, die verschiedene Betriebssysteme zu unterstützen vermag. Gleichwohl trifft es zu, daß auf dem Markt für die in der DVZ eingesetzten Betriebssysteme zur Zeit keine gemeinsamen Sicherheitsprodukte angeboten werden. Die Verwaltung sollte hier jedoch ihren Bedarf formulieren, um bei den Herstellern entsprechende Bemühungen zu fördern.

Unsere Prüfung hat außerdem Hinweise auf Schwachstellen im Paßwortmanagement ergeben. Da die Paßwortprüfung der wichtigste in der DVZ zur Zeit eingesetzte Authentifikationsmechanismus ist, wird hierdurch die Systemsicherheit entscheidend in Frage gestellt. Das Senatsamt hat zugesagt, unserer Forderung nachzukommen, verbindliche Grundsätze zur Paßwortvergabe zu erstellen.

Unserer Forderung, Paßwörter grundsätzlich nur einwegverschlüsselt zu speichern, kann die DVZ aus technischen Gründen nur zum Teil folgen. Bei der Datenbank ADABAS und im Betriebssystem BS2000 wird mit dem Einsatz neuer Versionen eine Einwegverschlüsselung gegeben sein.

Die Prüfung hat Lücken in der Dokumentation der Einrichtungsaufträge für Benutzerkennungen aufgedeckt. Dadurch war es im Einzelfall nicht möglich nachzuvollziehen, an wen aufgrund welchen Auftrags welche Berechtigungen vergeben wurden. Wir haben deshalb gefordert, in der DVZ eine lückenlose Sammlung der Einrichtungsaufträge für Benutzerkennungen aufzubauen. Jeder Einrichtungsauftrag muß Angaben darüber enthalten, welche Zugriffsrechte erteilt werden sollen. Sofern Einrichtungsaufträge noch an anderem Ort archiviert sind, müssen sie an die DVZ übergeben werden. Unvollständige Einrichtungsaufträge müssen kurzfristig ergänzt, fehlende angefordert werden. Das Senatsamt will dieser Forderung entsprechen.

3.6.5 MVS-Bereich

Unter dem Betriebssystem MVS kann grundsätzlich auf alles zugegriffen werden, was nicht besonders geschützt ist (Erlaubnis mit Verbotsvorbehalt). Der Systemverwalter (Supervisor) hat standardmäßig umfassende Rechte, die theoretisch auch von nichtprivilegierten Benutzern mit detaillierten Systemkenntnissen erschlichen werden könnten. Durch den Einsatz entsprechender Sicherheitssoftware kann jedoch eine wirksame Benutzer- und Zugriffskontrolle realisiert werden.

Im Hinblick auf die Gewährleistung eines ordnungsgemäßen Funktionierens des zentralen Sicherheitssystemes im IBM-Bereich haben wir gefordert, die bereits 1987 zugesagte umfassende Darstellung von Top Secret Security möglichst bald zu verfassen und sicherzustellen, daß sie auf dem jeweils aktuellen Stand gehalten wird. Eine solche Dokumentation sollte aus sich heraus gleichermaßen für Prüfer, Rechenstelle und Anwender eine verständliche, nachvollziehbare Beschreibung der jeweils wahrzunehmenden Fachaufgaben, der Zuordnung von Funktionen zu zuständigen Stellen sowie der zur Datensicherung ergriffenen Maßnahmen ergeben. Eine bloße Sammlung detaillierter Übersichten und vorhandener Herstellerunterlagen genügt unserer Meinung nach nicht diesen Ansprüchen.

Das Senatsamt teilt diese Auffassung nicht. Es verweist auf die durch Dienstanweisung vorgeschriebene Produktdokumentation. Diese sei vollständig vorhanden, immer einsehbar und entgegen unserer Meinung hinsichtlich der Parameterisierung von Top Secret Security auch jederzeit nachvollziehbar.

Die Einrichtung von Top Secret Security und seine Einbindung in das Betriebssystem erfolgt zentral durch die Systemprogrammierung im Organisationsamt. Die Administration der Sicherheitssoftware (z.B. Eintragung und Löschung von Benutzern, Neutralisierung von Paßwörtern) wird, ebenfalls zentral, in der DVZ durchgeführt. Dabei handelt die DVZ weisungsgebunden nach den von der fachlich zuständigen Stelle schriftlich erteilten Aufträgen. Verbindliche Zuständigkeitsregelungen bestehen allerdings nicht. Diesen Organisationsmangel haben wir moniert, das Senatsamt will ihn beheben.

In Behördenverfahren mit einer hohen Zahl zugriffsberechtigter Benutzer ist eine zentrale Verwaltung vergessener Paßwörter in der DVZ kaum den zeitlichen Anforderungen entsprechend zu realisieren. Bestrebungen, neben der Paßwortabfrage unter Top Secret Security den Zugriff auf Programme und Daten zusätzlich dezentral auf Anwendungsebene mit einer administrierbaren Kennwortprüfung zu belegen, erfüllen nicht die an eine Benutzerverwaltung zu stellenden Sicherheitsansprüche. Die Sachbearbeiter könnten dazu übergehen, ihr zentrales Paßwort auf beiden Ebenen zu verwenden. Auf Anwendungsebene besteht aber im Gegensatz zu Top Secret Security ein erheblich geringerer Schutz gegen unerlaubten Datenzugriff, da Paßwörter z.B. unverschlüsselt in nicht besonders gesicherten Dateien gespeichert werden (siehe dazu auch 9.TB, 4.1.1.1). Das Sicherheitssystem Top Secret Security bietet die Möglichkeit, seine Administration zu dezentralisieren, d.h. nach „Departments" und „Divisions" zu untergliedern. Unserer Anregung, dezentrale Paßwortverwaltung deshalb nicht auf Anwendungsebene, sondern mit Top Secret Security durchzuführen und auf die jeweils fachlich zuständigen Stellen zu übertragen, hat das Senatsamt zugestimmt. Bei Funktionstrennung obliege den fachlichen Leitstellen auch die Autorisierung von anwendenden Stellen und Benutzern.

Top Secret Security kann den Zugang zu Programmen, Dateien, Datenträgern, Katalogen, Terminals, Transaktionen und Jobs schützen. Ein Benutzer darf jeweils nur auf die Ressourcen zugreifen, für die er ausdrücklich berechtigt wird. Beim Generieren muß daher dem System über Steuerungsparameter von der Systemprogrammierung mitgeteilt werden, welche Ressourcen im einzelnen geschützt werden sollen.

Unsere Prüfung hat ergeben, daß sich der Schutz von Top Secret Security in der DVZ standardmäßig auf Dateien, Magnetplatten und Benutzerkennungen erstreckt; die übrigen Ressourcen werden nur in bestimmten Fällen einbezogen. Beispielsweise wird nicht von der Möglichkeit Gebrauch gemacht, Terminals durch Top Secret Security zu schützen, d.h. prüfen zu lassen, ob eine Anmeldung von einem Benutzer ausgelöst wurde, für den das verwendete Terminal zugelassen ist. Wir haben daher vorgeschlagen, bei Dialoganwendungen mit sensiblen personenbezogenen Daten ausnahmslos von der Möglichkeit des Terminalschutzes Gebrauch zu machen. Das Senatsamt will diesem Vorschlag folgen.

Benutzerkennungen sind individuell zu vergeben, d.h. jedem Benutzer ist eine eigene Kennung zuzuweisen. Wir haben feststellen müssen, daß hiervon nicht durchgängig Gebrauch gemacht wurde, d.h. einzelne Kennungen von mehreren Benutzern verwendet wurden. Das Fehlen eindeutiger Zuordnungen von Benutzerkennungen zu Personen widerspricht, soweit personenbezogene Daten verarbeitet werden, dem Gebot der Eingabekontrolle (§ 8 Abs. 2 Nr. 7 HmbDSG). Bereits bei der Einrichtung von Benutzerkennungen muß deshalb der Top Secret Security-Administration mitgeteilt werden, auf welche Person sich die Kennungen beziehen. Es ist zu gewährleisten, daß die Eintragungen unter Top Secret Security auf dem aktuellen Stand bleiben. Neben einer maschinellen Überprüfung nicht mehr aktueller Einträge müssen die Behörden zu einer laufenden Aktualisierung ihrer Angaben veranlaßt werden. Die von uns festgestellte mangelnde Pflege der Eintragungen bedeutet ein erhebliches Sicherheitsrisiko, da auf diese Weise längst nicht mehr berechtigte Mitarbeiter Zugriff auf Daten hätten.

Die von Top Secret Security angebotenen Möglichkeiten zur genauen Definition von Zugriffsrechten wurden bei weitem nicht ausgenutzt. So konnten Benutzer aufgrund ihres Berechtigungsprofils nicht nur auf Daten zugreifen, die sie im Rahmen ihrer Befugnisse bearbeiten durften, sondern, ohne daß weitere Sicherungen griffen, auch auf alle anderen Produktionsdateien ihrer Behörde. Dies ist als schwerwiegender Organisationsmangel zu werten. Programmierende Stellen benötigen in der Regel keine Zugriffsberechtigung auf Echtdaten. Auch in der hamburgischen Verwaltung gilt, daß nur derjenige auf Daten zugreifen darf, der diese für seine Fachaufgabe benötigt. Wir haben leider feststellen müssen, daß unter der Benutzung von ROSCOE – eines im MVS-Bereich zur Programmentwicklung/-verwaltung eingesetzten Softwareproduktes – in Einzelfällen die Trennung von Test und Produktion unterlaufen werden konnte. Dies muß durch konsequente Anwendung der Namenskonventionen und Überprüfung der Benutzerberechtigungen verhindert werden. Unserer Forderung nach eindeutiger Zuordnung der Benutzerkennungen zu Personen im Top Secret Security und nach konsequenter Einhaltung der Namenskonventionen will das Senatsamt nachkommen. Es werde ein Verfahren zur Aktualisierung der Top Secret Security-Datenbank entwickelt, das die personelle Zuordnung von Benutzerkennungen unterstützt und die erforderliche Dokumentation für eine nachgehende Kontrolle erstellt.

Für die Benutzerrechte im Transaktionsmonitor COM-PLETE – unter MVS eingesetztes Systemprogramm, das Transaktionsprogramme oder Teile von diesen steuert und koordiniert – gelten die zur Administration von Top Secret Security aufgestellten Vorschläge und Forderungen entsprechend. Die bestehende Zuständigkeitsregelung (Top Secret Security wird von der DVZ verwaltet, COM-PLETE vom Organisationsamt) führt unserer Meinung nach fast zwangsläufig zu zusätzlichem, mit Fehlerrisiken behaftetem Koordinationsaufwand. Top Secret Security- und COM-PLETE-Administration sollten deshalb an einer Stelle zusammengefaßt werden. Nach Auffassung des Senatsamtes lassen

sich die Funktionen von COM-PLETE-SECURITY-Administration derzeit nicht klar von der Systemprogrammierung abgrenzen. Solange dies nicht möglich sei, wäre eine Zusammenlegung mit der Top Secret Security-Administration nicht beabsichtigt. Die Software AG entwickelt allerdings ein Produkt, daß die in Einzelkomponenten vorhandene Sicherheitssoftware vereinigt. Sobald dieses verfügbar sei, könne die Administration in der DVZ zusammengefaßt werden, soweit dabei nicht eindeutig Aufgabenbereiche der Systemtechnik berührt werden. Unsere Forderung, auch bei COM-PLETE-Benutzern bereits auf der Ebene von Top Secret Security dafür Sorge zu tragen, daß Test und Produktion voneinander getrennt werden, ist nach Auffassung des Senatsamtes derzeit technisch nicht umsetzbar. Eine Realisierung würde jedoch beim Einsatz neuer Versionen erneut geprüft.

3.6.6 BS2000-Bereich

Im Betriebssystem BS2000 verfügt jedes Softwareprodukt über spezielle Sicherheitsinstrumente, wobei die Ergebnisse der jeweiligen Kontrolle aber in der bislang von der DVZ eingesetzten Betriebssystemversion nicht an andere Ebenen weitergegeben werden. Um eine wirksame Benutzer- und Zugriffskontrolle zu gewährleisten, ist es deshalb zwingend geboten, für die Verarbeitung personenbezogener Daten alle derzeit verfügbaren Sicherungsinstrumente des Betriebssystems BS2000 zu verwenden.

Mit dem Einsatz der Version 10 eröffnen sich neue Möglichkeiten der Zugriffskontrolle auf Daten und Programme, z.B. Mechanismen zur erweiterten Rechteverwaltung, zur Dezentralisierung der Systemverwaltung und der Protokollierung sicherheitsrelevanter Vorgänge. Die Funktionen der Beweissicherung gewährleisten dann eine lückenlose Auswertung aller Verarbeitungsschritte und Aktionen.

Nach Eingabe von Benutzerkennung, Paßwort und verfahrensbezogener Abrechnungsnummer wird einem Benutzer der Zugang zum Betriebssystem BS2000 gewährt, wenn die Angaben mit Einträgen im zentralen Benutzerkatalog übereinstimmen. Zugriffsberechtigungen werden über die Benutzerkennung als zentrales Merkmal verwaltet, beispielsweise ist jede Datei an die User-ID eines Eigentümers gebunden.

Obwohl individuelle Benutzerkennungen bei BS2000 möglich sind, wurden zum Zeitpunkt der Prüfung in der DVZ anwendungsbezogene User-ID's vergeben. Sämtliche Benutzer mit einheitlicher Aufgabe wiesen sich in diesem Fall mit derselben Kennung gegenüber dem System aus. Als Begründung wurde in der DVZ der anderenfalls entstehende Verwaltungsaufwand für dateispezifische Paßwörter genannt. Greifen nämlich im Rahmen ihrer Aufgaben mehrere Benutzer auf die gleiche Datei zu, müßte diese als mehrbenutzerfähig („sharable") deklariert werden, da die Rechte an jeder Datei ansonsten immer nur dem Eigentümer zustehen. Um den Zugriff nichtberechtigter Benutzer auf diese „sharable" gesetzten Dateien auszuschließen, müßte jeweils ein zusätzliches

Paßwort für diese Dateien vergeben werden. Wegen der anwendungsbezogenen Vergabe von Benutzerkennungen und Paßwörtern war die Benutzer- und Zugriffskontrolle nicht sichergestellt. Die Eingabekontrolle war ebenfalls nicht gewährleistet, weil die Eingaben lediglich auf Kennungen und nicht auf einzelne Benutzer zurückzuführen gewesen wären.

Wir haben daher gefordert, in der DVZ so schnell wie möglich die Version 10 des Betriebssystems BS2000 einzusetzen und die mit dieser Version vorgesehene benutzerbezogene Zugriffskontrolle einzuführen. Solange dies noch nicht der Fall ist, sollten sämtliche Dateien mit personenbezogenen Daten, die „sharable" gesetzt sind, zusätzlich mit einem Paßwort gegen unberechtigtes Lesen, Schreiben oder Verändern geschützt werden. Das Senatsamt wird die Version 10 von BS2000 schrittweise auf den betreffenden Rechnern in der DVZ einsetzen. Für den Schutz mehrfachbenutzbarer Dateien wurde die Entwicklung einer entsprechenden Prozedur zugesagt.

Das Betriebssystem BS2000 läßt über den Eintrag im zentralen Benutzerkatalog die Möglichkeit zu, Benutzerkennungen ohne Paßwort einzurichten sowie die Änderung von Paßwörtern durch den Anwender zu unterbinden. Beide Optionen sind dahingehend festzulegen, daß lediglich User-ID mit veränderbarem Paßwort vergeben werden dürfen. Dieser Forderung wird vom Senatsamt entsprochen. Ferner sollen vergessene Kennwörter grundsätzlich neu vergeben werden, ohne daß die Systemverwaltung auf das alte Paßwort zugreifen muß.

Unter der Systemverwalterkennung TSOS stehen umfangreiche Zugriffsrechte zur Verfügung, z.B. können alle Einträge im zentralen Benutzerkatalog unter dieser Kennung gelesen und geändert werden. TSOS-berechtigt ist entsprechend den bestehenden Zuständigkeiten ausschließlich das Organisationsamt, die DVZ hat sich auf die Produktionssteuerung zu beschränken. Da jedoch bestimmte von der DVZ wahrzunehmende Aufgaben nur unter der TSOS-Kennung abgewickelt werden können, haben die Systemverwalter eine schreibgeschützte und lediglich ausführbare Prozedur installiert, mit der TSOS-privilegierte Programme durch die Mitarbeiter der Produktionssteuerung in der DVZ angestoßen werden können, ohne daß sie direkt die TSOS-Berechtigung erhalten. Unsere Forderung, sämtliche in der DVZ unter TSOS wahrzunehmende Tätigkeiten unter einer solchen Prozedur abzuwickeln, entspricht der zwischen Organisationsamt und DVZ getroffenen Vereinbarung.

Unter dem Betriebssystem BS2000 werden in der DVZ unter anderem alle Aktionen an der Konsole, Eingaben, Meldungen des Systems, Fehlermeldungen, LOGON-Meldungen (Benutzerkennung, Terminal) und gestartete Druckaufträge protokolliert. Aktionen unter TSOS können hierüber bisher aber nicht festgehalten werden. Im Sinne einer angemessenen Eingabekontrolle wurde aufgrund unserer Forderung für TSOS eine benutzereigene Protokolldatei angelegt.

Vom Betriebssystem BS2000 werden sowohl Teilnehmer- als auch Teilhaberbetrieb unterstützt. Der Teilnehmerbetrieb ist eine Form des Dialogbetriebes, bei

der mehrere Benutzer unabhängige, im allgemeinen voneinander verschiedene Aufgaben, bearbeiten. Im Teilhaberbetrieb bearbeiten mehrere Benutzer dasselbe Aufgabengebiet mit einem oder mehreren zentral gespeicherten Anwendungsprogrammen. Diese Programme führen Transaktionen aus, d.h. Folgen logisch zusammengehöriger Aktionen, die Operationen auf gemeinsam gespeicherte Daten ausführen. Im Gegensatz zum Teilnehmerbetrieb nutzt nicht ein einzelner Anwender, sondern ein Programm die Funktionen des Betriebssystems. Dabei stellt dieses Programm selbst wieder Funktionen für seine Benutzer zur Verfügung.

In der DVZ wird hierfür der Transaktionsmonitor UTM (Systemprogramm, das Transaktionsprogramme oder Teile von diesen steuert und koordiniert) eingesetzt. UTM verfügt über eigene Zugangs- und Zugriffssicherungen. Jede UTM-Anwendung wird gesondert generiert und administriert. Dabei kann eine Schutzhierarchie dahingehend aufgebaut werden, daß

— bestimmte Benutzer nur bestimmte Teilprogramme verwenden dürfen,

— bestimmte Benutzer nur an bestimmten Datenstationen arbeiten dürfen,

— von bestimmten Datenstationen nur bestimmte Teilprogramme genutzt werden dürfen,

— bestimmte Teilprogramme nur auf bestimmte Teile der Datenbank zugreifen können.

Die zu schützenden Objekte (Datenbanken, Teilprogramme, Datenstationen) werden dafür auf Systemebene mit einem logischen Schloß versehen, die Benutzer dieser Objekte (Anwender, Datenstationen, Teilprogramme) erhalten einen entsprechenden logischen Schlüssel. Anwendungen unter UTM im Teilhaberbetrieb bieten damit wesentlich umfangreichere Zugriffskontrollfunktionen, als sie derzeit im Teilnehmerbetrieb möglich sind. Leider haben wir festgestellt, daß der Schlüssel-/Schloß-Mechanismus bei keiner UTM-Anwendung in der hamburgischen Verwaltung benutzerbezogen eingesetzt wird. Nach dem Anschalten des Bildschirmgeräts werden lediglich die Zugriffsrechte des Terminals abgefragt.

Wir halten es für unbedingt notwendig, sämtliche Verfahren im Teilhaberbetrieb abzuwickeln. Die Zugangskontrolle sollte auf oberster Ebene mittels Schlüssel-/Schloß-Konzept unter dem Transaktionsmonitor UTM erfolgen. UTM-autorisierten Benutzern könnten auf Datenbankebene weitere Zugriffsrechte eingeräumt werden. Dieser Vorschlag entspricht der Planung des Senatsamtes. Im Teilnehmerbetrieb sollen grundsätzlich nur noch Verfahrensentwicklung und -pflege betrieben werden. Bei Verfahren, die weiterhin im Teilnehmerbetrieb ablaufen müßten, z.B. bei Nutzung konfektionierter Software, werde der vorhandene Befehlsvorrat für den Benutzer eingeschränkt.

Die UTM-Administration wird zentral von der DVZ übernommen. Das Senatsamt beabsichtigt, durch entsprechende Generierungsmaßnahmen den Verbin-

dungsaufbau zu Datensichtgeräten im Rahmen von Tests durch die UTM-Anwendung zu verhindern und die Nutzung einzelner UTM-Sicherungsmaßnahmen zu erzwingen. Die Konzentration der Generierung von UTM-Anwendungen von den programmierenden Stellen auf eine zentrale Stelle sei mangels des hierfür erforderlichen qualifizierten Personals gegenwärtig nicht geplant.

Die Magnetplattenverwaltung im BS2000 bietet mit dem Produkt MPVS (Multiple-Public-Volume-Set) die Möglichkeit, Zugriffsberechtigungen auf einzelne Speicherbereiche zu beschränken. Die Umstellung der einem alleinigen Eigentümer zur Verfügung stehenden Datenträger (private volume) auf MPVS wurde im Laufe des Jahres abgeschlossen. Dabei sind grundsätzlich die Behörden voneinander sowie Test und Produktion getrennt worden.

BS2000 unterstützt den Datenträgeraustausch auf Magnetbändern gemäß der DIN 66029, die die Struktur der auf dem Datenträger befindlichen Band- und Dateikennsätze enthält. Hierzu zählen u.a. auch Schutzattribute der gespeicherten Dateien. Fehlen diese Kennsätze oder sind sie nicht genormt, ist es für einen Datenzugriff unter Umständen erforderlich, entsprechende Kennsatzprüfungen zu umgehen. Die Erteilung der hierfür erforderlichen Berechtigung sollte aber allein auf die TSOS-Kennung beschränkt bleiben. Programmierer sollten sich daher im Bedarfsfall nicht, wie bisher, an die Produktionssteuerung, sondern an die Systemprogrammierung wenden, um im Einzelfall befristet Kennsatzprüfungen umgehen zu dürfen. Die Möglichkeit, unter bestimmten Umständen die Kennsatzprüfung umgehen zu können, ist nach Auffassung des Senatsamtes bei jedem Betriebssystem gegeben und im Interesse der Aufrechterhaltung des Betriebes in Ausnahmesituationen unverzichtbar. Diese Optionen seien selbstverständlich besonders abzusichern.

3.6.7 Produkte der Software AG

In der DVZ werden sowohl im MVS-Bereich als auch im BS2000-Bereich Produkte der Software AG eingesetzt. Es handelt sich dabei um die Datenbanksoftware ADABAS, die Datenbankabfragesprache NATURAL und das Dateninformations- und Verwaltungssystem PREDICT. Unter ADABAS gespeicherte Daten lassen sich zusätzlich durch ADABAS SECURITY vor unerlaubten Zugriffen schützen. Mittels NATURAL SECURITY kann die Berechtigung von Anwendern, die über die Abfragesprache NATURAL auf ADABAS-Dateien zugreifen, überprüft werden. Alle Produkte der Software AG werden zentral vom Organisationsamt verwaltet.

Auf ADABAS-Daten kann sowohl über NATURAL als auch durch direkte Programmierung, dem sogenannten „native mode", zugegriffen werden. Hiervon machen verschiedene Behörden auch bei sensiblen Daten Gebrauch. Der direkte Zugriff bot erfahrenen Programmierern mit detaillierten ADABAS-Kenntnissen zum Zeitpunkt der Prüfung unter bestimmten Voraussetzungen die Möglichkeit, verfahrensfremde Daten zu bearbeiten. Das Gefährdungspotential

war besonders hoch, wenn sich Test- und Produktionsdaten verschiedener Anwendungen auf einem Rechner befanden. Um diese Sicherheitslücke zu schließen, wären mehrere Maßnahmen notwendig.

Wir haben daher gefordert, sämtliche ADABAS-Zugriffe nur noch über die Abfragesprache NATURAL erfolgen zu lassen. Es sollte darüber hinaus sichergestellt werden, daß zumindest keine weiteren Verfahren entwickelt werden, die mittels Direktprogrammierung im „native mode" den Zugang auf ADABAS-Daten eröffnen. Anwender, die sensible personenbezogene Daten unter ADABAS speichern, sollten diese zusätzlich vor unerlaubten Fremdzugriffen über den „native mode" schützen. ADABAS SECURITY bietet hierfür die Möglichkeit, Dateien mit einem einwegverschlüsselten Paßwort zu belegen, daß dem Anwendungsprogramm für eine berechtigte Nutzung bekannt sein muß. Es sollte auch sichergestellt werden, daß auf der gleichen Anlage keine Produktionsdaten anderer Verfahren gespeichert werden.

In der seit Januar 1991 eingesetzten ADABAS-Version stehen nach Mitteilung des Senatsamtes zwei neue Benutzerausgänge zur Verfügung, mit deren Hilfe es möglich sei, auch bei Direkt-Programmierung die Datenbanken gegen unberechtigten Zugang zu schützen. Der Direktzugriff stelle mit dem Einsatz dieser „User-Exits" kein besonderes Risiko mehr dar.

Im MVS-Bereich gelangt ein durch Top Secret Security autorisierter Benutzer über den Transaktionsmonitor COM-PLETE auf die NATURAL-Ebene. Benutzerkennung und Paßwort der ursprünglichen Anmeldung werden von NATURAL SECURITY automatisch übernommen und auf die damit verbundenen Zugriffsberechtigungen geprüft.

Im BS2000-Bereich haben wir dagegen kein Verfahren vorgefunden, daß sowohl Sicherungsinstrumente des Transaktionsmonitors UTM als auch von NATURAL SECURITY verwendet. Entweder wird auf den Einsatz von UTM verzichtet oder es kann unter Umgehung von NATURAL SECURITY über Direktprogrammierung auf ADABAS-Dateien zugegriffen werden. Der Datenbankzugang im Teilnehmerbetrieb, d.h. ohne die Sicherheitsmechanismen von UTM, stellt eine zusätzliche Schwachstelle für Anwendungen dar. Nach der Anmeldungsüberprüfung im BS2000 ruft der Benutzer ein Programm auf, das für ihn die Verbindung zur ADABAS-Datenbank herstellt. Das hiermit vorhandene Gefährdungspotential könnte durch den Einsatz der Kommandosprache SDF-A verringert werden, da dieses Produkt die Möglichkeit bietet, für jede Benutzerkennung den Umfang der verfügbaren Befehle zu beschränken. Wir haben deshalb für den Fall, daß der Zugriff auf ADABAS-Daten nicht kurzfristig durch Einsatz des Transaktionsmonitors UTM zu realisieren ist, gefordert, zumindest das Produkt SDF-A einzusetzen.

Das Senatsamt wird den Behörden SDF-A schrittweise zur Verfügung stellen. Der Einsatz von UTM wird dagegen nicht als geeignetes Mittel gesehen, die Sicherheit des Zugriffs auf Datenbanken zu erhöhen. Der Datenbankschutz liege nach Auffassung des Senatsamtes in NATURAL sowie in ADABAS.

3.7 Verlagerung der DVZ

Während der Sanierung des III. Bauabschnittes im Polizeipräsidium ist auch in den Räumen der Datenverarbeitungszentrale eine akute Asbestbelastung festgestellt worden. Um Gesundheitsgefährdungen der Mitarbeiter und Produktionsunterbrechungen aufgrund von Asbestfreisetzungen im Maschinensaal bzw. im Datenträgerarchiv auszuschließen, war die Auslagerung der DVZ bis zum Jahresbeginn 1992 unumgänglich.

Der Hamburgische Datenschutzbeauftragte ist dabei ständig über die Inhalte und den Stand der Maßnahmen zur Sicherstellung des Betriebes der DVZ während der Sanierung im Polizeipräsidium unterrichtet worden. Wir hatten durch Teilnahme an den Projektgruppensitzungen, Besichtigungen der neuen Räumlichkeiten und anlaßbezogene Gespräche mit verantwortlichen Mitarbeitern der DVZ und des Senatsamtes für den Verwaltungsdienst jederzeit die Möglichkeit, datenschutzrechtliche Anforderungen in die mit der Betriebsverlagerung verbundenen Aktivitäten einzubringen.

3.8 Nutzung von Privat-PC

Durch die zunehmende Funktionalität von tragbaren Geräten werden private PC häufig, insbesondere bei verwaltungsinternen Automatisierungsengpässen, zu dienstlichen Zwecken eingesetzt, sei es bei der täglichen Arbeit im Büro oder außerhalb der Dienstzeit zu Hause. Der Einsatz privater PC zu dienstlichen Zwecken begegnet erheblichen datenschutzrechtlichen Bedenken:

— Datenverarbeitung auf privaten Rechnern schränkt die Möglichkeit der speichernden Stelle erheblich ein, eine ordnungsgemäße Verarbeitung personenbezogener Daten zu gewährleisten, da Hardware und Software häufig auch zu privaten Zwecken genutzt werden.

— § 18 HmbDSG regelt das generelle Auskunftsrecht der Betroffenen gegenüber der speichernden Stelle. Dieses Recht ist bei Einsatz privater Datenträger in der Regel nur schwer zu gewährleisten.

— Die speichernde Stelle ist verpflichtet sicherzustellen, daß sich der Mitarbeiter im Rahmen der Nutzung privater PC der Kontrolle des Hamburgischen Datenschutzbeauftragten unterwirft. Dies kann zu Konflikten mit dem Eigentumsrecht des Mitarbeiters sowie dessen Recht auf Unversehrtheit der eigenen Wohnung führen.

— Eine Zugangskontrolle wird beim Einsatz von PC u.a. durch räumliche Maßnahmen wie Sicherheitsschlösser an der Zimmertür erreicht, um einen unbefugten Zugang zum Raum zu verhindern. Da beim Einsatz privater Hardware und Software zu dienstlichen Zwecken eine häusliche Nutzung nicht ausgeschlossen werden kann, ist eine Zugangskontrolle nicht ausreichend zu gewährleisten.

Um eine ordnungsgemäße Datenverarbeitung in angemessener Form sicherzustellen, sollte angesichts der aufgezeigten datenschutzrechtlichen Probleme

möglichst auf einen Einsatz privater PC zu dienstlichen Zwecken verzichtet werden. Die mit dem Einsatz zu dienstlichen Zwecken zusammenhängenden Fragen – mit der erforderlichen Differenzierung zwischen den verschiedenen Tätigkeitsbereichen wie Schulen, Polizei, Justiz – werden vom Hamburgischen Datenschutzbeauftragten in Abstimmung mit den Datenschutzbeauftragten des Bundes und der Länder weiter geklärt.

Falls der Einsatz privater PC zu dienstlichen Zwecken von der jeweiligen Stelle für unabdingbar gehalten wird, gelten hierfür die gleichen Sicherungsanforderungen, die auch an dienstliche Geräte zu stellen sind. Der Einsatz privater PC ist dabei nur vorübergehend vertretbar, bis dienstliche Geräte zur Verfügung stehen.

4. Telekommunikation

Angesichts der Entwicklung der Telekommunikation im privaten und im geschäftlichen Bereich und in der öffentlichen Verwaltung kommt der Sicherung des Fernmeldegeheimnisses und des Grundrechts auf unbeobachtete Kommunikation steigendes Gewicht zu. Allein in Hamburg gibt es 1,2 Millionen Telefon-Hauptanschlüsse. Davon sind z. Zt. 200.000 an digitale Vermittlungsstellen angeschlossen. Hinzu kommen zahlreiche an private Telekommunikationsanlagen angeschlossene Nebenstellen. Nimmt man die neuen Kommunikationstechniken – von Telefax bis ISDN – hinzu, wird deutlich, daß moderne Telekommunikation als fester Bestandteil zum täglichen Leben gehört.

Um so wichtiger ist es, daß die technische Ausgestaltung der Telekommunikationsnetze und -dienste datenschutzfreundlich erfolgt und technisch unvermeidliche „Restrisiken" durch rechtliche Regelungen begrenzt werden. Leider entspricht die technische und rechtliche Entwicklung nicht diesen Anforderungen:

— Durch die Digitalisierung der Telekommunikationsnetze und -dienste fallen immer mehr Verbindungsdaten (z.B. gewählte Anschlußnummern, Art und Dauer der Verbindung, bei Mobilfunk und Telefonkarten zusätzlich Standortkennungen) an, die sich zu „Datenspuren" oder „Kommunikationsprofilen" verdichten lassen (vgl. 7. TB, 3.5.2).

— Auch wenn in der rechtlichen Normierung des Datenschutzes in der Telekommunikation einige Fortschritte erzielt werden konnten, sind die Datenschutzregelungen im Fernmeldeanlagengesetz und im Postverfassungsgesetz sowie die Datenschutzverordnungen für die TELEKOM und für private Teledienst-Unternehmen noch erheblich verbesserungsbedürftig.

— Neben einer Verbesserung des rechtlichen Rahmens wird es in Zukunft angesichts der Liberalisierung und Entmonopolisierung des Fernmeldewesens verstärkt darauf ankommen, daß die Telekommunikations-„Verbraucher" den Datenschutz zu ihrer Sache machen und von den Anbietern von Telekommunikationsdiensten datenschutzfreundliche Lösungen verlangen. Die Datenschutzbeauftragten werden derartige Bemühungen nach Kräften

unterstützen. Ein „Mehr" an Wettbewerb um eine Verbesserung des Datenschutzes können sie nur begrüßen.

4.1 Datenschutzverordnungen zur Telekommunikation

Das Poststrukturgesetz vom 8. Juni 1989 verpflichtet die Bundesregierung dazu, für die TELEKOM und für die privaten Teledienst-Unternehmen Datenschutzverordnungen zu erlassen, die dem Grundsatz der Verhältnismäßigkeit, vor allem der Beschränkung der Erhebung und Verarbeitung auf das Erforderliche, und der Zweckbindung Rechnung tragen.

Erst im Dezember 1990 legte der Bundesminister für Post und Telekommunkation die ersten Verordnungsentwürfe vor. Deren Beratung stand von vornherein unter starkem Zeitdruck, da die bisherigen Rechtsverordnungen – insbesondere die Telekommunikationsordnung (TKO) – Ende Juni 1991 außer Kraft treten sollten. Am 8. März 1991 haben sich die Datenschutzbeauftragten von Bund und Ländern mit den Verordnungsentwürfen befaßt und eine Entschließung zum Datenschutz in der Telekommunikation verabschiedet. Die Bundesregierung ist den dort formulierten Forderungen nur in geringem Maß gefolgt.

Die nunmehr verabschiedeten Verordnungen erscheinen nicht nur in datenschutzrechtlicher Hinsicht als unzureichend, sondern in manchen Bestimmungen schlicht als unpraktikabel. Eine Nachbesserung ist unumgänglich.

4.1.1 TELEKOM-Datenschutzverordnung (TDSV)

Die TELEKOM-Datenschutzverordnung vom 24. Juni 1991 bildet die Rechtsgrundlage für die Datenerhebung und -verarbeitung durch die Deutsche Bundespost TELEKOM. Sie ist deshalb von besonderer Bedeutung, weil die TELEKOM in bestimmten Bereichen nach wie vor ein Fernmeldemonopol ausübt und der Bürger dort nicht die Möglichkeit hat, auf – datenschutzfreundlichere – Alternativanbieter auszuweichen. Um so bedauerlicher ist es, daß die TDSV weitgehend den Unternehmensinteressen der TELEKOM Vorrang vor dem „kommunikativen Selbstbestimmungsrecht" der Bürger einräumt.

Die Datenschutzbeauftragten des Bundes und der Länder hatten in ihrer Entschließung vom 8. März 1991 auf die wesentlichen Mängel der damaligen Verordnungsentwürfe hingewiesen und Forderungen zur Sicherung eines datenschutzrechtlichen Mindeststandards formuliert. Ein Vergleich dieser Forderungen mit den Regelungen der TDSV macht die wesentlichen datenschutzrechtlichen Defizite deutlich:

1. Verbindungsdatenspeicherung/Einzelentgeltnachweis

Entgegen der Forderung, alle Verbindungsdaten nach dem Ende der Verbindung zu löschen und nur die für die Entgeltabrechnung unabdingbaren Daten (als verkürzte Rufnummern oder in Summenform) zu speichern, dürfen gemäß § 6 Abs.1 TDSV sämtliche Verbindungsdaten von den Unternehmen vollständig gespeichert werden. § 6 Abs.2 enthält nur für die Sprachkommunikationsdienste ein Wahlrecht des Kunden über die Datenspeicherung für die Zeit nach der Versendung der Entgeltrechnung. In sämtlichen anderen Diensten dürfen die Verbindungdaten stets bis zu achzig Tagen nach Versendung der Entgeltrechnung gespeichert bleiben. Gemäß § 6 Abs. 6 darf die TELEKOM den Dienstanbietern, die sich dem Fernmeldegeheimnis unterwerfen und deren Kunden darin eingewilligt haben, die vollständigen (also unverkürzten) Verbindungsdaten zur Entgeltabrechnung übermitteln.

§ 6 Abs. 9 erlaubt es der TELEKOM, ihren Kunden ausführliche Einzelentgeltnachweise mit unverkürzten Rufnummern zur Verfügung zu stellen. Ausnahmen sind lediglich vorgesehen für Anrufe bei „Personen, Behörden und Organisationen, die selbst oder deren Mitarbeiter besonderen Verschwiegenheitsverpflichtungen unterliegen und die Beratungsaufgaben in sozialen oder kirchlichen Bereichen ganz oder überwiegend über Telefon abwickeln". Nur auf Antrag dieser Personen oder Institutionen muß die TELEKOM sicherstellen, daß die an diese gerichteten Anrufe aus den Nachweisen „nicht ersichtlich" sind.

Die Umsetzung dieser Regelung trifft auf erhebliche Auslegungsprobleme, da unklar ist, wer antragsberechtigt ist: Gehören zu den Antragsberechtigten auch solche Stellen, die zwar telefonische Beratung vornehmen, bei denen jedoch die persönliche Beratung überwiegt? Dürfen Stellen, die zwar ihre Beratungsaufgaben telefonisch wahrnehmen, bei denen aber die Beratungstätigkeit nur einen Teil ihrer Aufgaben einnimmt, Anträge stellen? Wie sind allgemeine Beratungsstellen zu qualifizieren, deren Beratungsspektrum nur teilweise den sozialen oder kirchlichen Bereich berührt? Gehören auch die in § 203 Abs. 1 Nr. 1, 2, 3, 5 und Abs. 2 StGB genannten Personengruppen zu den Antragsberechtigten, wenn sie beratend tätig werden? Ferner ist unklar, wie weit das Prüfungsrecht der TELEKOM geht, also ob und wie sie prüfen darf und muß, ob die Antragsteller zu dem Kreis der nach der Verordnung Berechtigten gehören und welche Informationen die Antragsteller beizubringen haben.

Die Umsetzung dieser Bestimmung dürfte ferner auf praktische Schwierigkeiten stoßen, da der Verordnungstext darauf abstellt, daß der Anruf bei solchen Einrichtungen nicht „ersichtlich" sein darf. Es reicht also nicht aus, entsprechende Anrufe ohne Nummernangabe auf dem Nachweis zu verzeichnen oder die bei Anrufen bei solchen Stellen aufgelaufenen Gebühren zwar in der Summe, nicht aber bei der Einzelaufstellung zu berücksichtigen. Bei beiden Verfahrensweisen wäre der Anruf nach wie vor „ersichtlich", was der Formulierung und dem Schutzzweck der Regelung zuwider liefe.

Ferner ist unklar, wie bei Anschlüssen von Personen, Organisationen und Behörden verfahren werden soll, die an betriebliche Nebenstellenanlagen angeschlossen sind, ob die Sperre einzelner Nebenstellennummern im Einzelentgeltnachweis möglich und inwieweit die Antragstellung direkt gegenüber der TELEKOM oder über die Stelle erfolgen muß, die die Nebenstellenanlage betreibt.

Die Ausnahmeregelung für Beratungsstellen tritt im übrigen gemäß § 16 erst zum 1. Juli 1992 in Kraft, während Einzelentgeltnachweise mit dem Inkrafttreten der TDSV am 1. Juli 1991 erstellt werden dürfen. Diese (zeitliche) Schutzlücke begegnet verfassungsrechtlichen Bedenken (siehe auch unter 3.).

2. Verbot von Kommunikationsprofilen

Anstatt die Erstellung von „Kommunikationsprofilen" generell auszuschließen, die Aussagen über das persönliche Telefonierverhalten des Bürgers und die Nutzung anderer Telekommunikationsdienste enthalten, erlaubt § 7 Abs. 2 zur Verhütung und Aufdeckung einer mißbräuchlichen Inanspruchnahme von Mobilfunknetzen praktisch die vorsorgliche Durchrasterung sämtlicher Verbindungsdaten. Sämtliche in diesen Netzen erhobenen Verbindungsdaten sollen regelmäßig in der Weise verarbeitet und genutzt werden dürfen, daß aus dem Gesamtbestand aller Verbindungsdaten die Daten derjenigen Verbindungen ermittelt werden, bei denen ein Verdacht auf Mißbrauch von Fernmeldeanlagen oder eine mißbräuchliche Inanspruchnahme von Telekommunikationsdiensten begründet wird.

Durch diese Auswertungsmöglichkeit werden die – aufgrund der mitgespeicherten Standortkennungen besonders sensiblen – Verbindungsdaten von Mobilfunkteilnehmern pauschal zu einer Durchrasterung freigegeben. Die – auch ohne konkreten Verdacht zulässige – Auswertung nach Standortkennungen und Zielrufnummern kommt der Erstellung von Kommunikations- und Bewegungsprofilen nahe.

3. Rufnummernanzeige

Während nach § 9 Abs. 1 die Rufnummernanzeige ab sofort angeboten werden darf, soll die fallweise Unterdrückung der Rufnummernanzeige durch den Anrufer erst zum 1. Januar 1994 möglich sein. Der Angerufene kann auch nach dem Auslaufen der Übergangsfrist die Rufnummernanzeige nicht fall- oder zeitweise abschalten; er muß sich vielmehr zwischen Anschlüssen mit oder ohne Anzeige entscheiden. Es steht in direktem Widerspruch zu den im „Volkszählungsurteil" des Bundesverfassungsgerichts formulierten Grundsätzen, daß neue – mit Informationseingriffen verbundene – technische Möglichkeiten genutzt werden, ehe die erforderlichen technischen Mittel zur (rechtlich unabdingbaren) Begrenzung der Eingriffe in das informationelle Selbstbestimmungsrecht verfügbar sind.

4.1.2 Teledienst-Unternehmen-Datenschutzverordnung (UDSV)

Die Bundesregierung hat dem Bundesrat im Juli 1991 aufgrund der Verpflichtung des § 14a Abs.2 Fernmeldeanlagengesetz den Entwurf einer Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (Teledienstunternehmen-Datenschutzverordnung – UDSV), zugeleitet. Da sich der Regelungsinhalt praktisch mit dem der TDSV deckt, wird für die Bewertung auf die Ausführungen unter 4.1.1 hingewiesen.

In den Beratungen des Bundesrates haben sich verschiedene Bundesländer – auch Hamburg – wesentliche der von den Datenschutzbeauftragten und von sozialen Organisationen und den Kirchen vorgebrachten Forderungen zu eigen gemacht. Leider ist der Bundesrat diesen Forderungen mit seinem Beschluß vom 27. September 1991 nur zum Teil gefolgt.

Erfreulich ist, daß in privaten Telefondiensten nunmehr erst dann ausführliche Einzelentgeltnachweise mit Angabe der angerufenen Telefonnummern eingeführt werden dürfen, wenn Anrufe bei Beratungsinstitutionen nicht darin aufgeführt werden.

Eine weitere Verbesserung besteht darin, daß nach dem Willen des Bundesrates die Verbindungsdaten (hierzu gehören die angerufenen Telefonnummern, Zeitpunkt und Dauer der Verbindung) in der Verordnung abschließend aufgezählt werden und das Bundesministerium für Post und Telekommunikation nicht die Speicherung zusätzlicher Daten zulassen darf.

Bedauerlicherweise hat der Bundesrat aber den Kreis der antragsberechtigten Beratungseinrichtungen, deren Nummern nicht auf den Einzelentgeltnachweisen erscheinen, nicht unabhängig davon festgelegt, ob die Einrichtungen ihre Beratungsaufgabe überwiegend über Telefon abwickeln. Zu bedauern ist auch, daß die Gültigkeit der Verordnung nicht zeitlich begrenzt worden ist, wie dies der Innenausschuß des Bundesrates vorgeschlagen hatte. Eine derartige Befristung hätte dem Bundesrat die Möglichkeit gegeben, auf Grundlage der bis Ende 1993 erworbenen Erfahrungen erneut über die zusätzlich erforderlichen Datenschutzmaßnahmen zu entscheiden und dabei den Umfang der Verbindungsdaten bereits bei der Speicherung zu reduzieren.

Es ist zu hoffen, daß die Bundesregierung der Aufforderung des Bundesrates folgt, die für die Post geltende TELEKOM-Datenschutzverordnung (TDSV) auf den Stand der UDSV zu bringen, damit auch der Telefonkunde der TELEKOM in den Genuß eines verbesserten Datenschutzes kommt.

4.2 Fernmeldegeheimnis

Eingriffe in das grundgesetzlich geschützte Fernmeldegeheimnis (Art.10 GG) müssen auf das unerläßliche Maß beschränkt und dürfen insbesondere nicht schon im Bereich der Bagatellkriminalität zugelassen werden, wie § 12 Fernmeldeanlagengesetz (FAG) dies zuläßt. Danach kann in strafgerichtlichen Untersuchungen der Richter und bei Gefahr im Verzug auch die Staatsanwaltschaft Auskunft über den Fernmeldeverkehr verlangen.

Diese Regelung hat im Zuge der technischen Entwicklung eine verfassungsrechtlich bedenkliche neue Qualität erhalten, da sie nunmehr auch die bei Einsatz neuer Kommunikationstechniken anfallenden Abrechnungs-, Verbindungs-, Nutzungs- und Inhaltsdaten umfaßt. Die Eingriffsmöglichkeiten in das Fernmeldegeheimnis im Rahmen der Strafverfolgung sollten – schon aus Gründen der Normenklarheit – in der Strafprozeßordnung unter engen Voraussetzungen und Beschränkungen abschließend geregelt werden.

Es ist erfreulich, daß der Bundesrat bei seiner Befassung mit der UDSV (vgl. 4.1.2) auch eine Entschließung zum § 12 FAG angenommen hat, in der dies datenschutzrechtliche Anliegen aufgegriffen wird. Unter Beachtung des Bestimmtheitsgebotes sei der Gesetzgeber gehalten, eine Neuregelung vorzunehmen, mit der die Eingriffsmöglichkeiten – abgestimmt mit den Vorschriften der Strafprozeßordnung – unter engen Voraussetzungen und abschließend festgelegt werden. Noch steht die Umsetzung dieser Entschließung aus.

Dagegen sollen mit dem Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG – Bundestagsdrs. 12/989) die Überwachungsbefugnisse noch ausgeweitet werden (siehe 19.1.1). Nach dem im Gesetzentwurf vorgesehenen § 12a FAG soll die Überwachung und Aufzeichnung des Fernmeldeverkehrs angeordnet werden können, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leben, Leib oder Freiheit einer Person erforderlich ist. Der Bundesbeauftragte für den Datenschutz hat in seiner Stellungnahme zu diesem Gesetzentwurf treffend bemerkt, daß aufgrund dieses Vorschlags noch vor einem hinreichenden Tatverdacht eine Überwachung bereits angeordnet werden dürfte, um der Gefahr einer drohenden Ohrfeige zu begegnen.

4.3 Regelungen für die Verwaltung

Leider ist festzustellen, daß es immer noch keine verbindlichen Regelungen über die Verarbeitung der Daten gibt, die bei der Telekommunikation in der Verwaltung erhoben und gespeichert werden, obwohl mit der fortschreitenden Digitalisierung des Behördenfernsprechnetzes auch hier solche Daten verstärkt entstehen. Bereits Mitte 1991 gab es im hamburgischen Behördennetz elf ISDN-fähige Vermittlungszentralen und 60 ISDN-fähige Telefonanlagen im schulischen Bereich; auf längere Sicht wird auch das Behördennetz vollständig auf ISDN-Basis gestellt werden.

Bis auf ein „Diskussionspapier" aus dem Senatsamt für den Verwaltungsdienst vom Mai 1991, das sich auf Überschriften beschränkt, sind uns keine Informationen darüber zugegangen, wie der Umgang mit Telekommunikationsdaten in Zukunft inhaltlich geregelt werden soll. Insbesondere steht das Ergebnis der vom Senat zugesagten Prüfung, inwieweit unseren Anregungen im 9. TB (4.2.2) gefolgt wird, noch aus. Zu befürchten ist also, daß auch bis Ende 1991 die Telekommunikationsrichtlinie nicht fertiggestellt sein wird.

Es ist zu hoffen, daß die inzwischen begonnenen Gespräche mit den Spitzenorganisationen des Öffentlichen Dienstes über eine entsprechende Vereinbarung nach § 94 HmbPersVG zügig zu einem datenschutzrechtlich befriedigenden Abschluß gebracht werden.

4.4 Teilnehmerverzeichnisse auf CD-ROM

Neben die herkömmlichen Telefonbücher sind in den letzten Jahren Teilnehmerverzeichnisse getreten, die sich automatisiert erschließen lassen. Bereits

seit längerem wird über den Bildschirmtextdienst der TELEKOM ein bundesweites Elektronisches Telefonbuch (ETB) angeboten, in das alle Teilnehmereinträge aus den amtlichen Telefonbüchern übernommen worden sind. Automatisiert erschließen lassen sich ebenfalls Teilnehmerverzeichnisse, die neuerdings auf CD-ROM angeboten werden.

Bei der CD-ROM handelt es sich um ein sogenanntes „optisches Speichermedium" in Form einer Compact-Disk, wie sie für Tonaufnahmen weit verbreitet sind. Im Unterschied zu magnetisierten Datenträgern lassen sich die einmal auf CD-ROM gespeicherten Daten nicht mehr verändern (ROM steht für „Read Only Memory"); auch ihre Löschung ist mit den verbreiteten CD-ROM-Laufwerken nicht möglich, da es sich üblicherweise um reine Abspielgeräte handelt. Auf einer CD-ROM können derzeit bis zu 650 Mega-Byte Daten (dies entspricht etwa 30.000 Schreibmaschinenseiten) gespeichert und in Sekundenschnelle wiedergefunden werden.

Bereits seit 1990 bietet ein Verlag bundesweite Telefonverzeichnisse auf CD-ROM zum Einzelverkauf und im Abonnement an. Die Deutsche Postreklame hat ein Telefax-Teilnehmerverzeichnis auf CD-ROM herausgegeben und bereitet ebenfalls ein bundesweites Telefonverzeichnis auf CD-ROM vor.

Die datenschutzrechtliche Problematik derartiger Verzeichnisse liegt weniger darin, daß sie eine – auch überregionale – Suche zulassen. Problematisch ist vielmehr, daß die Datensammlungen anders als papierne Telefonbücher auch über andere Merkmale als den Namen erschlossen werden können. Damit wird es ermöglicht, Teilnehmer z.B. anhand ihrer Anschrift oder ihres Berufs zu identifizieren oder (auch wenn dies von den Herstellern bislang nicht unterstützt wird) von der Telefonnummer auf den Teilnehmer zu schließen. Besonders die Möglichkeit einer „umgekehrten Suche" begegnet großen Bedenken, denn in einer Vielzahl von Fällen beschränken Menschen die Preisgabe einer Kontaktmöglichkeit aus verständlichen Gründen auf ihre Telefonnummer.

Brisant wird diese Möglichkeit auch im Zusammenhang mit den geplanten detaillierten Einzelentgeltnachweisen und mit der Rufnummernanzeige (vgl. 4.1.1), denn von der Rufnummer kann mit dieser Technik grundsätzlich auf den Teilnehmer geschlossen werden. Die Datenschutzrelevanz der Telefonnummer wird damit deutlich erhöht.

Besonders problematisch ist, daß bisher erstellte Telefonbuch-CD's auf dem Zwangseintrag in das amtliche Fernsprechverzeichnis beruhen. Angesichts der fehlenden Löschungs- und Änderungsmöglichkeiten halten wir diese Datensammlungen für unzulässig. Zwar haben seit dem 1. Juli 1991 Telefonkunden die Möglichkeit, ohne Begründung dem Eintrag in Telefonteilnehmerverzeichnisse zu widersprechen, doch weist die TELEKOM nicht darauf hin, daß die Daten zukünftig eben nicht nur im herkömmlichen Telefonbuch, sondern auch auf CD-ROM und im ETB gespeichert und übermittelt werden sollen; die Information ist deshalb unzureichend.

Aufgrund einer Anfrage aus der Polizei hatten wir uns auch mit der Frage auseinanderzusetzen, ob Telefonbuch-CD's im Rahmen polizeilicher Arbeit genutzt werden dürfen. Wir haben der Behörde für Inneres mitgeteilt, daß wir die Nutzung deshalb für unzulässig halten, weil es sich aus den genannten Gründen um eine – zumindest bislang – unzulässige Datensammlung handelt. Sobald Telefonkunden auf Grundlage einer ausreichenden Information die Gelegenheit hatten, der Aufnahme in Teilnehmerverzeichnisse zu widersprechen, wäre dieses Ergebnis noch einmal zu überprüfen.

Bedenklich ist in diesem Zusammenhang ferner, daß die TELEKOM offenbar die in der TELEKOM-Datenschutzverordnung (TDSV) vorgesehene Möglichkeit einschränken will, der Eintragung in Teilnehmerverzeichnisse differenziert zu widersprechen. Die TELEKOM geht davon aus, daß der Telefonkunde nur der Eintragung in sämtliche Verzeichnisse widersprechen könne; dagegen verpflichtet § 10 Abs. 3 TDSV die TELEKOM, auf Verlangen des Kunden die Eintragung in öffentliche Kundenverzeichnisse ganz oder teilweise zu unterlassen. Diese Vorschrift ist im Sinne der Wahrung des Grundsatzes, selbst über die Verwendung seiner Daten zu bestimmen, und im Sinne des Verhältnismäßigkeitsgrundsatzes dahingehend auszulegen, daß man sich zwar in ein Telefonbuch eintragen läßt, aber der – aus den genannten Gründen problematischen – Aufnahme in elektronische Teilnehmerverzeichnisse im Bildschirmtext und auf CD-ROM widersprechen kann. Der Bundesbeauftragte für den Datenschutz ist gebeten worden, diese Problematik gegenüber der TELEKOM zu klären.

Einzelne Probleme des Datenschutzes im öffentlichen Bereich

5. Rundfunk/Neue Medien

5.1 Mediendienstestaatsverträge

Im Berichtszeitraum wurde mit der Unterzeichnung des Staatsvertrages über den Rundfunk im vereinten Deutschland (Rundfunkgesamtstaatsvertrag) der rechtliche Rahmen für Rundfunk, Fernsehen und den Bildschirmtext fortgeschrieben. Die Neufassung des Staatsvertrages über den Norddeutschen Rundfunk steht unmittelbar bevor. Bei den Beratungen der Staatsverträge haben wir darauf hingewirkt, daß diese auch den datenschutzrechtlichen Erfordernissen gerecht werden. Dieses Ziel konnte weitgehend erreicht werden (siehe auch 1.2.2).

5.1.1 Rundfunkgesamtstaatsvertrag

Der Rundfunkgesamtstaatsvertrag umfaßt den Rundfunkstaatsvertrag, den ZDF-Staatsvertrag, den Rundfunkgebühren- und den Rundfunkfinanzierungs-

staatsvertrag und den Bildschirmtextstaatsvertrag. Die folgende Darstellung beschränkt sich auf Neuregelungen mit Bezug zum Datenschutz:

— Der Rundfunkstaatsvertrag enthält mit dem § 28 nunmehr eine eigene Datenschutzvorschrift für den privaten Rundfunk. Die Regelungen gelten ausdrücklich auch für solche Daten, die nicht in Dateien verarbeitet werden.

  Die Verarbeitung personenbezogener Daten über die Inanspruchnahme einzelner Programmangebote ist nur zulässig, soweit dies für die Bereitstellung der Programme und die Abrechnung von Entgelten erforderlich ist. Die Abrechnungsdaten dürfen Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter, vom Teilnehmer in Anspruch genommener Programmangebote nicht erkennen lassen. Abrechnungs- und Verbindungsdaten dürfen nicht an Dritte übermittelt werden. Dies gilt nicht für die Übermittlung von Abrechnungsdaten an den Rundfunkveranstalter zum Zwecke der Einziehung einer Forderung, wenn diese auch nach Mahnung nicht beglichen wird. Verbindungsdaten sind nach Ende der jeweiligen Verbindung, Abrechnungsdaten dagegen dann zu löschen, wenn sie für Zwecke der Abrechnung nicht mehr erforderlich sind.

  Ferner schreibt die Datensicherungsvorschrift des § 28 Abs. 6 vor, daß Teilnehmer nur durch eindeutige und bewußte Handlungen Daten übermitteln können, also heimliche Datenerhebungen unzulässig sind. Ferner enthält diese Vorschrift – anders als z.B. das neue Hamburgische Datenschutzgesetz – das sachgerechte Gebot zur Anpassung der Maßnahmen an den Stand der Technik.

  Diese Regelungen stehen in einem erfreulichen Kontrast zu den weitergehenden Verarbeitungsbefugnissen bei der Telekommunikation (vgl. 4).

— Im ZDF-Staatsvertrag nehmen die Datenschutzbestimmungen einen breiten Raum ein. Hervorzuheben sind die Bestimmungen zur Datenverarbeitung für journalistisch-redaktionelle Zwecke. Da auf die für solche Zwecke verarbeiteten Daten im Hinblick auf die Freiheit der Berichterstattung das allgemeine Datenschutzrecht nur begrenzt anwendbar ist, sind Regelungen notwendig, die den Besonderheiten dieses Bereichs Rechnung tragen. Die Vorschriften im ZDF-Staatsvertrag bilden einen tragfähigen Kompromiß zwischen der Rundfunkfreiheit (Art. 5 GG) und dem Recht auf informationelle Selbstbestimmung.

  Rechtlich und praktisch bedeutsam ist die Verpflichtung der Medien, Gegendarstellungen, Widerrufe usw. zu den gespeicherten Daten zu nehmen und die Daten stets nur gemeinsam mit diesen zu übermitteln. Neu ist auch ein Auskunftsrecht von Betroffenen über die einer Berichterstattung zugrunde liegenden Daten und ihr Recht, eine Berichtigung unrichtiger Daten oder die Hinzufügung einer eigenen Darstellung von angemessenem Umfang zu verlangen.

Für die nicht journalistisch-redaktionelle Datenverarbeitung des ZDF gilt das Datenschutzgesetz von Rheinland-Pfalz. Die Einhaltung der Datenschutzbestimmungen wird von einem Datenschutzbeauftragten des ZDF kontrolliert, der an die Stelle des Landesbeauftragten für den Datenschutz tritt.

— Der Rundfunkgebührenstaatsvertrag regelt nunmehr, welche Daten für die Rundfunkgebühren erhoben und verarbeitet werden dürfen. Diese Daten dürfen nur zweckgebunden verarbeitet werden. Die Einholung von Melderegisterauskünften ist nur in Einzelfällen zulässig, soweit tatsächliche Anhaltspunkte vorliegen, daß Rundfunkgeräte betrieben werden, die vorschriftswidrig nicht angemeldet sind.

  Problematisch könnte die Übermittlung von Daten solcher Personen sein, die von der Rundfunkgebührenpflicht befreit sind. Die Datenschutzbeauftragten werden die Erstellung von Rechtsverordnungen, die dies näher regeln sollen, kritisch begleiten.

— Im Bildschirmtextstaatsvertrag sind die Datenschutzbestimmungen unverändert geblieben. Unserer Anregung, die Bestimmungen ausdrücklich auch auf besondere Bildschirmtextdienste (z.B.Mailbox-Netze) zu erstrecken, wurde nicht gefolgt. Zugesagt wurde aber, diese Thematik weiter zu prüfen.

5.1.2 NDR-Staatsvertrag

Aufgrund der Debatte darüber, ob Mecklenburg-Vorpommern sich am NDR beteiligt, hat sich die Neufassung des Staatsvertrages über den Norddeutschen Rundfunk verzögert. Da der alte NDR-Staatsvertrag keine datenschutzrechtlichen Regelungen enthielt und solche Regelungen auch im Hamburgischen Datenschutzgesetz als Sitzlandregelung nur begrenzt für den NDR getroffen wurden, war die datenschutzrechtliche Ergänzung überfällig.

Die Datenschutzvorschriften im mittlerweile unterzeichneten neuen NDR-Staatsvertrag entsprechen weitgehend den entsprechenden Bestimmungen des neuen ZDF-Staatsvertrags (vgl. 5.1.1) und genügen wie diese den datenschutzrechtlichen Anforderungen. Sie regeln die Datenverarbeitung zu journalistisch-redaktionellen Zwecken und werden – bezüglich der Datenschutzkontrolle – an die Stelle des § 31 HmbDSG treten; hinsichtlich der sonstigen Datenverarbeitung durch den NDR sind auch weiterhin die Vorschriften des Hamburgischen Datenschutzgesetzes anzuwenden.

5.2 Offener Kanal Hamburg

Im Berichtszeitraum haben wir uns über datenschutzrechtliche Probleme des Offenen Kanals Hamburg informiert. Der Offene Kanal gibt gemäß § 30 Abs.2 Hamburgisches Mediengesetz einzelnen Bürgern und gesellschaftlichen Gruppen die Gelegenheit, eigene Beiträge in Rundfunk und Fernsehen zu verbreiten.

Beim Offenen Kanal handelt es sich um eine rechtlich und organisatorisch unselbständige Einrichtung der Hamburgischen Anstalt für neue Medien (HAM), auf die die Vorschriften des Hamburgischen Datenschutzgesetzes anzuwenden sind. Die datenschutzrechtliche Verantwortung der HAM beschränkt sich auf den programmtechnischen Rahmen; für die inhaltliche Gestaltung der Beiträge sind – auch datenschutzrechtlich – die jeweiligen Programmveranstalter verantwortlich.

Für die Wahrnehmung seiner Aufgaben führt der Offene Kanal eine Reihe von Datensammlungen. So besteht eine Kartei der Benutzer technischer Einrichtungen und der Veranstalter von Sendungen. Diese Kartei enthält neben den Such- und Sortiermerkmalen (Name, Anschrift, Telefonnummer) häufig auch die Nummer und das Ausstellungsdatum des Personalausweises. Ferner werden auf den Karteikarten chronologisch die Benutzeraktivitäten verzeichnet (z.B. Beratungs- und Informationsgespräche, Ausleihe von Geräten, Sendetermine und Sendethemen). Diese Kartei, auf die nur Mitarbeiter des Offenen Kanals Zugriff haben, ist datenschutzrechtlich zulässig, denn die gespeicherten Daten sind für den Betrieb des Offenen Kanals erforderlich (z.T. ergibt sich die Notwendigkeit der Speicherung schon aus der Aufzeichnungspflicht des § 30 Abs.7 HmbMedienG).

Es sollte in Zukunft dafür Sorge getragen werden, daß die gespeicherten Daten regelmäßig auf die Erforderlichkeit der weiteren Speicherung überprüft und nicht mehr erforderliche Daten gelöscht werden.

5.3 Datenschutzregelungen für Neue Medien

Die neuen Datenschutzverordnungen für das Fernmeldewesen (vgl. 4.1) enthalten auch einige Regelungen über Dienste, die als „Neue Medien" zu qualifizieren sind (z.B. Bildschirmtext, Fernmeß- und Fernwirkdienste, Nachrichtenübermittlungssysteme mit Zwischenspeicherung). Der Hamburgische Datenschutzbeauftragte hat wiederholt darauf hingewiesen, daß sich die Regelungskompetenz des Bundes auf den Netzbereich, also auf die Bereitstellung der technischen Infrastruktur beschränkt, während die Regelung des Nutzungsbereichs Länderangelegenheit ist (vgl. 7. TB, 3.5.2.8). Leider hat es seitens der Länder – bis auf den Bildschirmtextstaatsvertrag und die Regelungen zum privaten Rundfunk – bisher keine nennenswerten Aktivitäten auf diesem Gebiet gegeben.

Abgesehen von der Kompetenzlage wäre eine Länderinitiative auch unter materiell-rechtlichen Gesichtspunkten sicher von Vorteil, wie z.B. ein Vergleich der bundes- und landesrechtlichen Regelungen über die Verbindungsdatenspeicherung zeigt. Während die TELEKOM-Datenschutzverordnung (TDSV) und die Teledienst-Unternehmen Datenschutzverordnung (UDSV) den Dienstanbietern die Verbindungsdatenspeicherung weitgehend gestatten, schreibt der Rundfunkstaatsvertrag der Länder vor, die Verbindungsdaten im privaten Rundfunk nach Beendigung der Verbindung zu löschen.

Angesichts der zunehmenden Differenzierung der „Neuen Medien" wäre es zu begrüßen, wenn die Länder sich entschließen könnten, einen Länderstaatsvertrag über den Datenschutz bei neuen Medien abzuschließen, um auch hier den erforderlichen Datenschutz zu gewährleisten. Andernfalls müßten die notwendigen Regelungen in den jeweiligen Sachzusammenhängen in den Landesgesetzen getroffen werden, wie wir dies für die überfällige Regelung für Fernmeß- und Fernwirkdienste (Temex) seit längerem vorgeschlagen haben.

6. Sozialwesen

6.1 Projekt Sozialhilfe-Automation (PROSA)

Das Projekt wurde im Anschluß an den Sachstand im letzten Bericht (9.TB, 4.1.1) weiter vorbereitet und von der Lenkungsgruppe begleitet. Der Ablaufplan wurde – trotz zeitweiliger technischer Probleme – im wesentlichen eingehalten. Anfang Oktober 1991 hat der Modellversuch im Bezirksamt Eimsbüttel begonnen.

Die PROSA-Datenschutzkonzeption wurde unter unserer Beteiligung stetig fortentwickelt. Zu der Anonymisierungsstrategie, die für die statistischen Auswertungen des Datenbestandes erforderlich ist, existiert bislang lediglich ein noch unabgestimmtes Papier der Behörde für Arbeit, Gesundheit und Soziales (BAGS).

Für gesundheitlich begründete Mehrbedarfe sind zwischenzeitlich Fallgruppen gebildet worden, so daß ein Rückschluß auf konkrete Einzeldiagnosen nur eingeschränkt möglich ist.

Im Berichtszeitraum waren jedoch wiederholt Diskussionen um die Verarbeitung der nachfolgend genannten Datenarten zu führen, die teilweise sehr mühsam waren.

6.1.1 Dauer der Arbeitslosigkeit

Bisher war angenommen worden, die BAGS hätte im wesentlichen akzeptiert, daß eine Datenerhebung allein zu statistischen/planerischen/politischen Zwecken ohne spezielle Rechtsgrundlage unzulässig ist (9. TB, 4.1.1.2). Auf derartige Erwägungen stellte die BAGS aber zunächst ab, um die Erhebung der Dauer der Arbeitslosigkeit zu begründen. Der nächste Begründungsversuch stützte sich dann auf die These, die Dauer der Arbeitslosigkeit sei maßgeblich für die Überprüfung, ob eine Arbeitsaufnahme zumutbar sei. Dem haben wir entgegengehalten, daß es datenschutzrechtlich im Rahmen von PROSA darauf ankommt, ob die Dauer der Arbeitslosigkeit ein Kriterium für Sozialhilfeleistungen ist.

Die BAGS legte daraufhin anhand eines neuen Konzepts differenziert dar, daß die nähere Kenntnis der Dauer der Arbeitslosigkeit die Grundlage für unterschiedliche Formen der Hilfe zur Arbeit sei. Dieser Ansatz beruht wesentlich

auf dem Grundsatz der Subsidiarität der Sozialhilfe. Diesem Ansatz habe ich mich angeschlossen. Es muß in der Tat möglich sein, zu prüfen, ob der Hilfesuchende andere vorrangige Leistungen in Anspruch nehmen kann. Über die Umsetzung dieses Ansatzes wird noch diskutiert.

Diese Diskussion macht zugleich deutlich, daß die Einschätzung des Senates (Senatsdrucksache Nr.588 vom 30.April 1991, S.4, 2.Abs.) unzutreffend ist, wir würden den Umfang der notwendigerweise zu erhebenden Daten unterschätzen. Richtig ist vielmehr, daß eine stichhaltige fachliche Begründung einer Datenverarbeitung notwendige Grundlage für eine verbindliche datenschutzrechtliche Zulässigkeitsprüfung ist.

6.1.2 Ursachen der Bedürftigkeit

Hier konnte durchgesetzt werden, daß die Merkmale „Folgen einer Ehescheidung" und „Häusliche Bindung" entfallen. Im übrigen war grundsätzlich zu akzeptieren, daß die Kenntnis der Ursachen erforderlich ist für eine individuelle Hilfestellung.

6.1.3 Empfängerstatistik

Es wurde erreicht, daß die Erhebung der schulischen/beruflichen Qualifikation und der zuletzt ausgeübten Tätigkeit bei bestimmten Hilfeempfängergruppen unterbleibt, für die dieses Merkmal nicht hilferelevant ist. Hierzu gehören Kinder unter 18, Senioren über 60 und Erwerbsunfähige, da für sie eine Arbeitsaufnahme nicht zumutbar ist. Wir haben darauf hingewiesen, daß es daneben noch weitere von dieser Erhebung auszunehmende Empfängergruppen gibt, nämlich Schwangere, Empfänger von Hilfe in besonderen Lebenslagen und Hilfeempfänger mit Regelsatzerhöhungen wegen Betreuung oder Betreuung durch Dritte. Dieser Einschätzung hat die BAGS auch nicht mehr widersprochen. Allerdings wollte die BAGS die Erhebung in jedem Einzelfall der Entscheidung des Sachbearbeiters überlassen. Demgegenüber haben wir darauf bestanden, daß programmgesteuert die Abfrage bereits unterbleibt, wenn der Hilfeempfänger einer der insoweit ausgenommenen Empfängergruppen angehört.

6.1.4 Erfolgsstatistik

Hier konnte zunächst Einvernehmen darüber erzielt werden, daß die Gründe für die Beendigung des Sozialhilfebezuges durch eine anonyme Geschäftsstatistik ersetzt wird, die außerhalb des automatisierten Verfahrens geführt wird. Später versuchte die BAGS zwar, von diesem Ergebnis wieder abzurücken. Letztlich wurde dann aber akzeptiert, daß diese Daten für die Hilfeleistung irrelevant und daher nicht zu erheben sind.

6.1.5 Ausländer/Staatsangehörigkeit

Zur Staatsangehörigkeit hatte die BAGS zeitweilig die These vertreten, es bedürfe der Erhebung dieses Datums, damit man es dann der Ausländerbe-

hörde übermitteln könne. Letztlich hat sich auf unser Betreiben aber doch die Einsicht durchsetzen können, daß es nur der Erhebung bestimmter Statusgruppen bedarf. Solche Statusgruppen sind zum einen

— De-facto-Flüchtlinge (abgelehnte, aber nicht abgeschobene Asylbewerber),

— Asylbewerber, über deren Antrag noch nicht entschieden wurde, und

— abgelehnte Aussiedler.

Für diese Empfängergruppen gelten gemäß § 120 BSHG Einschränkungen des Leistungsanspruchs.

Zum anderen können auch der Status

— Aussiedler mit Vertriebenenausweis und

— Asylberechtigte/Kontingentflüchtlinge

zulässigerweise erhoben werden, da Angehörige dieser Gruppe einige besondere Leistungsansprüche haben.

Gegenwärtig noch offen ist die Erfassung der Zugehörigkeit zur Statusgruppe „Ausländer, für die zwischenstaatliches oder internationales Recht gilt". Die BAGS hat zuletzt darauf abgestellt, daß bei diesen Personen die grundsätzlich erforderliche Meldung an die Ausländerbehörde gemäß § 71 Abs.2 SGB-X nicht erforderlich ist, da der Sozialhilfebezug allein nicht zur Beendigung des Aufenthalts führen kann. Die Erhebung der Statuszugehörigkeit würde daher überflüssige Meldungen vermeiden helfen. Bisher ist jedoch bei PROSA kein zusätzlicher Teilbereich vorgesehen, der unabhängig von Sozialhilfeleistungen die Datenverarbeitung hinsichtlich Meldungen nach dem Ausländergesetz umfaßt. Nur wenn diese Erweiterung vorgenommen wird, wäre hier auch der Ausschluß von Meldungen festzulegen. Aus der Sicht des Datenschutzes wäre es vorzuziehen, wenn die Fragen zum Ausländergesetz, für die federführend die Behörde für Inneres zuständig ist, insgesamt getrennt von PROSA behandelt würden.

6.1.6 Künftige Aktenführung

Auch nach Einführung des automatisierten Verfahrens werden in den Sozialdienststellen noch Akten zu führen sein. Über die Art dieser Aktenführung – insbesondere die Akteninhalte – konnte Einvernehmen erzielt werden. Zu den aktenmäßig geführten Unterlagen gehören überwiegend solche, die zum Beleg der gemachten Angaben dienen, sowie Daten, die nicht automatisiert gespeichert werden dürfen (z.B. medizinische Daten). Aufbewahrungsfristen werden insoweit noch zu regeln sein.

Kurz vor Redaktionsschluß haben wir allerdings völlig überraschend erfahren, daß die geplante Umstellung der Aktenführung an der Haushaltsabteilung der BAGS zu scheitern droht, da diese die Kosten für die Ergänzung/Veränderung eines Vordrucks nicht zu tragen bereit ist. Offenbar wird dort nicht berücksichtigt, daß der Senat ausweislich der amtlichen Begründung zum Hamburgischen Datenschutzgesetz (Bürgerschaftsdrucksache 13/3282, A 3.) bereits anerkannt hat, daß ein moderner verfassungsgemäßer Datenschutz mit einer Steigerung des verwaltungsmäßigen Aufwandes einschließlich entsprechender Kostensteigerungen verbunden ist. Dieser Erkenntnis hat die BAGS – auch – im Rahmen ihrer Haushaltsplanungen Rechnung zu tragen.

6.2 Praktizierter Sozialdatenschutz in den Sozialdienststellen

Wie bereits gelegentlich in der Vergangenheit haben wir auch im Berichtszeitraum unangekündigt Sozialdienststellen aufgesucht, um vor Ort einen Eindruck gewinnen zu können, inwieweit die äußeren Bedingungen der dortigen Arbeit die Wahrung des Sozialgeheimnisses gewährleisten. In einem Fall ging diesem Besuch eine konkrete Beschwerde voraus; im anderen Fall handelte es sich um eine zufällige Stichprobe.

Da diese stichprobenartigen Prüfungen aber kein annähernd repräsentatives Bild der örtlichen Verhältnisse in den Sozialdienststellen vermitteln können, haben wir zu verschiedenen Punkten, deren Relevanz sich teilweise aus den örtlichen Prüfungen ergab, eine Umfrage bei allen 28 Sozialdienststellen durchgeführt.

Im Ergebnis kann danach festgestellt werden, daß zwar der Sozialdatenschutz weitgehend nach Kräften realisiert wird. Gleichwohl sind zur Realisierung des Grundrechts auf informationelle Selbstbestimmung weiterhin Verbesserungen möglich und notwendig. Die betroffenen Dienststellen haben wir um entsprechende Maßnahmen gebeten.

Bemängelt haben wir vor allem, daß teilweise noch immer in Doppelzimmern zwei Hilfeempfänger gleichzeitig betreut werden, ohne daß beide sich damit ausdrücklich einverstanden erklärt haben. Eine Verbesserung dieser Situation ist allerdings durch die Ausweitung des Einzelzimmerbestandes zu erwarten, der im Zuge der u.a. mit PROSA verbundenen baulichen Maßnahmen erfolgt. Daneben verhält es sich leider bei der Betreuung in Einzelzimmern teilweise so, daß Verbindungstüren zu benachbarten Betreuungsräumen geöffnet bleiben, ohne daß die Hilfeempfänger sich damit ausdrücklich einverstanden erklärt haben. Auch diese Verfahrensweise erfüllt den Anspruch auf ungestörte Einzelberatung nicht, wie er vom Senat bereits anerkannt wurde (vgl. z.B. Bürgerschaftsdrucksache 13/5691).

Als völlig unvertretbar muß der Umstand bezeichnet werden, daß im Bezirksamt Bergedorf die Hilfeempfänger noch namentlich aufgerufen werden. 1988 war dort der Verzicht auf ein Wartemarkensystem noch damit begründet worden, daß die Abwicklung des Publikumsverkehrs ohne Namensaufruf möglich sei und praktiziert werde. Im Rahmen meiner Fragebogenaktion wurde jetzt die Praktizierung des namentlichen Aufrufs damit begründet, daß die räumliche Situation eine andere Verfahrensweise gar nicht zulasse. Dieses Verfahren ist kurzfristig zu ändern, aber bei Redaktionsschluß noch nicht umgestellt worden.

6.3 Offenbarung von Sozialdaten auf Überweisungsträgern

Bereits mehrfach – zuletzt im 7. TB, 4.1.12 – wurde an dieser Stelle darüber berichtet, daß mit der exakten Bezeichnung von Sozialleistungen auf Überweisungsträgern eine unbefugte Offenbarung von Sozialdaten an das kontoführende Kreditinstitut erfolgt. Obwohl auch die Bürgerschaft diese Verfahrensweise als unzumutbar empfand, wurde diese rechtswidrige Praxis mit ausdrücklicher Billigung des Senats lange Zeit beibehalten.

Die Behörde für Arbeit, Gesundheit und Soziales (BAGS) hat inzwischen einen Kompromißvorschlag erarbeitet, der so aussieht, daß alle Sozialleistungen einheitlich durch einen Hinweis auf § 55 SGB-I gekennzeichnet werden sollen. Als Absender der Leistung soll nur noch die Landeshauptkasse angegeben werden. Zu diesen Sozialleistungen zählen neben der Sozialhilfe insbesondere Wohngeld, Kinder- und Erziehungsgeld, Leistungen der Kranken- und der Rentenversicherung und Leistungen nach dem Bundesausbildungsförderungsgesetz.

Die BAGS hatte sich deshalb an das zur Baubehörde gehörende Amt für Wohnungswesen, das zur Behörde für Wissenschaft und Forschung gehörende Hochschulamt und das zur Behörde für Schule, Jugend und Berufsbildung gehörende Amt für Jugend gewandt, damit diese Stellen hinsichtlich der von ihnen gewährten Sozialleistungen eine entsprechende Umstellung der Überweisungspraxis vornehmen. Lediglich das Hochschulamt, die für Zahlungen nach dem Unterhaltsvorschußgesetz zuständige Stelle des Amtes für Jugend und das Versorgungsamt konnten sich nicht entschließen, diesen Vorschlag umzusetzen. Besonders erstaunt hat uns dabei, daß sich selbst das zur BAGS gehörende Versorgungsamt dagegen sperrte. Auf unsere diesbezügliche Nachfrage bei der BAGS wurde uns zur „Erklärung" mitgeteilt, daß man selbst eine Änderung der Überweisungspraxis nie für erforderlich gehalten und daher Verständnis für die Zurückhaltung einzelner Dienststellen habe.

Die anderen betroffenen Stellen haben dankenswerterweise inzwischen die Umstellung vorgenommen, womit nunmehr für eine Vielzahl von Sozialleistungen eine einheitliche Bezeichnung erreicht wurde, die künftig Außenstehende nicht mehr erkennen läßt, um welche Leistung konkret es sich jeweils handelt. Insbesondere entfällt für die Zukunft der oft als stigmatisierend empfundene Hinweis auf den Sozialhilfebezug.

6.4 Amtshilfeverpflichtung gegenüber den Fernmeldeämtern

Durch eine Krankenkasse wurde darauf hingewiesen, daß die zur TELEKOM gehörenden Fernmeldeämter unter Berufung auf die Amtshilfevorschriften des Sozialgesetzbuches/Zehntes Buch (SGB-X) Auskunftsersuchen an Krankenkassen richten, um auf diesem Wege z.B. den Arbeitgeber eines säumigen Entgeltzahlers herauszufinden. Für diese Verfahrensweise gibt es jedoch keine Rechtsgrundlage. Eine solche Amtshilfeberechtigung setzt nämlich u.a. voraus, daß die ersuchende Stelle Behörde im Sinne von § 1 Abs.2 SGB-X ist.

Seit dem 1.Juli 1991 ist die Beitreibung von Entgeltforderungen, die aus einer Inanspruchnahme der Einrichtungen der TELEKOM herrühren, ausschließlich durch § 9 Fernmeldeanlagengesetz (FAG) geregelt. § 9 FAG nimmt in den Absätzen 2 und 4 eine Unterscheidung von im Monopolbereich erbrachten Leistungen und anderen Leistungen vor, wobei die daraus resultierenden Forderungen jeweils als privatrechtlich qualifiziert werden. Das Monopol beschränkt sich auf das Betreiben von Fernmeldeanlagen, soweit es der Vermittlung von Sprache für andere dient (Telefondienstmonopol), auf die Errichtung und Betreibung von Übertragungswegen einschließlich der zugehörigen Abschlußeinrichtungen (Netzmonopol) sowie auf die Errichtung und Betreibung von Funkanlagen.

Hinsichtlich der nicht im Monopolbereich erbrachten Leistungen fehlt ohnehin jeder Anhaltspunkt dafür, daß die TELEKOM Behörde und damit amtshilfeberechtigt sein könnte, denn insoweit ist die TELEKOM wie ein privates Wirtschaftsunternehmen zu behandeln. Hinsichtlich der Forderungen, die aus im Monopolbereich erbrachten Leistungen resultieren, gibt es allerdings für die Entgeltbeitreibung eine Verweisung auf das Verwaltungs-Vollstreckungsgesetz, die diese Forderungen damit öffentlichrechtlichen Forderungen gleichstellt und daher zu dem Schluß verleiten könnte, die Fernmeldeämter seien hier doch wie eine Behörde zu behandeln.

Bei näherer Betrachtung ergibt sich jedoch, daß die TELEKOM auch hinsichtlich der im Monopolbereich erbrachten Leistungen nicht als Behörde anzusehen ist. Auch die Leistungen im Monopolbereich werden nämlich nicht hoheitlich erbracht. Die erfolgte Verweisung auf das Verwaltungs-Vollstreckungsgesetz bezieht sich zudem ausschließlich auf die – unmittelbare – Beitreibung dieser Forderungen und hat also Ausnahmecharakter. Die Ermittlung z.B. des Arbeitgebers eines Schuldners dient jedoch lediglich der Vorbereitung der Beitreibung.

Die TELEKOM ist also nicht Behörde i.S.d. § 1 Abs.2 SGB-X und damit auch nicht amtshilfeberechtigt i.S.d. § 4 Abs. 1 SGB-X. Unabhängig davon bestimmt zudem § 68 SGB-X, daß ein Amtshilfeersuchen abzulehnen ist, wenn die ersuchende Stelle sich ihre Informationen auf andere Weise beschaffen kann. Da die Fernmeldeämter aber auch die Möglichkeit haben, z.B. den Arbeitgeber durch eine eidesstattliche Versicherung des Betroffenen im Zwangsvollstreckungsverfahren zu erfahren, wäre ein Amtshilfeersuchen auch aus diesem Grund abzulehnen. Die Mitwirkung des Betroffenen entspricht zudem am besten dem allgemeinen datenschutzrechtlichen Gebot der primären Datenerhebung beim Betroffenen.

6.5 Zweites SGB-Änderungsgesetz

Das Sozialgesetzbuch enthält – insbesondere im X. Buch – eine Fülle von Verweisungen auf das Bundesdatenschutzgesetz. Nachdem der Bundesgesetzgeber die Verweisungen im SGB nicht an das am 1. Juni 1991 in Kraft getre-

tene neue Bundesdatenschutzgesetz angepaßt hat, ist hinsichtlich der Verweisungen eine erhebliche Rechtsunsicherheit eingetreten. U.a. der Korrektur dieses Mißstandes dient der Entwurf eines 2. SGB-Änderungsgesetzes, der uns im April 1991 erreichte. Dieser Gesetzentwurf verfolgt daneben als zweites wesentliches Ziel, im Sozialgesetzbuch nicht nur wie bisher die Datenoffenbarung (= -übermittlung) zu regeln, sondern die Datenerhebung, -verarbeitung und -nutzung insgesamt.

Beide Gesetzesziele sind begrüßenswert. Eine Durchsicht im Detail ergab jedoch zahlreiche Mängel. Kritikwürdig ist dabei vor allem, daß die Datenverarbeitungsbefugnisse der Krankenkassen und des Medizinischen Dienstes erweitert werden sollen. Daneben fällt auf, daß zahlreiche Regelungen des Bundesdatenschutzgesetzes in kaum veränderter Form in das SGB eingefügt werden sollen. Dies wird dem speziellen und stärkeren Schutzbedürfnis der Sozialdaten jedoch nicht gerecht.

Wir haben den Änderungsbedarf im einzelnen sowohl dem Bundesdatenschutzbeauftragten als auch der fachlich zuständigen Behörde für Arbeit, Gesundheit und Soziales mitgeteilt, damit ihm im weiteren Gesetzgebungsverfahren Rechnung getragen werden kann. Bis Redaktionsschluß lag ein überarbeiteter Gesetzentwurf noch nicht vor.

6.6 Auswirkungen des Betreuungsgesetzes

Der Deutsche Bundestag hat am 25. April 1990 einen Entschließungsantrag der Bundestagsfraktionen der CDU/CSU, SPD und FDP (Bundestagsdrucksache 11/6983) angenommen, wonach die Bundesregierung alle vier Jahre, erstmalig zum 1.Januar 1996, über die praktischen Auswirkungen der im Betreuungsgesetz enthaltenen Regelungen zur Sterilisation berichten möge.

Der Bundesminister der Justiz (BMJ) beabsichtigt, diesem Entschluß zu entsprechen; die Landesjustizverwaltungen sind zu einer entsprechenden Mitwirkung bereit. Hinsichtlich der Verfahrensweise ist dem Bundesdatenschutzbeauftragten und durch diesen den Landesdatenschutzbeauftragten Gelegenheit zur Stellungnahme gegeben worden.

Benötigt werden ab 1.Januar 1992 im wesentlichen personenbezogene Daten aus den gerichtlichen Verfahren über die Bestellung eines besonderen Betreuers (§ 1899 Abs. 2 – neu – BGB) und über die vormundschaftsgerichtliche Genehmigung der Einwilligung des Betreuers in eine Sterilisation (§ 1905 Abs. 2 Satz 1 – neu – BGB).

Für unerläßlich hält der BMJ Angaben über

— Alter, Geschlecht und Wohnverhältnisse der betroffenen Person,

— die Zahl der Gutachten,

— den Ausgang des Verfahrens und

— die Indikation (im Falle der Genehmigung).

Zudem hält er es für wünschenswert bzw. hilfreich, wenn ihm gerichtliche Entscheidungen zur Verfügung gestellt würden und er Angaben erhielte über

— frühere Schwangerschaften,

— Kinder,

— Trennung von Kindern,

— Art der Behinderung oder Krankheit und

— den Anlaß des Verfahrens.

Die jeweiligen Informationen sollen nur in anonymisierter Form gegeben werden.

Wir haben darauf hingewiesen, daß der Bundestagsbeschluß keine ausreichende Rechtsgrundlage zur Erhebung und weiteren Verarbeitung dieser höchst sensiblen Daten darstellt. Es bedarf vielmehr einer bereichsspezifischen gesetzlichen Regelung, die dezidiert regeln muß, wer wann welche Daten erhebt und wer sie wann wem übermittelt.

Gegen die Verwendung anonymisierter Daten bestehen dann keine Bedenken, wenn eine Reidentifizierung mit hinreichender Sicherheit ausgeschlossen ist. Im Hinblick auf die relativ kleine Zahl betroffener Personen sollte daher ein Erhebungsbezirk keinesfalls kleiner als der eines Oberlandesgerichts sein.

Da gerichtliche Entscheidungen aufgrund des in ihnen dargestellten entscheidungserheblichen Sachverhalts auch dann eine Reidentfizierung ermöglichen, wenn das Rubrum der Entscheidung unkenntlich gemacht wurde, ist es nicht vertretbar, diese Entscheidungen für eine Berichterstattung zur Verfügung zu stellen. Soweit Daten lediglich hilfreich, nicht jedoch unerläßlich sind, muß auf sie ganz verzichtet werden.

Der Bundesdatenschutzbeauftragte hat sich diese Auffassung in seiner an den BMJ ergangenen Stellungnahme zu eigen gemacht.

6.7 Öffentliche Rechtsauskunft- und Vergleichsstelle (ÖRA)

Die Aufgaben der ÖRA sind die einer Gütestelle für zivile Streitigkeiten, einer Vergleichsstelle im strafrechtlichen Sühneverfahren und die der Rechtauskunft und -beratung. Eine Eingabe gab Veranlassung, das letztgenannte Verfahren, also das Beratungsverfahren, im Hinblick auf die Einhaltung datenschutzrechtlicher Bestimmungen bei der Datenerhebung und -übermittlung zu betrachten.

In dem zugrunde liegenden Fall hatte sich eine Bürgerin an die ÖRA gewandt, da sie vermutete, der Unterhaltsanspruch gegen ihren geschiedenen Ehemann hätte sich erhöht. Daraufhin wandte sich die ÖRA schriftlich an den geschiedenen Ehemann und wies darauf hin, es sei Aufgabe der ÖRA, bei Streitigkeiten oder bevorstehenden Streitigkeiten schlichtend und vermittelnd tätig zu werden. Es gehe der ÖRA jedoch nicht um eine einseitige Interessenvertretung.

Sodann wurde der Ehemann um Auskünfte gebeten, die zur Klärung der Rechtslage erforderlich waren. Im Laufe der sich weiter anschließenden Korrespondenz erfuhr der Ehemann erst nachträglich, daß die ÖRA die von ihm mitgeteilten Daten an seine geschiedene Ehefrau weitergereicht hatte.

Bei der rechtlichen Bewertung dieser Verfahrensweise konnte mit der ÖRA und auch mit der Rechtsabteilung der fachlich zuständigen BAGS Einvernehmen darüber erzielt werden, daß die Tätigkeit für die Ehefrau eine Sozialleistung gemäß § 8 Abs.2 BSHG darstellte. Insoweit war die ÖRA also Leistungsträger i.S.d. Sozialgesetzbuches (SGB). Erhobene Daten – hier bei dem Ehemann – fallen unter das Sozialgeheimnis (§§ 35 SGB-I, 67 SGB-X).

Für den Ehemann bestanden jedoch keine Mitwirkungspflichten, wie sie in den §§ 60 ff. des SGB-I beschrieben sind. Die Datenerhebung bei ihm mußte sich daher nach den §§ 5, 12 ff. HmbDSG richten. Nach dem HmbDSG selbst (§ 5 Abs.1 Nr.1 HmbDSG) wäre eine Erlaubnis aber nur dann gegeben gewesen, wenn die Datenerhebung zur Aufgabenerfüllung erforderlich gewesen wäre (§ 12 Abs.1 HmbDSG).

Eine Aufgabe in diesem Sinne hatte die ÖRA vorliegend jedoch nur gegenüber der Ehefrau zu erfüllen, da nur sie die ÖRA um Hilfe gebeten hatte. Daher konnte eine Datenerhebung bei dem Ehemann nur mit dessen Einwilligung erfolgen (§ 5 Abs.1 Nr.2 HmbDSG).

Der Ehemann wäre also ausdrücklich darüber aufzuklären gewesen, daß seine Mitwirkung rein freiwillig erfolgt und daß eine etwaige Nicht-Mitwirkung als solche keine Nachteile für ihn bringt. Das schließt nicht aus, daß ihm ggf. die Einschätzung der Rechtslage und der Aussichtslosigkeit des Rechtsweges mitgeteilt wird. Weiterhin wäre er ausdrücklich darauf hinzuweisen gewesen, daß die von ihm mitgeteilten Daten seiner Frau zur Verfügung gestellt werden.

Das war jedoch nicht in ausreichender Weise geschehen. Zwar enthielt das erste Schreiben der ÖRA neben der freundlich formulierten Bitte um Mitwirkung auch den Hinweis darauf, daß hier Rechte der Ehefrau geltend gemacht werden. Das macht einem unbefangenen und rechtsunkundigen Bürger aber nicht ausreichend deutlich, daß eine Datenübermittlung beabsichtigt ist. Vielmehr sieht er sich einer Behörde gegenüber, deren Begehren er – üblicherweise – zu entsprechen hat.

Wir haben die ÖRA daher gebeten, auf der Grundlage dieser rechtlichen Einschätzung die bisherige Praxis zu überdenken und insbesondere eine ausreichende Aufklärung vorzunehmen. Beispielsweise könnte in den Anschreiben an die Gegenseite die Aufgabenbeschreibung der ÖRA derart ergänzt werden, daß die angeschriebene Person zur Mitwirkung nicht verpflichtet sei und daß sie im Falle ihrer Mitwirkung mit der Übermittlung ihrer Angaben an den Hilfesuchenden rechnen müsse. Die ÖRA hat sich unserem Vorschlag gegenüber grundsätzlich aufgeschlossen gezeigt. Allerdings besteht seitens der ÖRA die Sorge, daß die dort ehrenamtlich tätigen Richter und Rechtsanwälte Bedenken

gegen allzu strikte Verhaltensvorgaben haben könnten. Wir haben daher in Gesprächen mit der ÖRA den Kompromiß erzielt, daß die Übersendung eines Merkblattes an die Gegenseite erfolgt, welches nicht nur die Aufgaben der ÖRA beschreibt, sondern auch die Freiwilligkeit der Mitwirkung. Im übrigen gehen wir mit der ÖRA davon aus, daß die Berater grundsätzlich von sich aus den Anforderungen des Datenschutzes entsprechen.

6.8 Drogenmortalitäts- und -notfallstudie

Das Bundesgesundheitsministerium hat das Sozialpädagogische Institut Berlin federführend beauftragt, in Zusammenarbeit mit den Instituten für Rechtsmedizin in Berlin, Bremen und Hamburg eine zeitlich befristete Studie zu medizinischen und soziologischen Ursachen und Hintergründen von Drogentodesfällen und Drogennotfällen durchzuführen. Die Machbarkeit des Forschungsprojektes wurde im Rahmen einer auf Drogentodesfälle beschränkten Vorstudie erprobt.

Über dieses Forschungsprojekt wurden wir Ende Januar 1991 durch das Referat Drogen und Sucht der Behörde für Arbeit, Gesundheit und Soziales (BAGS) informiert. Dazu wurde ein schriftliches Studienprotokoll vorgelegt. Im Rahmen der Vorstudie sollten in den drei teilnehmenden Städten insgesamt 100 Drogentodesfälle aus 1990 analysiert werden. In der sich anschließenden Hauptstudie sollten die Drogentodesfälle aus 1991 und – teilweise – 1992 vollständig analysiert werden. Hier sollten zum Vergleich auch Drogensüchtige herangezogen werden, die einen Drogennotfall überlebt haben.

Ziel der Studie ist es, die persönliche Situation des Drogensüchtigen, seine Lebensgeschichte, seine gesundheitliche Situation, die Umstände seines Todes, Auffälligkeiten bei seinen nahen Angehörigen (sog. Familienanamnese), die Drogenkarriere, Straffälligkeiten u.a. dezidiert zu erfassen.

Erkenntnisquellen sind

— die gerichtsmedizinischen Untersuchungen der Verstorbenen,

— Informationen aus polizeilichen Akten,

— Interviews mit Angehörigen,

— Interviews mit Drogenberatern,

— Interviews mit überlebenden Drogennotfällen,

— Blutentnahmen bei überlebenden Drogennotfällen,

— Notarzteinsatzprotokolle.

Eine inhaltliche Bewertung der Studie unter Datenschutzgesichtspunkten führt zu folgendem Ergebnis: Prinzipiell unproblematisch ist die – anonymisierte – Auswertung der gerichtsmedizinischen Untersuchungen. Ebenfalls unproblematisch sind Interviews mit Angehörigen, sofern der Zweck des Interviews von

vorneherein offengelegt wird. Die Auswertung der Notarzteinsatzprotokolle ist im Rahmen der Forschungsregelungen des § 12 Hamburgisches Krankenhausgesetz (HmbKHG) möglich. Die Preisgabe polizeilicher Informationen ist grundsätzlich im Rahmen der Forschungsregelungen in § 27 Hamburgisches Datenschutzgesetz (HmbDSG) ebenfalls möglich. Allerdings ist unsere in dem dort beschriebenen Verfahren vorgesehene Beteiligung im Rahmen der Vorstudie nie erfolgt, so daß dieses Verfahren nicht ordnungsgemäß betrieben wurde. Interviews mit überlebenden Drogennotfällen sind prinzipiell ebenfalls möglich. Insofern ist allerdings von besonderer Bedeutung, daß einem Interview die notwendige ärztliche Behandlung vorangeht, da anderenfalls – bei beeinträchtigtem Bewußtseinszustand – von einer bewußt freiwilligen Mitwirkung nicht ausgegangen werden kann. Uns wurde allerdings zugesagt, dies zu beachten.

Interviews mit Drogenberatern hingegen sind problematisch, da die im Rahmen der Studie vorgesehenen Interviews personenbezogen sind, die Drogenberater aber einer durch § 203 StGB strafbewehrten Schweigepflicht unterliegen. Diese Schweigepflicht gilt ausdrücklich über den Tod der Betroffenen hinaus. Zur Lösung dieser Problematik war daher zunächst vorgesehen, Angehörige bzw. Hinterbliebene um eine Einwilligung in diese Offenbarungen zu bitten. Eine solche Möglichkeit ist auch in der Rechtsprechung und Literatur bereits angeklungen. In § 5 Abs. 4 Hamburgisches Archivgesetz ist dies sogar ein für die Verkürzung von Schutzfristen normiertes Verfahren. Gleichwohl handelt es sich um eine sehr fragwürdige Verfahrensweise, die rechtlich nicht abgesichert ist. Manches spricht dafür, die Einwilligungsbefugnis als höchstpersönlich anzusehen.

In dem bereits angesprochenen § 12 HmbKHG ist für vergleichbare Fälle zugelassen worden, daß personenbezogene Daten unter bestimmten Voraussetzungen ohne Einwilligung der Betroffenen zu Forschungszwecken übermittelt werden dürfen. Allerdings gilt diese Regelung nur für Krankenhäuser. Nicht-öffentlichen Stellen, zu denen Drogenberatungsstellen regelmäßig zählen, erlaubt das Bundesdatenschutzgesetz in § 28 Abs. 2 Nr. 2, personenbezogene Daten ohne Einwilligung der Betroffenen an Forschungseinrichtungen zu übermitteln, wenn der Forschungszweck die schutzwürdigen Interessen der Betroffenen überwiegt und der Forschungszweck anders nicht oder nur mir unverhältnismäßigem Aufwand erreicht werden kann. Unmittelbar gilt diese Regelung allerdings nur für solche nicht-öffentlichen Stellen, die Daten in oder aus Dateien verarbeiten oder nutzen, was bei Drogenberatern nicht generell der Fall sein wird. Da jedoch in Dateien geführte Daten gesetzlich stärker geschützt sind als solche in Akten, wird bei letzteren erst recht von einer zulässigen Übermittlung für Forschungszwecke ausgegangen werden können.

Mit Rücksicht auf diese gesetzlichen Regelungen, auf den Forschungszweck und insbesondere darauf, daß die Offenbarung nur gegenüber einer einzigen ebenfalls zur Verschwiegenheit verpflichteten Person stattfindet, die die Daten dann unverzüglich anonymisiert, haben wir uns bereit erklärt, die Studie auch

insoweit inhaltlich mitzutragen. Allerdings trifft keinen Drogenberater eine Verpflichtung zur Offenbarung, so daß er über eine Offenbarung selbst entscheiden muß.

Außerordentlich problematisch sind die vorgesehenen Blutentnahmen bei überlebenden Drogennotfällen. Grundsätzlich sind solche Blutentnahmen möglich, wenn sie entweder medizinisch angezeigt sind oder aber die Betroffenen eingewilligt haben. Da diese Blutentnahmen bereits erfolgen sollen, bevor die ärztliche Behandlung des Notfalles durch Verabreichung eines Gegenmittels erfolgt, können die Betroffenen nicht in der Lage sein, ihr Einverständnis zu dieser Blutentnahme zu erklären. Die Blutentnahmen wurden aber damit begründet, daß sie grundsätzlich medizinisch erforderlich seien, um z.B. die exakt notwendige Dosis des Gegenmittels feststellen zu können. Die herkömmliche Notfallversorgung sei nicht optimal und im Rahmen der Studie kämen also die Betroffenen ausnahmsweise in den Genuß einer optimalen Versorgung. Unter datenschutzrechtlichen Gesichtspunkten besteht insoweit eine Grauzone. Hier kann nur darauf vertraut werden, daß die beteiligten Mediziner rechtlich und ethisch vertretbare Verfahren anwenden.

Leider konnten wir nicht immer den Eindruck haben, daß im Rahmen dieser Studie eine ausreichende Bereitschaft zur Berücksichtigung der datenschutzrechtlichen Aspekte und damit der Interessen der Betroffenen vorhanden war. Zunächst wurde sogar behauptet, die Verstorbenen hätten grundsätzlich ein Interesse an der Aufklärung der „in Rede stehenden Sachverhalte", womit nichts anderes als die geplante umfassende Datenerhebung gemeint war. Die Kriterien für den Datenschutz konnten dann erst mühsam Schritt für Schritt entwickelt werden. Mit der Vorstudie war bedauerlicherweise bereits ohne unsere Zustimmung begonnen worden. Es wurde dann aber immerhin verabredet, mit der Hauptstudie erst nach einer vorherigen länderübergreifenden Abstimmung zu beginnen. Die Hauptstudie begann dann am 1. Juli 1991. Die länderübergreifende Abstimmung fand jedoch erst im August statt, wenn auch mit einem für alle Seiten tragbaren Ergebnis. Dieses Ergebnis sollte dann in dem Studienprotokoll verbindlich festgeschrieben werden. Bis Redaktionsschluß lag das überarbeitete Studienprotokoll jedoch nicht vor.

Insgesamt gesehen fand daher die datenschutzrechtliche Abstimmung der Studie in einer Weise statt, die der inhaltlichen Sensibilität des Projektes nur in unzureichender Weise gerecht wurde.

6.9 Verträge zwischen Krankenkassen und Hamburgischer Krankenhausgesellschaft gemäß § 112 SGB-V

Die Arbeitsgemeinschaft der Krankenkassenverbände in Hamburg und die Hamburgische Krankenhausgesellschaft sind gesetzlich verpflichtet, durch Abschluß von Verträgen sicherzustellen, daß Art und Umfang der Krankenhausbehandlung den Anforderungen des V. Buches des Sozialgesetzbuchs entsprechen. Der erste Vertrag über allgemeine Bedingungen der Krankenhaus-

behandlung ist bereits abgeschlossen worden; weitere Verträge über die Überprüfung der Notwendigkeit und Dauer der Krankenhausbehandlung und über die externe Qualitätssicherung in der stationären Versorgung sind in Vorbereitung.

Im Vertrag über die allgemeinen Bedingungen der Krankenhausbehandlung sind aus datenschutzrechtlicher Sicht vor allem die Regelungen über die Auskunfts- und Mitteilungspflichten des Krankenhauses gegenüber den Krankenkassen von Bedeutung, die im Laufe der Vertragsverhandlungen mit uns abgestimmt wurden. In einer Anlage, die Bestandteil des Vertrages ist, werden die Informationen aufgeführt, die im Antrag auf Erklärung der Kostenübernahme, in der Mitteilung über Rehabilitationsmaßnahmen und in Aufnahme- und Entlassungsanzeigen enthalten sein sollen. Ferner wird vereinbart, daß diese Daten von den Krankenhäusern an die Gemeinsame Datenverarbeitungsstelle der Krankenversicherung (GDKV) übermittelt werden.

Da die Weitergabe dieser Daten in das informationelle Selbstbestimmungsrecht des Patienten eingreift, ist die Übermittlung nur auf Grund einer gesetzlichen Offenbarungsbefugnis oder – wie bei Rehabilitationsmaßnahmen – mit Einwilligung des Betroffenen zulässig. Deshalb müssen sich die vertraglichen Regelungen hinsichtlich der Datenübermittlung streng am gesetzlichen Rahmen orientieren, denn eine zweiseitige Vereinbarung zwischen Krankenkassen und Krankenhausträgern reicht als Eingriffsgrundlage in Grundrechtspositionen des Patienten nicht aus.

Prüfungsmaßstab für die Zulässigkeit der Datenübermittlung der Krankenhäuser ist § 301 SGB-V, der konkret den Datensatz umschreibt, den die Krankenhäuser in Aufnahme- und Entlassungsanzeigen an die Krankenkassen weiterzugeben haben. Da diese Übermittlungsregelung auf Grund der Gesetzessystematik als abschließend anzusehen ist, mußten darüber hinausgehende Informationsbedürfnisse der Krankenkassen, wie z.B. die Angabe des Arbeitgebers bzw. der Dienststelle des Mitglieds, aus dem Datenkatalog gestrichen werden.

Zu einem weiteren Vertragsentwurf, der die Überprüfung der Notwendigkeit und Dauer der Krankenhausbehandlung betrifft, war aus datenschutzrechtlicher Sicht Stellung zu nehmen. Nach dem Entwurf verlangen die Krankenkassen von den Krankenhäusern unter anderem einen Kurzbericht über die Dauer der stationären Behandlung, um über eine Beteiligung des Medizinischen Dienstes zur Prüfung der Leistungspflicht entscheiden zu können. Ein solcher Bericht zur Erläuterung der Dauer der stationären Behandlung ist im Gesetz nicht vorgesehen. Zulässig ist lediglich die Weitergabe der Diagnose in kodierter Form. Eine weitergehende Offenbarung von medizinischen Daten ist nach geltendem Recht nicht erlaubt.

Dies mußten wir den Krankenkassen auch in einem anderen Zusammenhang wieder verdeutlichen: Nach dem Errichtungsvertrag für die Gemeinsame

Datenverarbeitungsstelle (GDKV) darf eine personenbezogene Datenverarbeitung dort erst dann durchgeführt werden, wenn der Hamburgische Datenschutzbeauftragte dem vorzulegenden Datensicherungskonzept zugestimmt hat (vgl. 9. TB, 4.16.2.1). Das uns im Juli 1991 zugesandte Konzept sieht in den Anlagen wieder die Übermittlung von „medizinischen Begründungen" für unüblich lange Krankenhausverweilzeiten vor.

In einem Gespräch betonten die Geschäftsführer der GDKV die Bedeutung gerade dieser Datenübermittlung für die Kostendämpfung im Hamburger Gesundheitswesen. Die Auslegung des bestehenden § 301 SGB-V blieb nach wie vor umstritten.

In einem Referentenentwurf zum 2. SGB-Änderungsgesetz ist nun eine Ergänzung des § 301 SGB-V um die Mitteilung einer medizinischen Begründung bei Verlängerungsanträgen vorgesehen. Dies setzt allerdings die Einführung einer grundsätzlich befristeten Krankenhauspflege bzw. Kostenübernahme durch die Kassen voraus, die auch der Änderungsentwurf bislang nicht normiert.

Insgesamt verkennen wir nicht das Bedürfnis nach einer Überprüfungsmöglichkeit von Krankenhausverweilzeiten. Wir müssen jedoch im Interesse des Patientendatenschutzes auf einer normenklaren gesetzlichen Regelung der Übermittlungspflichten der Krankenhäuser bestehen. Zu dem vorgelegten Datensicherheitskonzept der GDKV konnten wir deswegen, aber auch wegen einer noch offenen Klärung von Zugriffssicherungen unsere Zustimmung bisher nicht erteilen.

6.10 Hamburger Altenbericht

Durch eine Veröffentlichung im Wochendienst der Staatlichen Pressestelle und in der Presse am 25. Oktober 1991 erfuhren wir, daß die BAGS eine sozialempirische Erhebung zur Lebens- und Versorgungssituation älterer Menschen in Hamburg durch ein privates Unternehmen durchführen läßt. Erst auf unsere telefonische Bitte sind uns am 6. November 1991 Unterlagen über das Projekt zugegangen. Diese zeigten, daß die Überlegungen zu dem Projekt spätestens im April 1991 konkrete Gestalt angenommen hatten.

Im Rahmen des Projektes wird eine repräsentativ ausgewählte Stichprobe von etwa 1.500 Senioren über 60 Jahren befragt, und zwar zu

— Person, Arbeit und Beruf,

— Familienbeziehungen und sozialen Kontakten,

— Wohnbedingungen,

— Versorgung, Pflege und Gesundheit,

— Tätigkeit,

— Einkommen,

— Einstellung zum Alter.

Die Datenerhebung findet im Rahmen des Projekts – unabhängig von einer möglichen Anonymität bei der weiteren Datenverarbeitung – eindeutig personenbezogen statt, da die Daten durch unmittelbare persönliche Befragung der namentlich bekannten Bürger gewonnen werden. Die Daten sollen u.a. für eine „repräsentative Sozialstatistik zur Situation älterer Menschen (Einkommen, Wohnen, Gesundheit, Pflege, Partizipation)" herangezogen werden.

Eine Rechtsgrundlage für dieses Projekt hat es zunächst nicht gegeben. § 75 BSHG, der Sozialhilfeleistungen im Rahmen der Altenhilfe regelt, bietet keine geeignete Rechtsgrundlage. Auch das Gesetz über die Durchführung von Statistiken auf dem Gebiet der Sozialhilfe und der Kriegsopferfürsorge kommt als Grundlage nicht in Betracht. Eine entsprechende aufgrund § 1 Abs. 2 Nr. 1 dieses Gesetzes erlassene Rechtsverordnung gibt es ebenfalls nicht. Als allgemeine Rechtsgrundlage verbleibt demnach das Hamburgische Statistikgesetz (HmbStatG).

Ausgehend von den formulierten Zielsetzungen der Befragung handelt es sich um eine Landesstatistik ohne Auskunftspflicht. Sie bedarf gemäß § 2 Abs.3 HmbStatG einer vom Senat zu erlassenden Rechtsverordnung, die den Kreis der zu Befragenden, die Erhebungs- und Hilfsmerkmale sowie die Art und den Berichtszeitraum der Erhebung festlegt.

Die Durchführung einer solchen Statistik obliegt gemäß § 5 Abs.1 HmbStatG dem Statistischen Landesamt, soweit nichts anderes bestimmt ist. Über die Durchführung einer Statistik durch eine andere Stelle als das Statistische Landesamt hat der Senat zu entscheiden. Sofern die praktische Durchführung der Statistik an Dritte vergeben wird, ist § 5 Abs.2 HmbStatG zu beachten, wonach u.a. sicherzustellen ist, daß der Dritte sich der Kontrolle des Hamburgischen Datenschutzbeauftragten unterwirft. Dem Hamburgischen Datenschutzbeauftragten ist vor der Vergabe der Arbeiten Gelegenheit zur Stellungnahme zu geben.

Wie wenig datenschutzrechtliche Belange berücksichtigt wurden, wird an folgendem beispielhaft deutlich:

— In einem ersten Anschreiben des Senators an die Betroffenen war nicht der erforderliche Hinweis auf die Freiwilligkeit der Mitwirkung enthalten. Ebenso fehlten konkrete Informationen über den Verwendungszweck der Daten. Damit wurde gegen § 17 BStatG verstoßen, der gemäß § 4 Abs.1 HmbStatG auch für Landesstatistiken gilt und demzufolge die zu Befragenden schriftlich zu unterrichten sind, und zwar u.a. über Zweck, Art und Umfang der Erhebung, die statistische Geheimhaltung, die Freiwilligkeit der Auskunftserteilung sowie die Hilfs- und Erhebungsmerkmale.

— Bei kranken Senioren sollte die Datenerhebung nicht bei diesen selbst, sondern bei deren Betreuern vorgenommen werden. Damit würde in völlig unvertretbarer Weise die Privatsphäre alter Menschen notfalls auch gegen ihren Willen ausgeforscht.

— Die Verpflichtung der Interviewer auf das Datengeheimnis berief sich auf zwei bereits nicht mehr geltende Datenschutzgesetze.

— Um die Bereitschaft der Betroffenen zur Mitwirkung zu fördern, sollten die Interviewer auf die individuelle Bedeutung der Auskünfte hinweisen, obwohl diese gerade nicht Gegenstand der Befragung ist.

Ich habe umgehend darum gebeten, die Befragung bis zur verbindlichen Klärung der Rechtsgrundlage auszusetzen und die bereits erhobenen Daten zunächst nicht weiter zu verarbeiten. Die Klärung der statistikrechtlichen Fragen hat dabei grundsätzliche Bedeutung, weil sich daraus Schlußfolgerungen für die Auswirkungen des neuen Hamburgischen Statistikgesetzes auf die vielfältigen Behördenerhebungen ergeben. Damit ist die gesetzlich geregelte Zuständigkeit des Statistischen Landesamtes ebenso berührt wie die Beteiligung des Hamburgischen Datenschutzbeauftragten.

Am 19. November 1991 hat der Senat anhand einer mit mir kurzfristig abgestimmten Senatsdrucksache eine Rechtsverordnung beschlossen.

Der durch sie gedeckte Erhebungszeitraum endet am 31. Dezember 1991. In der Verordung wurde bereits festgelegt, daß Betreuungspersonen nur mit dem Einverständnis der Betreuten befragt werden dürfen. Im Anschluß an die Rechtsverordnung hat die BAGS die Betroffenen in einem zweiten Anschreiben über die in § 17 BStatG genannten Punkte unterrichtet. Sie hat außerdem die Verpflichtung der Interviewer zur Verschwiegenheit ordnungsgemäß überarbeitet. Der mit dem durchführenden Institut geschlossene Vertrag wurde zudem durch einseitige Erklärung des Instituts gemäß den Anforderungen des § 5 Abs. 2 HmbStatG ergänzt. Dabei wurde zwar die Unterwerfung unter die Kontrolle des Hamburgischen Datenschutzbeauftragten an die unzulässige Bedingung der vorherigen Unterrichtung des Auftraggebers geknüpft. Dies haben wir jedoch ausnahmsweise toleriert.

Kurz vor Redaktionsschluß wurde plötzlich klärungsbedürftig, ob das durchführende Unternehmen unzulässigerweise und mit Wissen der BAGS Unteraufträge vergeben hat, nachdem wir kurz zuvor noch mit der BAGS die Unzulässigkeit der Unterauftragsvergabe festgestellt hatten. Ebenfalls noch ungeklärt waren einzelne Punkte des Datensicherungskonzepts und die Regelungen zur Abschottung (§ 7 HmbStatG) innerhalb der BAGS. Auch die Prüfung, ob die einzelnen Fragen den erforderlichen Bezug zu den Aufgaben der öffentlichen Verwaltung haben, konnte noch nicht zu Ende geführt werden.

7. Personalwesen

7.1 Automationsvorhaben Projekt Personalwesen

Im 8. TB (3.2.1) wurde von der Voruntersuchung zur Reorganisation der hamburgischen Personalverwaltung berichtet. Am 14.Mai 1990 erließ Senatorin Klausch die Einsetzungsverfügung für das eigentliche Projekt. Aufbauend auf

den Ergebnissen der Voruntersuchung sollen die Aufgaben der Personalverwaltung insgesamt beschrieben und ggf. neu definiert werden, daraus abgeleitet neue Organisationsstrukturen geschaffen und insbesondere durch IuK-Unterstützung Rationalisierungspotentiale ausgeschöpft werden. Dabei muß „der Datenschutz für die besonders sensiblen personenbezogenen Daten der Mitarbeiter/innen und ihrer Angehörigen vollen Umfangs gewährleistet" werden, wie es in der Einsetzungsverfügung ausdrücklich heißt. Der Hamburgische Datenschutzbeauftragte wurde zum Mitglied in der Lenkungsgruppe des Projekts berufen.

Die Projektgruppe und die Lenkungsgruppe haben seitdem folgende Themenbereiche bearbeitet und hierzu Grundsatzpapiere entwickelt:

— Projektplanung und Verfahren

— Aufgaben der Personalverwaltung einschließlich einer Funktionsstruktur- und Informationsstrukturanalyse

— Abgrenzung der Aufgaben des Personalwesens zu den anderen Behörden (Schnittstellen)

— Alternativen der Kindergeldbearbeitung

— Leitlinien zum Datenschutz

— Leitlinien für die Organisation des Personalwesens

— Projektbericht und Entscheidungsvorschlag zur Auswahl der geeigneten Standardsoftware.

Mit der Entscheidung der Lenkungsgruppe zur Vorab-Installation einer ausgewählten Standardsoftware wurde ein erstes Etappenziel des Projekts erreicht. Dies war Anlaß zu einer grundsätzlicheren datenschutzrechtlichen Stellungnahme.

In ihr wurde zunächst darauf hingewiesen, daß es an einer Gesamtbewertung und Folgenabschätzung eines derart umfassenden Vorhabens im Projektbericht fehlt. In ihm wird der Anspruch formuliert, für das gesamte Personalwesen mit allen seinen Funktionen ein einheitliches System zu schaffen, in das die derzeitigen behördenspezifischen Insellösungen – ggf. über Schnittstellen – integriert werden sollen. Es geht also nicht nur um die Abrechnung der Bezüge, der Beihilfe, des Kindergeldes, sondern um alle Verwaltungs-, Planungs-, Durchführungs-, Kontrollaufgaben im gesamten hamburgischen öffentlichen Personalwesen.

Die damit geschaffene potentielle Verfügbarkeit und Verknüpfbarkeit aller Personaldaten aller Hamburger Beschäftigten ist typisches Merkmal eines umfassenden Personalinformationssystems. Je umfassender das System angelegt ist, desto kritischer ist die Regelung der Zugriffsmöglichkeiten auf die Daten. Erscheint dies auf der Ebene der Sachbearbeitung durchaus zufriedenstellend organisiert werden zu können, so ist die Frage der Zugriffsmöglichkeiten auf

den höheren Ebenen (fachlich: Personalamt, technisch: Systemverwaltung, Wartung) nach dem bislang vorliegenden Erkenntnisstand noch weitgehend ungeklärt. Hierüber wird erst das schrittweise zu entwickelnde Realisierungskonzept Aufschluß geben können. Für jeden Teilbereich sind – wie auch von der Projektgruppe und der Lenkungsgruppe bekräftigt wurde – die Datenschutzanforderungen festzustellen und zu erfüllen. In einer Gesamtbetrachtung ist abschließend zu prüfen und sicherzustellen, daß nicht unbedingt erforderliche Querverbindungen unterbleiben. Es muß auf jeden Fall vermieden werden, daß einzelne Personen einen umfassenden Personaldaten-Einblick bekommen können.

Generell vermittelt die Projektgruppe durchaus den Eindruck, ein ausgeprägtes Datenschutzbewußtsein in die Arbeit einzubringen. Dennoch erfolgte die – vorläufige – Auswahl der einzusetzenden Standardsoftware im Ergebnis vorrangig aufgrund der technischen Möglichkeiten und nicht der datenschutzrelevanten Gesichtspunkte. Die Projektgruppe selbst gibt im Projektbericht zu erkennen, daß das nicht ausgewählte Produkt datenschutzrechtlichen Anforderung deutlich besser genügt. Hierbei geht es zum Beispiel um die wichtige Möglichkeit, die Anwendung von Auswertungsprogrammen revisionsfähig zu protokollieren.

Hinsichtlich der datenschutzrelevanten rechtlichen Anforderungen liegen dem Datenschutzbeauftragten bisher kaum Erkenntnisse vor. So werden unter dem Aspekt der „Erforderlichkeit der Datenverarbeitung" im Sinne des § 28 HmbDSG (Datenverarbeitung bei Beschäftigungsverhältnissen) etwa folgende Fragen zu klären sein:

— Inwieweit ist bei Auswertungen überhaupt ein Personenbezug erforderlich? Diese Frage ist sowohl bei den Standardauswertungen als auch jeweils bei neu zu programmierenden Auswertungen zu beantworten. In diesem Zusammenhang ist ein Hinweis auf die Personalstrukturdatei (vgl. 6. TB, 4.3.3) angebracht. Das Personalamt hatte seinerzeit zugesagt, im Rahmen des Projekts Personalwesen auch die Möglichkeit einer Anonymisierung dieser Strukturdatei zu untersuchen.

— Welche Verknüpfungsmöglichkeiten sind für die in § 28 HmbDSG genannten Zwecke erforderlich? Angesichts der potentiell umfassenden technischen Möglichkeiten und der sehr allgemeinen Fassung des § 28 HmbDSG ist die Festlegung der zulässigen Verknüpfungen von ganz besonderer datenschutzrechtlicher Relevanz. Die Definitions-Kompetenz sollte hier jedenfalls nicht bei der an einer bestimmten Verknüpfungs-Auswertung interessierten Stelle liegen. Auch dürfen schon erreichte Fortschritte wie etwa die Abschottung von Beihilfe-Sachbearbeitung und Personalverwaltung nicht wieder zur Disposition stehen.

— Welche Schnittstellen sind erforderlich? Die Zielvorstellung eines umfassenden integrierten Personalinformationssystems rechtfertigt es nicht, alle tech-

nisch anschließbaren Datenkomplexe für das Gesamtsystem verfügbar zu machen. Gerade der Erhalt von unabhängigen Teilsystemen kann möglicherweise datenschutzrechtlichen Anforderungen eher gerecht werden. Dies gilt insbesondere für eine Anbindung von Personalcomputern.

— Für welche Daten ist eine Historik überhaupt erforderlich? Die Projektgruppe betont die besondere Historik-Fähigkeit des ausgewählten Softwareprodukts. Diese technischen Möglichkeiten sollten jedoch nicht dazu verführen, neben einem breiteren (Datenmenge) auch noch ein tieferes (Langzeitbetrachtung) Personenprofil einzelner Beschäftigter des Öffentlichen Dienstes zu erstellen.

Eine umfassende datenschutzrechtliche Klärung dieser Fragen ist ohne eine Kenntnis der Funktionsstrukturanalyse und der Informationsstrukturanalyse der Projektgruppe nicht möglich und kann angesichts des Umfangs und der Komplexität der einzelnen Personalverwaltungsmaterien sicher nur nach und nach bzw. stichprobenweise erfolgen. Die Bedenken wegen technischer Mängel des ausgewählten Systems beziehen sich z.Zt. insbesondere auf die fehlende Protokollierungsmöglichkeit verschiedener Systemaktivitäten und auf die unzureichende Anonymisierungsmöglichkeit bei der Erstellung von Statistiken.

Die beschlossene Vorab-Installation wird uns eventuell Gelegenheit geben, diese Bedenken zu konkretisieren und auf Abhilfe zu drängen sowie weitere technische Details zu überprüfen. Die aufgrund technischer Möglichkeiten getroffene Entscheidung für eine bestimmte Software kann nicht zum Verzicht auf wichtige datenschutzrechtliche Forderungen führen, sondern muß durch Modifikationen des Systems datenschutzgerecht ergänzt werden.

Ich bin zuversichtlich, daß die gegenseitige Kooperationsbereitschaft zu Fortschritten bei der Realisierung der Datensicherheit führen wird. Die Projektgruppe und die Lenkungsgruppe haben bestätigt, daß die datenschutzrechtlich notwendigen Vorkehrungen mit dem dazugehörigen technischen und finanziellen Aufwand getroffen werden oder – falls nicht realisierbar – datenschutzrechtlich unzulässige Anwendungen unterbleiben.

7.2 Psychologischer Dienst

Der 9. TB enthält die Darstellung der bisherigen Praxis des Psychologischen Dienstes (ehemals: „Prüfungsamt für den Öffentlichen Dienst") bei der Aufbewahrung von Prüfungsunterlagen (4.2.5.3). Im November 1990 erhielt der Psychologische Dienst eine Reihe von datenschutzrechtlichen Anregungen zur Veränderung dieser Praxis. Ein Teil dieser Vorschläge wurde akzeptiert und die Umsetzung für das 2. Halbjahr 1991 in Aussicht gestellt:

So werden in Zukunft die behinderten Bewerber wesentlich ausführlicher über das Verfahren unterrichtet und um Einwilligung dafür gebeten, daß die Prüfungsergebnisse an interessierte Personalstellen weitergegeben bzw. ihnen zur Einsicht vorgelegt werden. Nach vier Jahren sollen die behinderten Bewerber

gefragt werden, ob die Prüfungsunterlagen gelöscht oder weiter aufbewahrt und zur Verfügung gestellt werden sollen.

Auch über die Vernichtung früherer Ausdrucke aus der Prüfungsergebnis-Datei sowie über eine Verbesserung der Anonymisierung dieser Datei konnte ebenso Einvernehmen erzielt werden wie über die Gewährleistung der äußeren Datensicherheit (Stahlschränke, Sicherheitsschlösser). Bei der Aufbewahrung von Prüfungsunterlagen geeigneter und eingestellter Bewerber konnte mit einer Frist von 5 Jahren ein Kompromiß erreicht werden, der noch die gewünschte Bewährungskontrolle für die Tests gewährleistet.

Hinsichtlich der Aufbewahrung von Prüfungsunterlagen von nicht geeigneten und nicht eingestellten Bewerbern fordert § 28 Abs. 5 HmbDSG die unverzügliche Löschung der personenbezogenen Daten, „sobald feststeht, daß ein Beschäftigungsverhältnis nicht zustande kommt". Dieser Zeitpunkt ist abhängig von einem möglichen Rechtsmittelverfahren gegen die Ablehnung der Bewerbung. Die endgültige Nichteinstellung muß überdies dem Psychologischen Dienst mitgeteilt werden. Das Bundesarbeitsgericht räumte in einer Entscheidung von 1984 dem Arbeitgeber lediglich ein, daß er Name, Prüfungstag und -ergebnis festhält, um sich vor ständigen Wiederholungsbewerbungen zu schützen. Demgegenüber vertrat der Psychologische Dienst zunächst die Auffassung, daß er für die Entscheidung, ob ein Wiederholungs-Bewerber noch einmal eine Prüfungsmöglichkeit bekommt, auf die vollständigen Prüfungsunterlagen zurückgreifen können muß. Da das Prüfungsamt auch nicht darüber informiert werde, wann eine Einstellung endgültig scheitert, müsse bei den Prüfungsunterlagen von nicht geeigneten Bewerbern mindestens von einer zweijährigen Aufbewahrungspflicht ausgegangen werden. Inzwischen ist der Psychologische Dienst aber bereit, die Unterlagen der nicht geeigneten Bewerber nach einem Jahr zu vernichten. Angesichts der – ohne Rechtsmittelbelehrung bestehenden – einjährigen Widerspruchsfrist ist damit eine dem § 28 Abs. 5 HmbDSG entsprechende Lösung gefunden.

7.3 Personalärztlicher Dienst

Nachdem wir eine Reihe von Anfragen und Beschwerden zu beantworten hatten, welche die Übermittlung von ärztlichen Erkenntnissen des Personalärztlichen Dienstes an andere Behörden betrafen, fand im Juni 1991 eine datenschutzrechtliche Prüfung dieser Dienststelle des Senatsamtes für den Verwaltungsdienst (Personalamt) statt.

Der Personalärztliche Dienst (PÄD) hat zwei Hauptaufgaben: Zum einen führt er die Einstellungs- und Eignungsuntersuchungen aus Anlaß von Bewerbungen, Ernennungen, Verbeamtungen auf Lebenszeit durch und stellt entsprechende „Personalärztliche Zeugnisse" aus. Zum anderen fertigt der PÄD medizinische Gutachten auf Antrag der jeweiligen Beschäftigungsbehörde zu Fragen der Dienstfähigkeit (für Diensterleichterungen, Versetzungen in den vorzeitigen Ruhestand, in bestimmten Bereichen der Beihilfegewährung). Dar-

über hinaus ist der PÄD zuständig für Untersuchungen von Arbeitnehmern zur Weiterbeschäftigung über die Altersgrenze hinaus, für Untersuchungen wegen Dienstunfallfolgen, für Tuberkulosetests nach dem Bundesseuchengesetz und für Gutachten nach dem Ruhegeldgesetz.

„Personalärztliche Zeugnisse" werden aufgrund von Untersuchungen erstellt, die die Anamnese, Laboranalysen und ggf. frühere Berichte, Unterlagen und medizinische Gutachten durch Dritte einschließen. Bei diesen Untersuchungen wird eine mögliche HIV-Infektion weder erfragt noch ermittelt. Pathologische Befunde werden den Probanden zur Behandlung durch einen anderen Arzt schriftlich mitgeteilt. Die Einstellungsbehörde, die den Probanden beim PÄD angemeldet hatte, erhält das personalärztliche Zeugnis auf einem Formblatt, welches das Ergebnis: „geeignet", „nicht geeignet" oder „in das Ermessen der Behörde gestellt" und darunter die Rubrik „Bemerkungen" enthält.

Die Eignung bzw. Nichteignung bezieht sich immer auf den jeweiligen Anlaß der Untersuchung: So erfordert die Eignungsfeststellung für Ernennungen auf Lebenszeit eine weitergehende Prognose als die Ernennung auf Widerruf (Ausbildung) oder auf Probe. In die Rubrik „Bemerkungen" schreibt der PÄD nicht nur die Begründung für einen Eignungsmangel oder dafür, daß die Einstellung in das Ermessen der Behörde gestellt wird, sondern auch Auffälligkeiten bei geeigneten Probanden. Dabei werden zwar keine Befunde im engeren Sinne mitgeteilt, aber durchaus Umschreibungen für Krankheiten bzw. körperliche oder psychische Besonderheiten. So wurde häufig auch bei geeigneten Probanden ein Hinweis auf Übergewichtigkeit, manchmal auf den Tabakkonsum gegeben. Es kamen in der Vergangenheit – selbst bei einer geeigneten Probandin – Bemerkungen vor wie: „Depressionen wegen Entfernung eines Unterleibstumors nicht ausgeschlossen."

Die eigentlichen Befunde, Drittgutachten und eventuelle Krankenhausunterlagen verbleiben dagegen beim PÄD.

Bei den Gutachten zur Dienstfähigkeit grenzt die beantragende Behörde in der Regel die Untersuchung auf bestimmte Fragestellungen ein. Oft geht es um die Begründung für auffällig häufige Fehlzeiten. In diesen Gutachten antwortet der PÄD ausführlicher auf die gestellten Fragen; die Mitteilung an die Beschäftigungsbehörde enthält also mehr und tiefergehende medizinische Daten als ein Personalärztliches Zeugnis. Die Einzelbefunde sowie weitere Unterlagen verbleiben jedoch auch hier beim PÄD.

Die Begutachtung in Beihilfefragen erfolgt nicht getrennt von anderen Aufträgen. Die Gutachter müßten hier davon absehen, ihre Kenntnisse aus Beihilfe- und anderen Verfahren zu verwerten. Dies ist aber nicht zu gewährleisten und nicht überprüfbar.

Die Versendung der Zeugnisse und Gutachten erfolgt an die jeweilige Personalstelle der Behörde in geschlossenem Sammelumschlag.

Im PÄD werden die Unterlagen sowohl der Einstellungs- und Ernennungsuntersuchungen als auch der Dienstfähigkeits-Untersuchungen oft über Jahrzehnte, z.T. bis hin zum 75. Lebensjahr der Probanden, aufbewahrt. Sie werden z.Zt. mikroverfilmt.

Der EDV-Einsatz im PÄD beschränkt sich derzeit auf die Textverarbeitung. Für die Zukunft ist jedoch eine EDV-Unterstützung auch der Probanden-Verwaltung in der Geschäftsstelle geplant.

Die rechtliche Bewertung dieses Sachverhalts offenbart eine Reihe von datenschutzrechtlichen Problemen, von denen hier nur die wichtigsten genannt seien:

— Die im Personalärztlichen Zeugnis gemachten „Bemerkungen" bei geeigneten Probanden haben bei den Betroffenen oft Anstoß erregt. In § 28 Abs. 4 HmbDSG heißt es: „Bei medizinischen .... Untersuchungen und Tests zur Eingehung eines Beschäftigungsverhältnisses dürfen der Einstellungsbehörde in der Regel nur das Ergebnis und festgestellte Risikofaktoren übermittelt werden." Was unter „Risikofaktoren" zu verstehen ist, bleibt auch in der Gesetzesbegründung offen.

  Nach datenschutzrechtlichen Maßstäben muß die Übermittlung jedes einzelnen Datums jedenfalls geeignet und erforderlich sein. Dementsprechend faßte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im September 1991 eine Entschließung, nach der „durch Gesetz oder ergänzende Rechtsverordnung" festzulegen ist, „daß der Arzt der personalverwaltenden Stelle nur das Endergebnis seiner Untersuchung und – soweit erforderlich – nur tätigkeitsbezogene Risiken mitzuteilen hat".

  Nach Auskunft des PÄD wurden die genannten Bemerkungen bei geeigneten Probanden hinzugefügt, um einerseits dem jeweiligen Personalverantwortlichen eine Hilfestellung bei der Auswahl von Bewerbern zu geben, zum anderen, um mögliche Schutzmaßnahmen des Arbeitgebers zu veranlassen.

  Letzteres scheint jedoch bei den hier behandelten „Personalärztlichen Zeugnissen" nicht im Vordergrund zu stehen, weil die bekanntgewordenen Bemerkungen dem Arbeitgeber keinerlei Handlungsanleitung für Schutz- oder Hilfsmaßnahmen gaben. Bei Ernennungen auf Widerruf und auf Probe können die Bemerkungen dem Personalsachbearbeiter deutlich machen, daß bei der nächsten Statusveränderung – z.B. Ernennung auf Lebenszeit – oder zu einem im Zeugnis selbst genannten Zeitpunkt eine erneute Vorstellung beim PÄD erforderlich ist.

  Zumindest die Personalsachbearbeiter sehen sich ohne medizinische Detailkenntnisse verständlicherweise nicht in der Lage, die Bemerkungen in einer anderen Form umzusetzen, als eine Wiedervorstellung der Probanden zur angegebenen Zeit bzw. bei der nächsten Statusänderung zu verfügen. Um dies zu erreichen, bedarf es jedoch nicht der Mitteilung der konkreten

Auffälligkeit, des Leidens, der Krankheit, sondern nur des Termins bzw. Anlasses.

Bei der Auswahl von geeigneten Bewerbern führen ergänzende medizinische Hinweise zu einer Kennzeichnung der zwar geeigneten, aber gesundheitlich möglicherweise nicht stabilsten Bewerber. Diese Differenzierung in unterschiedliche Eignungen erscheint problematisch.

Die „Bemerkungen" des PÄD bei geeigneten Probanden sollten sich deswegen im Ergebnis entweder auf solche Hinweise beschränken, die für den Arbeitgeber eindeutige Handlungsanweisungen bedeuten wie z.B. „Erforderlichkeit eines ergonomischen Stuhls", „Erforderlichkeit einer Brille bei Bildschirmtätigkeit" usw., oder sich mit der Festlegung eines Termins zur Wiedervorstellung der Probanden beim PÄD begnügen.

— Bei nicht geeigneten Probanden und solchen, bei denen der PÄD die Entscheidung ohne eine Empfehlung in das Ermessen der Behörde stellt, dienen die Bemerkungen dazu, einen ablehnenden Bescheid begründen zu können. Ist der Untersuchungsanlaß eine Bewerbung für den öffentlichen Dienst, muß jedoch auch die Möglichkeit berücksichtigt werden, daß die Bewerber aufgrund des Ergebnisses der PÄD-Untersuchung von sich aus auf das weitere Verfahren verzichten und die Bewerbung zurückziehen. Für diesen Fall ist es nicht erforderlich, der Behörde die Gründe für die Nichteignung, ja noch nicht einmal die Nichteignung selbst, sondern nur den Rücktritt von der Bewerbung mitzuteilen. Es darf allerdings organisatorisch sichergestellt werden, daß der zurückgetretene Bewerber nicht binnen kurzem ein weiteres Mal das Bewerbungsverfahren einschließlich der PÄD-Untersuchung in Gang setzt.

— Angesichts der vorstehenden Ausführungen zu den „Bemerkungen" auf dem Personalärztlichen Zeugnis für geeignete und nicht geeignete Probanden erhält das Aufklärungsgespräch zwischen den Ärzten und den untersuchten Personen eine besondere Bedeutung. Das Recht auf informationelle Selbstbestimmung fordert hier – unbeschadet des sogenannten therapeutischen Vorbehalts bei besonders gefährdeten Patienten – eine umfassende Unterrichtung der Probanden über das Ergebnis der Untersuchung. Dies wird nach Auskunft des PÄD jetzt auch verstärkt verfolgt durch das generelle Angebot eines Arzt-Patienten-Gesprächs mit der Leitung des PÄD, in dem gesundheitliche Einschränkungen detailliert erläutert werden.

  Wegen der oben aufgezeigten Möglichkeiten sollte das Aufklärungsgespräch auch eine Information darüber enthalten, was genau der PÄD der Personaldienststelle mitzuteilen beabsichtigt. Sind die Probanden über die Gründe für eine Nichteignung oder für den Verzicht auf eine PÄD-Empfehlung ausreichend informiert, so läge es datenschutzrechtlich sogar nahe, der Personaldienststelle zunächst nur das Ergebnis der Untersuchung mitzuteilen und erst für den Fall, daß die Betroffenen sich gegen die ablehnende Entscheidung wehren, die – ihnen ja bekannten – Gründe für das Rechtsbehelfsverfahren nachzureichen.

— Ein weiteres, gravierendes datenschutzrechtliches Problem liegt in der jahrzehntelangen Aufbewahrung von Untersuchungsunterlagen im PÄD.

  Die Berufsordnung für Ärzte sieht eine zehnjährige Aufbewahrungspflicht für die medizinischen Dokumentationen vor. Dies gilt jedoch nur für Behandlungs-Unterlagen. Insbesondere für die Befunde und Ergebnisse der Eignungsuntersuchungen bei im Ergebnis nicht eingestellten Bewerbern ist eine jahrelange Aufbewahrung der Unterlagen nicht zu rechtfertigen. Ebenso wie die Prüfungsunterlagen des Psychologischen Dienstes (siehe oben 7.2) handelt es sich hier um „personenbezogene Daten, die vor der Eingehung eines Beschäftigungsverhältnisses erhoben wurden". Sie sind nach § 28 Abs. 5 HmbDSG „unverzüglich zu löschen, sobald feststeht, daß ein Beschäftigungsverhältnis nicht zustande kommt". Als noch vertretbar unter Berücksichtigung der Rechtsmittelfristen erscheint auch hier eine Aufbewahrungsfrist von 1 Jahr nach erfolgter Ablehnung. Um die Kenntnis des PÄD von einer Einstellung oder endgültigen Nichteinstellung zu gewährleisten, bedarf es entsprechender organisatorischer Maßnahmen.

— Die gleichzeitige Zuständigkeit der einzelnen Mitarbeiter für die Bearbeitung von beihilferechtlichen und anderen Fragestellungen verstößt auch im Bereich des PÄD gegen das allgemeine Abschottungsgebot, wonach sicherzustellen ist, daß Kenntnisse aus Beihilfeverfahren nicht zweckwidrig verwendet in allgemeine Personalentscheidungen einfließen dürfen. Dieses Erfordernis ist vom Personalamt auch grundsätzlich anerkannt worden und ein Anlaß für die Zentralisierung der Beihilfesachbearbeitung bei der Besoldungs- und Versorgungsstelle gewesen (vgl. 7. TB, 4.2.1). Gerade bei der Erhebung und Bewertung der Gesundheitsdaten durch den PÄD darf nichts anderes gelten. Dies entspricht auch der Entschließung der Datenschutzbeauftragten vom 26. September 1991. Das Zweckbindungsgebot kann durch ein bloßes Verbot der Datenverwertung durch die Gutachter nicht erfüllt werden.

7.4 Bewerberfragebogen

Im August 1989 veröffentlichte das Personalamt Musterformblätter „Fragebogen für Bewerberinnen und Bewerber" und „Ergänzende Angaben zur Person des/der Einzustellenden" (vgl. 8. TB, 3.2.4). Sie waren mit dem Datenschutzbeauftragten abgestimmt und wurden den Behörden und anderen öffentlichen Stellen zur Übernahme empfohlen, um einen einheitlichen datenschutzrechtlichen Standard zu erreichen. In einer umfassenden Befragung von 52 öffentlichen Stellen im Januar 1991 haben wir versucht, den Erfolg dieser Empfehlung zu messen. Zentral war die Frage, ob die angeschriebenen Stellen bei Bewerbungen/Einstellungen das zweistufige Daten-Erhebungsverfahren anwenden, d.h. bei der Bewerberauswahl nur die dafür notwendigen Daten erfassen und

erst nach der Einstellungs-Entscheidung die für die Personalverwaltung notwendigen Abrechnungs- und Familiendaten erheben.

Die Antworten auf die Befragung erbrachten folgendes Bild: Die Musterfragebogen des Personalamtes wurden durchgehend nur von den Bezirksämtern, teilweise auch von einzelnen Fachbehörden, überhaupt nicht jedoch von den Stellen der mittelbaren Staatsverwaltung verwendet. Von denjenigen Stellen, die eigene Fragebogen verwenden, hielten 6 die datenschutzrechtlich gebotene Zweistufigkeit der Datenerhebung nicht ein. So wurde z.B. bereits bei der Bewerberauswahl nach den Personalien des Ehegatten und nach der Bankverbindung gefragt.

Darüber hinaus enthielten einige der zugesandten Fragebogen eine Reihe von datenschutzrechtlich bedenklichen Abfragen, die zu folgenden typischen Problemfragen zusammengefaßt werden können:

— Frage nach Vorstrafen ohne eine Begrenzung auf arbeitsplatzrelevante Verstöße oder Strafen, die ins Führungszeugnis aufzunehmen sind,

— undifferenzierte Fragen nach schwebenden Ermittlungsverfahren ohne eine Begrenzung auf arbeitsplatzrelevante bzw. schwerere Verstöße,

— detaillierte Fragen nach Schuldenhöhe, Gläubiger, Kreditzweck, monatlichem Schuldendienst und ähnlichem,

— Frage nach dem Namen der Eltern,

— Frage nach einer Schwangerschaft,

— Frage nach dem bisherigen Gehalt.

Gegenüber 17 öffentlichen Stellen baten wir um eine Korrektur der verwendeten Fragebogen bzw. um eine Übernahme des Musterfragebogens des Personalamtes. In den allermeisten Fällen konnte ein Konsens erreicht werden; sehr häufig wurden die beanstandeten Fragen in eine Neuauflage des Bewerberfragebogens nicht mehr aufgenommen. In Einzelfällen stellten wir die Bedenken wegen besonderer behördenspezifischer Umstände zurück. Andere öffentliche Stellen nahmen die Kritik zum Anlaß, nun den Musterfragebogen des Personalamtes zu übernehmen.

Insgesamt ist durch diese Aktion im öffentlichen Dienst Hamburgs weitgehend einheitlich ein Standard bei den Bewerberfragebogen erreicht worden, der den Erfordernissen des § 28 HmbDSG entspricht. Der vom Personalamt veröffentlichte Musterfragebogen für Bewerber wurde nun auch in seiner Datenschutzklausel an diese Vorschrift angepaßt (vgl. Mitteilungen für die Verwaltung 1991 S. 492).

7.5 Beihilfe

7.5.1 Beihilfe bei Psychotherapien

Im 8. TB (3.2.5) wurde die Kritik des Hamburgischen Datenschutzbeauftragten an dem Verfahren zur Feststellung der Beihilfefähigkeit von Aufwendungen für

Psychotherapien beschrieben. Insbesondere wurden Bedenken dagegen geltend gemacht, daß derselbe Arzt des Personalärztlichen Dienstes, der auch für die vom Dienstherren geforderten Untersuchungen im Bereich Nervenkrankheiten und Psychopathien zuständig ist, die Beihilfefähigkeit begutachtet (vgl. auch o. 7.3), ohne daß die Personalien des Bediensteten zuvor ausreichend anonymisiert werden.

Am 27. August 1991 erließ der Senat eine neue Hamburgische Beihilfeverordnung, die das Verfahren der Beihilfefähigkeitsfeststellung bei Psychotherapien nunmehr den Richtlinien des Bundesausschusses der Ärzte und Krankenkassen (Psychotherapie-Richtlinien) unterwirft. Diese sehen insbesondere vor, daß die Beihilfefähigkeit von externen Gutachtern in einem anonymisierten Verfahren beurteilt wird. Dies erfüllt die seit längerem bestehende Forderung des Hamburgischen Datenschutzbeauftragten. Das Personalamt hat jedoch wissen lassen, daß es auf die Erfahrung des bisher tätigen Arztes nicht ganz verzichten, sondern ihn auch weiterhin als Gutachter einsetzen will, „wenn – aus welchen Gründen auch immer – eine externe Begutachtung nicht möglich ist oder nicht zweckmäßig erscheint"; für diese Fälle ist jedoch ein anonymes Verfahren vorgesehen. Es kommt nun darauf an, das neue Verfahren in die Praxis umzusetzen und datenschutzrechtlichen Anforderungen im Detail gerecht zu werden.

7.5.2 Beihilfe für Angehörige

Das gegenwärtige Beihilferecht sieht vor, daß Angehörige von öffentlich Bediensteten ihre Aufwendungen für Arzt und Krankenhausbesuche nur in der Weise zurückerstattet bekommen können, daß die Bediensteten einen entsprechenden Antrag auf Beihilfe stellen. Eine direkte Antragstellung eines Angehörigen bei der Beschäftigungsstelle ist danach nicht möglich. Insbesondere bei voneinander getrennt lebenden Ehegatten oder sonstigen Beziehungsstörungen in der Familie kann dieses Verfahren zu ernsten Nachteilen für die Angehörigen führen. So berichtete eine Petentin davon, daß ihr beihilfeberechtigter Ehemann, von dem sie getrennt lebt, die Beihilfeunterlagen seiner Frau auch seiner neuen Lebenspartnerin zur Kenntnis gibt oder den notwendigen Beihilfeantrag gar nicht oder sehr spät stellt.

Diese Problematik hat zu einer intensiven Diskussion sowohl unter den Datenschutzbeauftragten des Bundes und der Länder wie auch in den für das Beihilferecht zuständigen Behörden geführt. Die Bund-Länder-Kommission für das Beihilferecht hat sich aus dienstrechtlichen Gründen jedoch nicht in der Lage gesehen, Familienangehörigen einen eigenen Beihilfeanspruch einzuräumen. Das Recht des Öffentlichen Dienstes sei auch nicht mit dem der gesetzlichen Krankenversicherung vergleichbar, das die vollständige Abhängigkeit der Familienangehörigen von dem Arbeitnehmer vermeidet.

Weil die durch das gegenwärtige Beihilferecht möglichen Unzuträglichkeiten allseits anerkannt werden, wird die Suche nach Lösungen fortgesetzt. Das

Senatsamt für den Verwaltungsdienst hat die Berechtigung der datenschutzrechtlichen Bedenken eingeräumt und eigene intensive Bemühungen um eine zufriedenstellende Klärung auf Bund-Länder-Ebene zugesagt.

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.

7.5.3 Speicherung von Beihilfedaten

Zum Datenschutz bei der Zentralisierung der Beihilfefestsetzung in der Besoldungs- und Versorgungsstelle haben das Senatsamt für den Verwaltungsdienst und die Spitzenverbände der Gewerkschaften des öffentlichen Dienstes am 28. Februar 1991 eine Vereinbarung getroffen, in der auch die Erfassung und elektronische Verarbeitung der Daten aus den Beihilfeunterlagen geregelt wird. Um sicherzustellen, daß ein Antragsteller nicht aufgrund derselben Arzt-/Krankenhaus-Rechnungen ein zweites Mal Beihilfe erhält, werden die Daten – ohne die Diagnose – 15 Monate gespeichert. Dabei wird auch die Art der Aufwendung („Arztkosten ambulant", „Sanatorium", „Medikamente" usw.) festgehalten.

Auf Grund unserer Initiative wurde die zuvor vorgesehene Kategorie „Psychotherapie" als eigene Aufwendungsart gestrichen und der Aufwendungsart „Ambulante Arztkosten" zugeordnet. Auf diese Weise ist eine besondere Auswertung und auch ein Mißbrauch dieses besonders sensiblen, mit einer Diagnose vergleichbaren Datums ausgeschlossen.

7.6 Wahlordnungen für Personalräte und Schwerbehindertenvertretungen

Anläßlich der letzten Wahlen für die Personal- und Schwerbehindertenvertretungen erreichten uns mehrere Eingaben. Zum einen wurde kritisiert, daß das Wählerverzeichnis für die Personalratswahlen das vollständige Geburtsdatum der Wahlberechtigten enthält und von sämtlichen Mitarbeitern eingesehen werden kann. Zum anderen wandten sich schwerbehinderte Bedienstete dagegen, daß die Wählerlisten, die nur Schwerbehinderte ausweisen, in den Behörden offen ausgelegt werden und daß bei der Briefwahl bereits das Adressenetikett mit dem Absender „Wahlvorstand für die Schwerbehinderten-Vertrauensleute" versehen ist.

Hinsichtlich der Wählerverzeichnisse wird diese Praxis durch die jeweiligen Wahlordnungen bestimmt. Im Schreiben an das Senatsamt für den Verwaltungsdienst sowie an die Behörde für Arbeit, Gesundheit und Soziales – Hauptfürsorgestelle – wurde deswegen angeregt, eine entsprechende Änderung der Wahlordnungen zu veranlassen.

Das Senatsamt für den Verwaltungsdienst „hat sich den Punkt für eine Änderung der Wahlordnung zum Hamburgischen Personalvertretungsgesetz vorgemerkt" und erklärte sich damit einverstanden, daß im Vorgriff auf diese Änderung schon jetzt die in der Dienststelle zur Einsichtnahme auszulegenden Wählerverzeichnisse die Geburtsdaten der Wahlberechtigten nicht mehr enthalten. Der Wahlvorstand müsse allerdings zu Überprüfungszwecken eine Liste mit Geburtsdaten erhalten.

Die Hauptfürsorgestelle hat das Schreiben des Datenschutzbeauftragten an die Arbeitsgemeinschaft der Deutschen Hauptfürsorgestellen weitergeleitet, ohne eine eigene Bewertung des Sachverhalts vorzunehmen. Auch auf unseren konkreten Vorschlag, die Adressierung der Briefwahlunterlagen so zu gestalten, daß nicht bereits der Briefumschlag den Empfänger als Schwerbehinderten identifiziert, haben wir bisher trotz Erinnerungen keine Antwort erhalten.

8. Statistik

8.1 Automationsprojekte

8.1.1 Datenvermittlungssystem der Statistischen Ämter

Das Statistische Landesamt Hamburg ist inzwischen – über die Datenverarbeitungszentrale (DVZ) – an das Datenvermittlungssystem Nordrhein-Westfalen (DVS) angeschlossen, mit dem die Statistischen Ämter Programme und Daten austauschen. Das DVS benutzt den Datex-P-Dienst der Deutschen Bundespost TELEKOM. Mit der Teilnahme an DVS ist die Datenverarbeitungszentrale erstmalig über Wählanschlüsse mit einem Telekommunikationsnetz verbunden (vgl. 8. TB, 2.4).

Bei der Einrichtung der Anschlüsse wurde seitens der DVZ großer Wert darauf gelegt, daß nur mit definierten Partnersystemen kommuniziert werden kann und daß Unbefugte nicht in Systeme der DVZ eindringen können. Auf die übertragenen Daten kann nur unter Kontrolle des in der DVZ eingesetzten Sicherheitssystems zugegriffen werden. Wir haben deshalb keine Bedenken gegen den Anschluß erhoben, zumal das neue Verfahren an die Stelle des ebenfalls mit Risiken verbundenen Magnetbandaustausches tritt.

8.1.2 Lokales Netzwerk des Statistischen Landesamtes

Mit der geplanten Einführung eines Lokalen Netzwerkes beabsichtigt das Statistische Landesamt, eine Vielzahl von – z.T. bisher manuell durchgeführten – Arbeiten maschinell zu unterstützen. Ein zentrales Anliegen dabei ist es, die auch weiterhin mittels Großrechnerverfahren erzeugten Daten zu verdichten, auszuwerten, aufzubereiten und den Nutzern zur Verfügung zu stellen. Längerfristig wird das System möglicherweise auch bei der Datenerhebung bzw. der Organisation von Zählungen eingesetzt werden. Mittels Terminalemulation sollen PC über den Server auf in der DVZ gespeicherte Daten zugreifen können. Dabei wird es sich auch um statistische Einzelangaben bestimmter Zählungen handeln, die online korrigiert werden sollen.

Angesichts des übergreifenden Charakters des Netzwerks, das 44 in verschiedenen Fachabteilungen untergebrachte Personalcomputer umfassen soll, muß gewährleistet sein, daß die Benutzer jeweils nur auf die Daten zugreifen können, für die sie berechtigt sind. Auch muß gewährleistet werden, daß die Daten nicht auf die lokalen PC heruntergeladen werden können. Ferner müssen die Rechte und Pflichten der Systemverwalter definiert werden.

Diese Zielvorstellungen werden vom Statistischen Landesamt geteilt. Bislang liegt uns jedoch das angekündigte Sicherheitskonzept nicht vor, auf dessen Grundlage sich beurteilen ließe, inwieweit das Netz den datenschutzrechtlichen Anforderungen gerecht wird (vgl. hierzu auch 3.5).

8.1.3 Statistisches Informationssystem (STATIS-Hamburg)

Im Rahmen einer Projektorganisation plant das Statistische Landesamt ein integriertes statistisches Informationssystem, das statistische Daten aus verschiedenen Quellen (z.B. Volkszählung, Mikrozensus, Handels- und Gaststättenzählung) umfassen soll. Die Daten sollen in einer Statistik-Datenbank zusammengefaßt werden, die den Kern des Systems bilden wird. Das Projekt ist eingebettet in das von verschiedenen Kommunen getragene Gemeinschaftsprojekt KOSIS (Kommunales Statistisches Informationssystem).

Angestrebt wird ein aussagekräftiger und aktueller Datenbestand, der sich entsprechend den „Kundenwünschen" flexibel auswerten läßt. Als Empfänger kommen sowohl öffentliche als auch private Stellen in Frage.

Die datenschutzrechtliche Bedeutung von STATIS liegt darin, daß hier unter anderem statistische Einzelangaben verarbeitet werden sollen, die – auch wenn die Daten „faktisch anonymisiert" sind – mit entsprechendem Zusatzwissen wieder einzelnen Personen zugeordnet werden könnten. Durch entsprechende „Filter" soll sichergestellt werden, daß nur solche Daten übermittelt werden, die von den Datenempfängern außerhalb des Statistischen Landesamtes nicht reidentifiziert werden können.

8.2 Hamburgisches Statistikgesetz

Mit dem neuen Hamburgischen Statistikgesetz (HmbStatG) verfügt Hamburg nunmehr über eine Rechtsgrundlage für Landesstatistiken und (ergänzend zum Bundesrecht) auch für die Durchführung von Bundestatistiken und EG-Statistiken.

Leider sind Senat und Bürgerschaft unseren Anregungen im wesentlichen nicht gefolgt, die darauf abzielten, datenschutzrechtliche Belange stärker zu berücksichtigen (vgl. 8. TB, 3.3.1 und 9. TB, 4.3.1). Nicht befriedigen können insbesondere die Vorschriften des § 8 über die Erstellung von Geschäftsstatistiken. Für solche Statistiken dürfen, „soweit dies zur Erreichung des mit der Geschäftsstatistik verfolgten Zwecks zwingend geboten ist", auch Daten aus Geschäftsvorgängen mit unterschiedlichem Sachbezug zusammengeführt werden, ohne daß eine spezielle Rechtsvorschrift dies vorsieht.

8.3 Mißbrauch von DVZ-Kennungen

Anläßlich einer Eingabe hatten wir uns mit der Einhaltung datenschutzrechtlicher Vorgaben für die automatisierte Datenverarbeitung bei dem Verfahren „Datei im produzierenden Gewerbe" auseinanderzusetzen.

Dabei hat sich herausgestellt, daß im Statistischen Landesamt für die Produktion eingerichtete – und damit mit Zugriffsberechtigung auf personenbezogene Echtdaten versehene – Benutzerkennungen nicht nur von den berechtigten Inhabern, sondern auch von Programmierern genutzt wurden. Damit wurde wiederholt gegen den in verschiedenen verbindlichen Regelungen festgeschriebenen Grundsatz der Trennung von Test und Produktion verstoßen. Dies ist geschehen, obwohl das Statistische Landesamt bereits anläßlich einer Prüfung desselben Verfahrens im Jahr 1988 zugesagt hatte, durch technische und organisatorische Maßnahmen die Trennung von Test und Produktion sicherzustellen (vgl. 7. TB, 3.1.1).

Mit der gemeinsamen Nutzung von Benutzerkennungen werden alle Bemühungen unterlaufen, durch konsequenten Einsatz von Sicherheitsmechanismen und Festlegung von Benutzerprofilen den Zugriff auf echte Daten zu steuern. Dies wiegt um so schwerer, als die „Mehrfachnutzung" der Produktionskennungen mit Wissen und im Auftrag der zuständigen Fachabteilungen geschah und die Programmierer die echten Daten bearbeiten sollten, ohne daß dabei die erforderlichen Verfahrenssicherungen gewährleistet waren.

9. Schulwesen

9.1 Noch kein neuer Schulgesetzentwurf

Im 9. TB (4.5) war berichtet worden, daß ein neuer Referentenentwurf zur Änderung des Schulgesetzes existiert, der die Einfügung von Datenschutzbestimmungen in das Schulgesetz vorsieht.

Dieser Entwurf entspricht mit geringfügigen Änderungen einem früheren Entwurf, der in den Jahren 1985/1986 diskutiert wurde. Gegenüber der Behörde für Schule, Jugend und Berufsbildung (BSJB) hatten wir diesen Referentenentwurf bereits als ungenügend kritisiert, da er hinter den Anforderungen an einen modernen Datenschutz, wie er sich beispielsweise im Gesetz zum Datenschutz im Schulwesen Bremens niederschlägt, weit zurückbleibt. Insbesondere enthält der Entwurf selbst zu so fundamentalen Fragen, wie denen der automatisierten Datenverarbeitung, lediglich eine viel zu weit gehende Verordnungsermächtigung und ist auch im übrigen so allgemein gehalten, daß die Betroffenen eben nicht in der verfassungsmäßig erforderlichen Art und Weise nachvollziehen können, wer wann was über sie weiß. Selbst die „Hinweise zur Datenverarbeitung und Datensicherung in den Schulen und Dienststellen („Datenschutz-Info")" vom 10.April 1985, die ihre Existenz nur dem gesetzlichen Regelungsdefizit verdanken und mit einer Schulgesetzreform obsolet werden

sollten, äußern sich zu wichtigen Fragen der Datenverarbeitung teilweise konkreter.

Auf unsere Nachfrage, ob und wie dieser Entwurf inzwischen weiterentwickelt wurde, mußten wir von der BSJB erfahren, daß der Referentenentwurf noch unverändert ist und ein Änderungsgesetzentwurf dem Senat 1992 vorgelegt werden soll. Aufgrund des weiterhin erheblichen Ergänzungsbedarfes für den bestehenden Gesetzentwurf muß jedoch mit einer weiteren Verzögerung gerechnet werden.

9.2 Schülerdatenverarbeitung auf Privat-PC der Lehrer

Da in Hamburg auch acht Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts für den Schulbereich noch keine bereichsspezifischen Datenschutzregelungen geschaffen wurden, bestimmt sich der Datenschutz im wesentlichen weiterhin nach dem von der damaligen Behörde für Schule und Berufsbildung (BSB) herausgegebenen „Datenschutz-Info" vom 10. April 1985.

Diese Hinweise lassen Verwaltungsarbeiten (Klassenlisten, Zensurenspiegel etc.) in automatisierter Form nur in der Schule und auf ausschließlich dazu bestimmten Rechnern zu. Damit ist es Lehrern verboten, solche Arbeiten zu Hause auf ihren vielfach vorhandenen privaten PC vorzunehmen.

Damit soll verhindert werden, daß die Lehrer eine automatisierte Datenverarbeitung vornehmen, ohne dabei die erforderlichen Datensicherungsmaßnahmen zu treffen. Die Verantwortung für die Datensicherheit trägt dabei die Schule, da sie rechtlich gesehen die speichernde Stelle ist.

Gleichwohl ist bekannt und von der BSJB unbestritten, daß dennoch viele Lehrer ihre privaten PC für Verwaltungsarbeiten nutzen. Um der Realität gerecht zu werden und zugleich dem Schutz der Betroffenen, nämlich der Schüler, Rechnung zu tragen, haben wir vorgeschlagen, statt des Verbots eine grundsätzliche Gestattung des Privat-PC-Einsatzes auszusprechen, die an bestimmte Bedingungen zu knüpfen wäre. Eine derartige Lösung des Problems gibt es bereits in Bayern, Rheinland-Pfalz und Niedersachsen.

Zu den erforderlichen Bedingungen, die in diesem Zusammenhang diskutiert werden müssen, gehören die

— Genehmigung des PC-Einsatzes durch den Schulleiter oder die Behörde,

— die Begrenzung der zu verarbeitenden Datenarten (Gesundheitsdaten dürften z.B. nicht zugelassen werden),

— die ausdrückliche Bindung der Lehrer an das Datengeheimnis,

— bestimmte Maßnahmen zur technischen Datensicherung,

— die Gewährleistung der Betroffenenrechte (Auskunftsanspruch usw.),

— eine Dateimeldung und

— die Gewährleistung des Kontrollrechts des Hamburgischen Datenschutzbeauftragten.

In einer ersten Stellungnahme hat sich die BSJB grundsätzlich zustimmend zu einer solchen Lösung geäußert. Einzelheiten konnten bis Redaktionsschluß jedoch noch nicht festgelegt werden.

10. Steuerwesen

10.1 Änderung der Abgabenordnung (AO)

In Zusammenarbeit mit den obersten Finanzbehörden der Länder bereitet das Bundesministerium der Finanzen seit längerem eine Änderung der Abgabenordnung vor. Im Mittelpunkt steht dabei die Neufassung insbesondere des § 30 AO; sie soll der neueren Datenschutzgesetzgebung Rechnung tragen und den Umgang mit Daten, die dem Steuergeheimnis unterliegen, klarer als bisher regeln. Soweit die AO keine bereichsspezifischen Datenschutzvorschriften enthält, sollen ergänzend die Vorschriften des Bundesdatenschutzgesetzes (BDSG) anwendbar sein. Dies entspricht für den Bereich der Bundesfinanzbehörden dem geltenden Recht.

Die ergänzende Anwendung des BDSG soll gemäß dem Referentenentwurf in Verfahren nach der AO aber auch auf die Landesfinanzbehörden, für die bisher die Datenschutzgesetze der Länder gelten, ausgedehnt werden. Begründet wird dieser Schritt damit, daß die Landesfinanzbehörden bundeseinheitlich materielles Recht (z.B. Einkommen-, Körperschaft-, Umsatzsteuergesetz) und Verfahrensrecht (AO mit Nebengesetzen) anzuwenden haben. Deshalb sei in Verfahren nach der AO auch bundeseinheitliches Datenschutzrecht zugrunde zu legen, weil dieses mit dem Verfahrensrecht untrennbar verbunden sei. Der Gesetzentwurf zur Änderung der Abgabenordnung sah dabei ursprünglich wörtlich vor, daß für die Rechte und Pflichten der Landesdatenschutzbeauftragten die Vorschriften der Landesdatenschutzgesetze nur noch gegenüber anderen öffentlichen Stellen als den Landesfinanzbehörden gelten sollen.

Eine solche Verdrängung der bestehenden Bestimmungen in den Landesdatenschutzgesetzen ist verfassungsrechtlich unzulässig und nicht hinnehmbar.

Die beteiligten Behörden sind darauf hingewiesen worden, daß derartige Regelungen bereits im Bundesrat verhindert werden sollen. Die Datenschutzbeauftragten der Länder haben auf der Konferenz am 26./27. September 1991 übereinstimmend festgehalten: „Grundsätzlich gelten auch im Abgabenrecht die Landesdatenschutzgesetze. In der Abgabenordnung dürfen bereichsspezifische materiellrechtliche Regelungen des Datenschutzrechts nur getroffen werden, soweit dies wegen der Besonderheiten des Abgabenrechts erforderlich ist." Damit sollte vor allem zum Ausdruck gebracht werden, daß sich das Kontrollrecht der Datenschutzbeauftragten und das dabei angewendete Verfahren ausschließlich nach den landesrechtlichen Regelungen richtet.

In der Sitzung des Arbeitskreises Steuerverwaltung der Datenschutzbeauftragten von Bund und Ländern am 8. Oktober 1991 wurde die verfassungsrechtliche Problematik mit Vertretern des Bundesfinanzministeriums ausführlich erörtert. Es bestand Einvernehmen darin, im Gesetzesentwurf die in den Landesdatenschutzgesetzen geregelten Kontrollrechte durch die Anwendung des Bundesdatenschutzgesetzes nicht einzuschränken. Dasselbe gelte für die Mitwirkung der Landesdatenschutzbeauftragten beim Erlaß von Verwaltungsvorschriften und für die inhaltliche Bestimmung der Dateiregistermeldungen. Ein entsprechender Vorbehalt soll in den Text des Änderungsgesetzes aufgenommen werden.

In einer geänderten Fassung des Referentenentwurfs von Ende November 1991 heißt es nunmehr, „die Vorschriften der Landesdatenschutzgesetze über die Bestellung, die Rechtsstellung und die Rechte und Pflichten der Landesdatenschutzbeauftragten bleiben unberührt". Demnach würde es bei dem derzeitigen Rechtszustand bleiben, daß die Überprüfung der Landesfinanzbehörden durch die Landesdatenschutzbeauftragten sich nach den Landesdatenschutzgesetzen richtet.

Unverändert ist dagegen vorgesehen, daß das Bundesdatenschutzgesetz materiell als ergänzendes Recht statt der Landesdatenschutzgesetze für die Landesfinanzbehörden gelten soll. Insoweit bleibt gemäß der übereinstimmenden Auffassung der Landesdatenschutzbeauftragten weiterhin kritisch zu prüfen, ob und inwieweit wegen der Besonderheiten des Abgabenrechts eine ergänzende Anwendung des Bundesdatenschutzgesetzes gemäß dem derzeitigen Entwurf der Abgabenordnung wirklich erforderlich ist.

Die zur Zeit aktuelle Fassung des Änderungsgesetzentwurfs berücksichtigt ferner noch immer nicht alle wiederholt von den Landesdatenschutzbeauftragten vorgetragenen Forderungen.

So bedürfen u.a. die bisherigen Regelungen der AO zur Wahrung gesetzlicher Geheimhaltungsverpflichtungen oder besonderer Berufs- und Amtsgeheimnisse einer Anpassung, wie sie in anderen neuen Gesetzen (z. B. dem Bundesverfassungsschutzgesetz) bereits zum Ausdruck gekommen ist. Hierzu gehört vor allem der ausdrückliche Schutz des Sozialgeheimnisses und die Anerkennung der ärztlichen Schweigepflicht bei Auskünften öffentlicher Stellen gegenüber den Finanzbehörden (§ 105 AO). Die bisher geltenden Bestimmungen zum Auskunftsverweigerungsrecht in § 102 AO sollten ferner dem Katalog der in § 203 Strafgesetzbuch aufgezählten Berufsgeheimnisse angeglichen werden; § 116 Abs. 2 AO (Anzeige von Steuerstraftaten) sollte hierauf verweisen bzw. eine entsprechende Regelung zur Wahrung gesetzlicher Geheimhaltungspflichten und besonderer Amts- und Berufsgeheimnisse erhalten.

Der Gesetzentwurf verzichtet auch weiterhin darauf, die Befugnisse der Steuerfahndung nach § 208 AO genauer zu definieren. Die bisher von der Rechtsprechung entwickelten Grundsätze, nach der Ermittlungen nur zulässig seien,

wenn ein hinreichender Anlaß hierfür bestünde und die Möglichkeit einer objektiven Steuerverkürzung vorliege, sollten in Hinblick auf das verfassungsrechtliche Gebot der Normenklarheit in § 208 AO aufgenommen werden.

10.2 Private PC im Betriebsprüfungsdienst

In der hamburgischen Steuerverwaltung werden Personal-Computer für die Aufgabenerfüllung im Betriebsprüfungsdienst der Finanzämter genutzt. Den Betriebsprüfern stehen dienstlich beschaffte Geräte zur Verfügung, deren Einsatz hinsichtlich der nach § 8 HmbDSG zu treffenden technischen und organisatorischen Sicherungsmaßnahmen bisher nur in einer vorläufigen Dienstanweisung geregelt ist. Die Steuerverwaltung beabsichtigte, die hierin enthaltenen Vorgaben an das im vergangenen Jahr veröffentlichte Schutzstufenkonzept für Einzelplatzrechner (9. TB, 3.2) anzupassen, allerdings ohne gleichzeitig die bisher geduldete Nutzung privater PC zumindest einzuschränken.

Da die Beschaffung einer ausreichenden Zahl dienstlicher Geräte noch nicht erfolgen konnte, werden von vielen Betriebsprüfern eigene Rechner zur Aufgabenerledigung benutzt. Die Steuerverwaltung hat zwar 1985 per Erlaß eine einengende Regelung für den Einsatz privater PC zu dienstlichen Zwecken getroffen. Danach dürfen Daten, die dem Steuergeheimnis gemäß § 30 AO unterliegen, nicht auf externen privateigenen Datenträgern gespeichert werden. Dieser Erlaß bedarf aber in Hinblick auf die veränderten technischen und rechtlichen Rahmenbedingungen dringend einer Überarbeitung.

Mit dem Einsatz privater PC zu dienstlichen Zwecken sind erhebliche datenschutzrechtliche Bedenken verbunden (siehe 3.8). Da sich die Finanzbehörde zur Zeit nicht in der Lage sieht, die Verwendung privater Geräte umgehend einzustellen, haben wir nach mehreren Gesprächen mit Vertretern der Steuerverwaltung und der Oberfinanzdirektion vereinbart, eine Dienstanweisung für den Betriebsprüfungsdienst zu erstellen, die sowohl den Einsatz dienstlicher als auch vorhandener privateigener PC verbindlich regelt. Darin wird der Einsatz privater Arbeitsplatzrechner für dienstliche Zwecke grundsätzlich untersagt.

Unter der Voraussetzung, daß umgehend die zur Beschaffung einer ausreichenden Zahl dienstlicher Geräte erforderlichen Mittel im Haushalt vorgesehen werden, können bereits vorhandene private PC für eine festzulegende Übergangszeit weiterhin genutzt werden. Dies gilt nur dann, wenn

- für den Einsatz privateigener Technik eine Genehmigung durch den Dienststellenleiter eingeholt und schriftlich festgehalten worden ist,
- entsprechend § 9 Abs. 3 HmbDSG die privaten DV-Anlagen in einem Geräteverzeichnis geführt werden,
- die betroffenen Systeme entsprechend den dienstlichen Geräten mit Sicherungssoftware ausgestattet werden,

— die Anwender verpflichtet werden, Daten nicht auf vorhandenen Festplatten, sondern nur über ein zur Verfügung gestelltes Verschlüsselungsprogramm auf dienstlichen Disketten zu speichern,

— diese Disketten zentral im Finanzamt verwaltet und archiviert werden,

— die Eigentümer privater Geräte sich schriftlich den festgelegten Einsatzbedingungen unterwerfen.

Rechner, die die technischen Anforderungen für den Einsatz des Verschlüsselungsprogramms nicht erfüllen, bleiben generell vom dienstlichen Einsatz ausgeschlossen.

Die Steuerverwaltung beabsichtigt, zukünftig tragbare Rechner zu beschaffen. Der mobile Einsatz transportabler PC käme den Belangen der Betriebsprüfer vor Ort entgegen, er birgt jedoch gegenüber stationären PC zusätzliches Gefährdungspotential wie den Diebstahl oder den Verlust des gesamten Gerätes. Organisatorische und bauliche Maßnahmen zur Zutrittssicherung lassen sich insoweit kaum treffen. Die Nutzung tragbarer Rechner bedarf daher der besonderen Beachtung zusätzlicher datenschutzrechtlicher Maßnahmen, die in die Dienstanweisung für den Betriebsprüfungsdienst aufzunehmen sind. Hierzu zählen das grundsätzliche Anlegen und regelmäßige Überprüfen von Zugriffsprotokolldateien auf den Systemen und das Sperren der Schnittstellen, um unbefugten Datenaustausch mit externen Rechnern zu verhindern. Das Verbot, personenbezogene Daten auf Festplatten zu speichern, sollte darüberhinaus auf die bei tragbaren Rechnern zunehmend üblichen batteriegepufferten Internspeicher ausgedehnt werden.

10.3 Zeichnungsvorbehalt der Finanzamtsvorsteher

Von Mitarbeitern der Finanzverwaltung wird kritisiert, daß ihre Dienstvorgesetzten durch eine Regelung in der bundeseinheitlich geltenden Geschäftsordnung für die Finanzämter (FAGO) weitreichende Einblicke in ihre persönlichen Verhältnisse erhalten, die unter Umständen Einfluß auf Entscheidungen im beamten- und personalrechtlichen Bereich gewinnen könnten.

Nach § 23 Abs.1 Nr. 4 FAGO hat der Finanzamtsvorsteher die Steuerangelegenheiten von Amtsangehörigen abschließend zu zeichnen. Mit dieser Vorschrift wird der Zweck verfolgt, einer unzulässigen Bevorzugung bei der Bearbeitung von Steuererklärungen unter Kollegen vorzubeugen. Unbestreitbar erhalten durch diese Regelung aber Dienstvorgesetzte über die geltendgemachten privaten Aufwendungen Kenntnis von den persönlichen Lebensverhältnissen der ihnen unterstellten Mitarbeiter. Für die Betroffenen ist darin eine unverhältnismäßige Beeinträchtigung ihres informationellen Selbstbestimmungsrechts zu sehen.

Die Referatsleiter Organisation der obersten Finanzbehörden der Länder haben auf entsprechende Initiativen der Landesdatenschutzbeauftragten die Problematik des Zeichnungsvorbehalts der Finanzamtsvorsteher mehrfach

erörtert. Für unsere Anregung, § 23 Abs. 1 Nr. 4 FAGO so zu verändern, daß Informationen aus Steuerfällen künftig nicht in Personalentscheidungen einfließen können, fand sich im März 1991 jedoch keine Mehrheit. Die bereits vorhandene Möglichkeit, nach § 27 AO auf persönlichen Wunsch des Betroffenen eine Zuständigkeitsvereinbarung zu treffen und die Besteuerung durch ein anderes Finanzamt vornehmen zu lassen, wurde als ausreichend angesehen. Eine generelle Überarbeitung des Zeichnungsrechts ist zwar in Hinblick auf die neuen Bundesländer beschlossen worden. Sie dürfte allerdings kurzfristig nicht zu realisieren sein.

Anders als die Finanzbehörde sind wir der Auffassung, daß bei entsprechender Konstellation grundsätzlich eine abweichende örtliche Zuständigkeit festgelegt werden sollte. Die hamburgische Praxis stellt bisher darauf ab, daß ein Betroffener von sich aus den Wunsch äußert, bei einem anderen Finanzamt steuerlich veranschlagt zu werden. Ein solches Verfahren ist übergangsweise nur dann zu akzeptieren, wenn die Betroffenen ausdrücklich auf ihr Recht hingewiesen werden, ihre Steuerangelegenheiten von einem anderen Finanzamt bearbeiten zu lassen, und in entsprechenden Fällen eine Verlagerung der Zuständigkeit ausnahmslos vorgenommen wird.

Die Oberfinanzdirektion Hamburg ist veranlaßt worden, in geeigneter Form sicherzustellen, daß alle Mitarbeiter in der Finanzverwaltung über ihren Anspruch auf Verlagerung der Bearbeitung ihrer Steuerangelegenheiten in Kenntnis gesetzt werden.

11. Wissenschaft und Forschung

11.1 Interviews mit Zeitzeugen der NS-Zeit und des KZ Neuengamme

Die Forschungsstelle für die Geschichte des Nationalsozialismus in Hamburg sowie die KZ-Gedenkstätte Neuengamme berichteten unabhängig voneinander von ihrer Absicht, Zeitzeugen des Nationalsozialismus bzw. ehemalige KZ-Häftlinge zu befragen und diese Zeugnisse zu dokumentieren.

Die datenschutzrechtliche Beratung bezog sich vor allem auf die vollständige Aufklärung der Interviewpartner über Form und Nutzung der Dokumentation sowie auf die Formulierung der Einverständniserklärung. Die Gesprächspartner sollten von vornherein die Möglichkeit erhalten, die Speicherung der Aussagen ganz oder teilweise abzulehnen oder die Verwendung für Veröffentlichungen und für Forschungszwecke nur in anonymisierter Form zu gestatten. Die beteiligten Forscherinnen sahen in der größtmöglichen Offenheit und informationellen Selbstbestimmung der potentiellen Gesprächspartner auch einen Beitrag zur notwendigen Vertrauensbasis für einen erfolgreichen Verlauf des Projekts.

Noch nicht abgeschlossen ist die datenschutzrechtliche Bewertung der technischen Speicherung mit dem Programm LIDOS und der notwendigen Sicherungsmaßnahmen.

11.2 Forschungsvorhaben im Justizbereich

Im Berichtszeitraum waren wir in einer Reihe von Forschungsprojekten, deren empirische Grundlage Justizakten sind, mit datenschutzrechtlichen Gesichtspunkten befaßt. Den rechtlichen Rahmen für die „Offenbarung personenbezogener Daten aus Akten für Forschungszwecke" stellt die Allgemeine Verfügung der Justizbehörde Nr. 12/1988 vom 27. September 1988 dar.

Besonders erwähnenswert ist das Forschungsprojekt „Neuere Hamburger Justizgeschichte". Hier geht es um eine Untersuchung des Wirkens der Hamburger Justiz in der Zeit der nationalsozialistischen Herrschaft und der ersten beiden Nachkriegsjahrzehnte. Es handelt sich um ein groß angelegtes Projekt, in dem die bislang vorliegenden wissenschaftlichen Ergebnisse zur Analyse der Justiz im Nationalsozialismus auf die spezifischen Hamburger Verhältnisse hin konkretisiert werden sollen. Im Kontext dieses Projekts bildet die Untersuchung der Justizjuristen einen Schwerpunkt. Beispielsweise werden Fragen wie die nach Ausbildungs- und Karriere-Weg der Justizjuristen, ihrer weltanschaulichen Orientierung und „subjektiven Befindlichkeit" thematisiert. Es liegt auf der Hand, daß hier personenbezogene Daten sensiblen Ausmaßes Gegenstand der Forschung sind.

In Abstimmung mit dem Präsidenten des Hanseatischen Oberlandesgerichts sind für die Verwertung personenbezogener Daten aus dort vorhandenen Akten die Details einer zulässigen personenbezogenen Datenverarbeitung für das Projekt definiert worden. Insbesondere ist Wert darauf gelegt worden, einerseits das Interessse der Wissenschaft zum Zuge kommen zu lassen, andererseits durch Anonymisierung der Namen der jeweils konkret betroffenen Justizjuristen deren schutzwürdige Belange oder, soweit sie verstorben sind, die schutzwürdigen Belange ihrer Nachkommen zu berücksichtigen.

Durch diese Vorgehensweise ist das wissenschaftliche Auswertungsinteresse nicht beeinträchtigt, zumal die Namen anderer Personen einschließlich der Gerichtspräsidenten, die in dem Verfahren nicht als Spruchrichter mitgewirkt haben, als Personen der Zeitgeschichte genannt werden können. Nicht erfaßt von der Auswertung sind noch verfügbare Handakten der Staatsanwaltschaft und andere innerdienstliche Vorgänge, da sie nach den Richtlinien für das Strafverfahren und das Bußgeldverfahren nicht einer Einsicht zugänglich sind.

Im Zusammenhang mit diesem Projekt haben wir die Justizbehörde darauf hingewiesen, daß die Allgemeine Verfügung vom 27. September 1988 dem inzwischen neu gefaßten § 27 HmbDSG über Datenverarbeitung zum Zwecke wissenschaftlicher Forschung anzupassen ist.

12. Bauwesen

12.1 Prüfung des Fehlbelegungsabgabe-Verfahrens

Bei der Prüfung des Fehlbelegungsabgabe-Verfahrens, das die Mietenausgleichszentrale (MAZ) als eine Abteilung der Hamburgischen Wohnungsbaukreditanstalt (WK) durchführt, haben wir schwerwiegende datenschutzrechtliche Verstöße festgestellt. Das Verfahren wurde Ende 1989 mit dem wohnungsbaupolitischen Ziel beschlossen, daß diejenigen Mieter eine Fehlbelegungsabgabe zahlen sollen, die aufgrund ihres Einkommens nicht mehr berechtigt sind, in öffentlich geförderten Wohnungen zu wohnen.

Datenschutzrechtlich konnte das Fehlbelegungsverfahren allerdings erst jetzt geprüft werden, da sich die WK über ein Jahr weigerte und auch nur aufgrund eines Senatsbeschlusses dazu veranlaßt werden konnte, die datenschutzrechtliche Prüfung der MAZ durch den Hamburgischen Datenschutzbeauftragten zu ermöglichen. Der Senat hat sich bei seiner Entscheidung weitgehend an unsere Rechtsauffassung gehalten, die bereits im 9. TB (4.8.2.2) ausführlich beschrieben und dabei der Auffassung der WK gegenübergestellt wurde.

Nunmehr haben sich jedoch unsere Bedenken voll bestätigt. Da die im folgenden noch ausführlicher dargestellten datenschutzrechtlichen Verstöße in fast allen geprüften Akten festgestellt wurden, die Umsetzung datenschutzrechtlicher Aspekte zudem durch keinerlei schriftliche Dokumente wie z.B. Dienstanweisungen geregelt ist, kann allerdings nicht von einem Fehlverhalten des jeweils zuständigen Sachbearbeiters ausgegangen werden, sondern von einem Organisationsmangel auf der Leitungsebene der MAZ und der WK:

— Der schwerwiegendste datenschutzrechtliche Verstoß liegt darin, daß sämtliche Dokumente von über 60 000 Mietern kopiert zur Akte genommen wurden, die bei der MAZ vorgelegt wurden. Verdienstbescheinigungen, Einkommens- und Lohnsteuerbescheide, Wohngeld- und Sozialhilfebescheide, Bescheide über Arbeitslosengeld oder Arbeitslosenhilfe, Kontoauszüge, Urteile aus Unterhaltsklagen samt Begründung sowie Bescheide vom Versorgungsamt über die Anerkennung einer Schwerbehinderung, die in diesem Umfang gar nicht benötigt werden, werden mit einer Vielzahl persönlicher Angaben in den Akten auf unbestimmte Zeit aufbewahrt. Diese Datensammlung trifft hauptsächlich einen Personenkreis von einkommensschwachen Mietern, die in der Regel überhaupt keine Abgabe zu zahlen brauchen. Diejenigen Mieter dagegen, die sich aufgrund ihres hohen Verdienstes freiwillig zu einer Zahlung bereit erklärt haben, müssen keine Angaben gegenüber der Mietenausgleichszentrale machen. Somit werden umfangreiche Daten gerade von Mietern gespeichert, für die das wohnungspolitische Instrument der Fehlbelegungsabgabe eigentlich nicht greift.

— Um Einkommensangaben des Mieters zu überprüfen, die er selbst noch nicht durch den letztjährigen Einkommen- oder Lohnsteuerbescheid belegen konnte, sind von der WK Auskünfte beim Finanzamt eingeholt worden. Eine derartige Praxis widerspricht § 2 Nr.11 des Hamburgischen Gesetzes über den Abbau der Fehlsubventionierung im Wohnungswesen, wonach alle Behörden, insbesondere die Finanzbehörden, sowie Arbeitgeber nur dann Auskunft erteilen dürfen, wenn Zweifel an der Richtigkeit der Angaben des Wohnungsinhabers bestehen. In den von uns geprüften Akten sind aller-

dings weder Zweifel entsprechend dokumentiert noch sind entgegen von Zusicherungen der WK die Wohnungsinhaber mehrfach aufgefordert worden, angezweifelte Tatbestände erst einmal selbst zu klären. Letzteres gilt im übrigen auch für Auskünfte beim Arbeitgeber, die von der WK eingeholt wurden, um Einkünfte des laufenden Jahres zu belegen, die nicht durch Einkommen- und Lohnsteuerbescheid ausgewiesen werden können.

— Angesichts der Sensibilität der beim Fehlbelegungsabgabe-Verfahren gespeicherten Daten sind hinsichtlich der Sicherheit der eingesetzten EDV-Systeme Maßnahmen zu ergreifen, die den Anforderungen des Sozial- oder Steuergeheimnisses entsprechen. Dies ist der WK jedoch nur unzureichend gelungen: Aufgrund von Programmfehlern war es während der Prüfung möglich, über eine nicht durch Paßwort geschützte Kennung auf Betriebssystemebene zu gelangen und durch Veränderung bestimmter Systemdateien umfangreiche Zugriffsrechte zu bekommen. Da diese Kennung zur Schulung von Mitarbeitern genutzt wurde, war es Unbefugten über einen längeren Zeitraum möglich, auf Daten des Fehlbelegungsabgabe-Verfahrens zuzugreifen, ohne dabei vom Systemverwalter entdeckt zu werden. Dieses Beispiel zeigt wieder einmal auf, daß der Einsatz von UNIX-Systemen aufgrund datensicherungstechnischer Schwachstellen erhebliche Anforderungen an die Systemadministration stellt. Andernfalls sind Datenschutzrisiken die Folge (vgl. 9. TB, 3.3).

Aufgrund der dargestellten Mängel habe ich die Verfahrensweise der WK förmlich beanstandet und die WK aufgefordert, sämtliche nicht erforderlichen Kopien zu vernichten bzw. nicht erforderliche Daten entsprechend unkenntlich zu machen, wie dies bereits zu Beginn des Verfahrens zugesagt worden war. Für die Bearbeitung des Verfahrens wäre es sogar ausreichend, nur noch die Vorlage der erforderlichen Dokumente in der Akte festzuhalten. Auskünfte beim Finanzamt oder beim Arbeitgeber sollten nur bei berechtigten Zweifeln eingeholt werden, die darüber hinaus in der Akte zu dokumentieren sind. Hinsichtlich der Sicherheit des EDV-Verfahrens haben wir vorgeschlagen, zum einen die Systemadministration zu verbessern, um die vorhandenen UNIX-Schwachstellen soweit wie möglich zu reduzieren, zum anderen sollte der Einsatz zusätzlicher Sicherheitskomponenten angestrebt werden.

12.2 Hamburger Mietenspiegel

Aufgrund steigender Mieten wird der Hamburger Mietenspiegel in der Regel alle zwei Jahre – so auch 1991 – zur Erhebung der ortsüblichen Vergleichsmiete von nicht preisgebundenen Wohnungen durchgeführt. Er dient Mietern und Vermietern gleichermaßen als Grundlage zur Bestimmung der Miethöhe und wird auch von Gerichten im Streitfall zur Urteilsfindung herangezogen. Die Durchführung des Mietenspiegels 1991 wurde, wie in den vergangenen Jahren auch, dem Hamburger Institut GEWOS von der Baubehörde übertragen; die Befragung der Mieter wurde wiederum vom Institut für angewandte Sozialwissenschaft (infas) als Unterauftragnehmer durchgeführt.

Datenschutzrechtlich ist der Mietenspiegel relevant, da Daten personenbezogen erhoben und bis zum Abschluß der Erhebung personenbezogen gespeichert werden. Hinsichtlich der Erhebung des Mietenspiegels galt es daher vor allem, den Umfang des Mieter-Fragebogens, das Erstellen einer geeigneten Stichprobe, die Form der freiwilligen Einwilligung sowie den hiervon betroffenen Personenkreis datenschutzrechtlich zu bewerten:

— Der Mieter-Fragebogen enthielt im Entwurf u.a. die Frage nach dem Bezug von Wohngeld. Da diese Frage dem Sozialdatenschutz unterliegt, wurde die GEWOS aufgefordert, für die Verarbeitung von Sozialdaten besondere technische und organisatorische Sicherungsmaßnahmen vorzusehen. Daraufhin wurde im Fragebogen auf das Merkmal „Bezug von Wohngeld" verzichtet.

— Um eine möglichst kostengünstige Erhebung mit einer geringen Stichprobenmenge durchführen zu können, wurde von der GEWOS eine sogenannte disproportionale Stichprobe angestrebt, die jedes relevante Tabellenfeld des Mietenspiegels mit ausreichenden Einträgen zu füllen in der Lage ist. Ein gleichverteiltes Erhebungsverfahren, das zufällig irgendwelche Wohnungen auswählt, hätte es dagegen nur bei einer sehr hohen Stichprobe ermöglicht, Miethöhen von beispielsweise sehr alten Häusern in bestimmten Wohngegenden zu liefern. Um im Rahmen der angestrebten disproportionalen Erhebung ausreichend mietenspiegelrelevante Wohnungen bestimmter Gebäudealtersklassen in die Stichprobe einbeziehen zu können, war die Hinzuziehung des Liegenschaftskatasters, der Stromzählerdatei der Hamburgischen Electricitätswerke (HEW) und der Datei der Gebäude- und Wohnungszählung 1968 des Statistischen Landesamtes geplant.

  Datenschutzrechtliche Bedenken bestanden insbesondere bei der Übermittlung gebäudebezogener Daten aus der Gebäude- und Wohnungszählung von 1968: Die von der GEWOS angeforderten Daten hätten längst nicht mehr vom Statistischen Landesamt mit genauen Adreßangaben gespeichert werden dürfen. Unabhängig davon würde ihre Übermittlung dem im Volkszählungsurteil formulierten Trennungsgebot von Statistik und Verwaltung widersprechen. Schließlich wäre die Reidentifizierung übermittelter Einzelangaben nach dem Bundesstatistikgesetz verboten.

  Aufgrund der vorgetragenen Bedenken war zum einen das Statistische Landesamt selbst nicht mehr zu einer Übermittlung der erbetenen Einzelangaben bereit. Zum anderen entschloß sich die GEWOS, ihr Verfahren zur Ermittlung des Gebäudealters dahingehend zu ändern, daß lediglich aggregierte bzw. altershomogene Blockseitendaten aus der Gebäude- und Wohnungszählung von 1987 Verwendung finden. Eine genaue Ermittlung des Gebäudealters sollte nunmehr durch Befragung des Mieters erfolgen.

— Aufgrund einschlägiger gesetzlicher Regelungen zum Mietenspiegel führt die GEWOS gemäß § 5 Abs. 1 HmbDSG den Mietenspiegel seit Erstellen

des ersten Mietenspiegels auf freiwilliger Basis durch. Uneinigkeit besteht allerdings bereits seit dieser Zeit darüber, ob die freiwillige Einwilligung der Schriftform bedarf (vgl. 4. TB, 4.15.2) oder ob es ausreicht, auf die Freiwilligkeit lediglich im Merkblatt hinzuweisen. Die GEWOS führt als besondere Umstände, die eine Schriftform unangemessen erscheinen lassen, die Tatsache an, daß durch eine schriftliche Einwilligung eine zusätzliche Hemmschwelle bei Mietern mit geringerer Bildung und beruflicher Qualifikation zu erwarten und somit die Repräsentativität der Erhebung nicht mehr gewährleistet sei. Darüber hinaus würde eine geringere Rücklaufquote von vornherein eine erweiterte Stichprobe erfordern und zu zusätzlichen Kosten führen.

Die Befürchtungen der GEWOS werden allerdings von uns bezweifelt. Um die Auswirkungen einer schriftlichen Einwilligung auf die Rücklaufquote konkreter beurteilen zu können, wurde für den diesjährigen Mietenspiegel vereinbart, für eine geringe Anzahl von Mietern eine schriftliche Einwilligung vorzusehen und die hierbei zu beobachtende Rücklaufquote mit der Quote der restlichen Fragebögen zu vergleichen, bei denen lediglich ein Hinweis auf einem Merkblatt vorgesehen ist. Die Ergebnisse sollen bei der Gestaltung des Mietenspiegels 1993 berücksichtigt werden.

— Der Mietenspiegel wird in Abstimmung mit Mieter- und Vermieterverbänden gleichermaßen bei Mietern als auch bei Vermietern erhoben. Die Vermieter-Befragung sollte jedoch nicht nur einer effektiveren Erhebung dienen, insbesondere bei Großvermietern. Sie war auch als Ersatzbefragung für den Fall geplant, daß ein Mieter zu keiner Auskunft über seine Wohnverhältnisse bereit ist.

Eine derartige Praxis wurde von uns datenschutzrechtlich entschieden abgelehnt. Das Recht auf informationelle Selbstbestimmung kann nicht einfach dadurch umgangen werden, daß die Daten ersatzweise an anderer Stelle erhoben werden. Vielmehr wird davon ausgegangen, daß die Durchführung des Mietenspiegels die Einwilligung sämtlicher Betroffenen, sowohl des Vermieters als auch des Mieters, erfordert. Dabei ist weiterhin zu berücksichtigen, daß bei der Erhebung von Mietdaten (Größe, Ausstattung, Wohnlage, Mietpreis) die Interessen des Mieters durchaus schutzwürdiger sind als die des Vermieters. Während die Erhebung lediglich Auskunft über Mieteinkünfte des Vermieters gibt, lassen Mietdaten sehr weitreichende Rückschlüsse auf die sozialen Verhältnisse des Mieters zu. Somit müßte im Konfliktfall das Geheimhaltungsinteresse des Mieters gegenüber dem Auskunftsinteresse des Vermieters überwiegen.

Da sowohl Vermieter als auch Mieter ein berechtigtes Interesse daran haben können, daß der Inhalt des Mietvertrages nicht bekannt wird, wäre es eigentlich notwendig gewesen, vor der Erhebung sowohl beim Mieter als auch beim Vermieter eine schriftliche Einwilligung einzuholen. Die Baubehörde war allerdings nicht bereit, dieser Argumentation zu folgen. Es wurde lediglich zugesichert, auf eine Befragung der Vermieter jener Wohnungen zu verzichten, deren Mieter bereits die Befragung aus datenschutzrechtlichen Gründen abgelehnt haben.

Im Hinblick auf künftige Verfahren schlagen wir vor, zumindest die Mieter als Hauptbetroffene von Wohnungen, die für den Mietenspiegel ausgesucht worden sind, über die geplante Erhebung zu informieren und ihnen ein generelles Widerspruchsrecht einzuräumen. Wird hiervon Gebrauch gemacht, muß auf eine Ersatzbefragung beim Vermieter verzichtet und eine andere Wohnung aus einer erweiterten Stichprobe ausgesucht werden.

12.3 Prüfung der Stadtreinigung

Im letzten Quartal des Jahres 1990 ist von uns auch die Datenverarbeitung der Stadtreinigung geprüft worden. Die Prüfung bezog sich zum einen auf Großrechnerverfahren, die im Rahmen von Auftragsdatenverarbeitung über die Datenverarbeitungszentrale (DVZ) abgewickelt werden, zum anderen auf dezentrale PC-Anwendungen. Die Prüfung der Großrechnerverfahren steht in einem engeren Zusammenhang mit der DVZ-Prüfung (3.6), da die Stadtreinigung einer der Hauptanwender im Siemens-Bereich ist: Während die DVZ-Prüfung eine verbesserte Datensicherheit hinsichtlich Systemprogrammierung, Systemadministration und Operating bezweckte, galt es bei der Prüfung der Stadtreinigung vor allem, die DVZ-Verfahren aus Anwendersicht hinsichtlich Anwendungsentwicklung und dezentraler Benutzerverwaltung zu bewerten.

Bei der Prüfung sind uns insgesamt folgende Sicherheitsdefizite aufgefallen:

— Für sämtliche Dateien – sowohl auf Großrechnern als auch auf Personalcomputern – fehlte eine Dateibeschreibung, die den Anforderungen des zum Prüftermin geltenden HmbDSG gerecht wurde. Wir haben vorgeschlagen, das fehlende Dateiverzeichnis auf der Grundlage des neuen HmbDSG zu vervollständigen.

— Es existiert keine verbindliche Regelung oder Dienstvereinbarung über die Verarbeitung personenbezogener Daten und die dabei zu treffenden Sicherungsmaßnahmen. Die Stadtreinigung wurde von uns aufgefordert, in nächster Zeit entsprechende Regelungen zu erlassen.

— Die in der Stadtreinigung eingesetzten Großrechner-Verfahren auf Siemens-Rechnern (Rechnungswesen, Fuhrparkinformationssystem, Lohnbuchhaltung) werden im Teilnehmerbetrieb administriert. Aufgrund der hierdurch sich ergebenden unzureichenden Zugriffskontrolle haben wir gefordert, die Administration der Verfahren auf die DVZ zu übertragen. Die Verfahren selbst sollten über den Transaktionsmonitor UTM abgewickelt werden, wobei wiederum die UTM-Administration im Teilhaberbetrieb innerhalb der UTM-Anwendung erfolgt. Darüber hinaus sollte das Produkt MPVS eingesetzt werden, das die Möglichkeit bietet, Zugriffsberechtigungen auf einzelne Speicherbereiche zu beschränken (vgl. 3.6).

— Obwohl die auf den PC der Stadtreinigung gespeicherten Daten als wenig sensibel einzuschätzen sind und somit keinen hohen Sicherungsstandard erfordern, haben wir vorgeschlagen, zumindest die Maßnahmen gemäß dem Schutzstufenkonzept (9. TB., 3.2) für Daten der Stufe A umzusetzen. Dadurch sind zusätzliche Maßnahmen insbesondere bei denjenigen PC notwendig, die von mehreren Anwendern benutzt werden.

Leider hat sich jedoch die Umsetzung der von uns geforderten Maßnahmen als sehr schwierig und langwierig erwiesen. Dies liegt zum einen daran, daß die Stadtreinigung nach eigenem Bekunden aufgrund von Personalengpässen nicht in der Lage ist, die datensicherungstechnischen Anforderungen in nächster Zeit umzusetzen. Zum anderen entsteht der Eindruck, daß die Stadtreinigung selbst wenig an einer Verbesserung des Datenschutzes interessiert ist. So haben wir angesichts der Personalengpässe zwar hinreichend dafür Verständnis, daß von der Stadtreinigung keine kurzfristigen Terminzusagen hinsichtlich der Beseitigung der Sicherungsdefizite abgegeben werden können. Unverständlich ist jedoch, daß die Stadtreinigung noch nicht einmal – trotz mehrfacher Aufforderung – bereit ist, einen Zeitplan über die durchzuführenden Maßnahmen zu erstellen. Dies zeigt wieder einmal, welcher Stellenwert dem Datenschutz in einigen Bereichen beigemessen wird, sobald Personalengpässe zu verzeichnen sind.

13. Meldewesen

13.1 Automation des Meldewesens und Novellierung des Hamburgischen Meldegesetzes (HmbMG)

Im 9. TB (4.9.2 und 4.9.3) war über die Pläne zur Novellierung des HmbMG anläßlich der Übertragung der Zuständigkeiten vom Einwohnerzentralamt auf die Bezirke und im Zusammenhang mit der vollständigen Automation des Melderegisters berichtet worden. Inzwischen haben die damaligen Absichten konkrete Form angenommen:

13.1.1 Wegfall der örtlichen Zuständigkeit örtlicher Meldedienststellen?

Der vorliegende Entwurf bedeutet, daß die bisherige örtlich begrenzte Zuständigkeit der Meldedienststellen in den Bezirks- und Ortsämtern weitgehend entfallen soll. Mit der Verlagerung von Aufgaben des Einwohnerzentralamts auf die Bezirke ist dies für Auskünfte aus dem Melderegister nach § 34 Abs. 1 HmbMG (sog. „einfache" Melderegisterauskünfte) und Übermittlung von Meldedaten an andere Stellen bereits vollzogen.

Darüber hinaus sollen die örtlichen Meldedienststellen in Zukunft auch An- und Abmeldungen von Bürgern verarbeiten können, die nicht im örtlichen Zuständigkeitsbereich wohnen, und den Meldedatenbestand ohne Rücksicht auf örtliche Zuständigkeitsgrenzen fortschreiben, berichtigen und löschen. Voraussetzung hierfür ist, daß die vom bestehenden Gesetz vorgegebenen Beschränkungen bei Zugriffsrechten auf den Gesamtbestand aller Meldedaten weitgehend entfallen. Dem liegt die Überlegung zugrunde, daß ein einheitlicher automatisierter Meldedatenbestand die Möglichkeit schafft, meldebehördliche Aufgaben den Bürgern näher zu bringen: sie sollen in der Meldedienststelle ihrer Wahl alle sie betreffenden Meldeangelegenheiten erledigen können. Nicht die Bürger sollen den Daten „hinterherlaufen", sondern die Daten den Bürgern.

Der Gesetzentwurf verfolgt also nicht mehr wie sein Vorgänger von 1986 die Absicht, der Bürgerschaft einen Vorschlag zur Beantwortung der Frage zu unterbreiten, welcher rechtliche Rahmen für technischen Wandel gelten soll. Vielmehr soll er lediglich die technisch bereits vollzogenen Tatsachen bestätigen und angebliche weitere rechtliche Barrieren ausräumen. Bei dieser Ausgangsposition haben wir im Rahmen der Behördenabstimmung eine Diskussion des Entwurfs unter folgenden Kriterien gefordert: Welche Risiken für den Schutz von Meldedaten entstehen dadurch, daß rechtliche und technische Zugriffsschranken entfallen sollen? Stehen diesen Risiken nachvollziehbar belegte Vorteile im Sinne von Bürgernähe, flexiblerer und ökonomischerer Aufgabenwahrnehmung gegenüber und überwiegen die Vorteile? Welche Verbesserungen zum Schutz der Meldedaten sind im Rahmen dieser Risikoabwägung und darüber hinaus möglich?

Im 9. TB (4.9.3) war bereits die Frage aufgeworfen worden, ob die Aufhebung der Zuständigkeitsgrenzen nicht die Wirkung haben würde, daß sich die zu erledigenden Aufgaben bei einigen wenigen zentral gelegenen Meldedienststellen konzentrieren würden, wodurch der angestrebte Effekt wieder aufgehoben würde. Erste Stellungnahmen aus den Bezirken und vom Senatsamt für den Verwaltungsdienst zum vorliegenden Entwurf bestätigen diese Vermutungen. Von Bürgernähe kann nicht die Rede sein, wenn die Bürger ihre Meldeangelegenheiten zwar in einer nahegelegenen Dienststelle erledigen können, dort aber unverhältnismäßige Wartezeiten in Kauf nehmen müssen. Eine Auseinandersetzung mit dieser Frage läßt der Entwurf vermissen.

Die Verlagerung der Auskunftsbearbeitung vom Einwohnerzentralamt auf die Meldedienststellen ist von einer sorgfältigen Arbeitsuntersuchung der Bezirksämter vorbereitet worden. Hieran hat sich die Umsetzung der Verlagerung orientiert und sie war letztlich auch Grundlage für die Zustimmung des Hamburgischen Datenschutzbeauftragten zu diesem Verfahren. Dagegen fehlt für die viel weitergehende Neuaufteilung der Zuständigkeiten, die der Entwurf vorsieht, ein vergleichbarer empirischer Ansatz.

Nur eine Analyse, ob und wenn ja welche Veränderungen im Publikumsverkehr durch die Aufhebung der Zuständigkeitsgrenzen zu erwarten sind und welche personellen und organisatorischen Maßnahmen etwaigen Veränderungen Rechnung tragen sollen, würde eine tragbare Grundlage für die Annahme einer größeren Bürgernähe darstellen. Ohne derartiges nachvollziehbares Material stehen aus datenschutzrechtlicher Sicht die Nachteile der Aufhebung der örtlichen Zuständigkeit im Vordergrund. Wir haben in unserer Stellung-

nahme deutlich gemacht, daß wir unter diesen Voraussetzungen diesem Ansatz im vorgelegten Gesetzentwurf nicht zustimmen können.

Auch in den Stellungnahmen des Senatsamtes für den Verwaltungsdienst und der Justizbehörde überwiegen die kritischen Stimmen zur Konzeption des Entwurfs. Es ist daher als offen zu betrachten, ob er tatsächlich unverändert verabschiedet werden wird.

13.1.2 Online-Zugriffe anderer Stellen auf das Melderegister

Auf der Grundlage des geltenden Meldegesetzes verfügt nur die Polizei über den Direktzugriff auf den Meldedatenbestand im automatisierten Verfahren (9. TB, 4.12.4). Inzwischen ist auch für die Kraftfahrzeug-Zulassungsstellen eine entsprechende Rechtsverordnung in Kraft getreten. Für das automatisierte Verfahren zur Sozialhilfe-Bearbeitung (PROSA) ist ebenfalls ein Online-Zugriff auf das Melderegister vorgesehen, bevor hierfür eine vereinheitlichende Rechtsgrundlage im Melderecht geschaffen worden ist.

Beide Verordnungen sind auf das Hamburgische Datenschutzgesetz gestützt worden. Dies ist zwar bei rechtssystematischer Betrachtung nicht unproblematisch, weil die Regelungen eigentlich auf die – noch nicht vorhandene – Verordnungsermächtigung im vorgesehenen neuen Meldegesetz zu stützen wären. Wir haben jedoch keine Einwendungen erhoben, da Übereinstimmung über die materielle Ausgestaltung der Verordnungen erzielt werden konnte. In beiden Fällen beschränkt sich der Zugriff auf die zwingend zur Aufgabenerfüllung erforderlichen Daten. Im Falle von PROSA wird technisch sichergestellt werden, daß nur Daten von Personen, die in diesem Verfahren gespeichert sind, abgerufen werden. Bei der Kfz-Zulassung besteht allerdings in Einzelfällen Bedarf für Melderegisterabfragen, bevor der Halter erfaßt wird. In diesen Fällen wird der Zugriff protokolliert.

Im Entwurf für das neue Meldegesetz ist eine allgemeine Regelung für Online-Zugriffe anderer Behörden vorgesehen, die sich an den im Hamburgischen Datenschutzgesetz geregelten Kriterien orientiert. Zu begrüßen ist insbesondere, daß Anfragen nur unter Verwendung der Grunddaten (Name, Geburtsdatum) zulässig sein sollen; die Suche nach allen Personen, die unter einer Adresse gemeldet sind, wird ausschließlich für die Polizei zugelassen. Allerdings halten wir es für notwendig, daß der zum Abruf zur Verfügung stehende Datensatz auf die in § 31 Abs. 1 HmbMG genannten Angaben begrenzt wird; der Zugriff auf die in § 31 Abs. 2 HmbMG genannten weiteren Daten im Online-Verfahren setzt eine besondere Prüfung durch die Meldebehörden voraus, die technisch nicht zu gewährleisten ist.

Unakzeptabel ist die Absicht, die gesetzliche Regelung des für den Online-Zugriff der Polizei zulässigen Datenumfangs in § 31 Abs. 4 HmbMG zu streichen und sie der Rechtsverordnung zu überlassen. Im Unterschied zu anderen Verwaltungsaufgaben zeichnet sich das Interesse der Polizei an Meldedaten

dadurch aus, daß es nicht entsprechend einer klar umrissenen Aufgabenstruktur rechtlich vorgegeben ist. Es ist vielmehr abhängig vom jeweiligen Fall der Gefahrenabwehr oder Strafverfolgung. Die Abwägung des polizeilichen Interesses mit dem Interesse der Mehrheit der Bürger, von polizeilichen Datenerhebungen unbehelligt zu bleiben, ist Sache des Gesetzgebers. Wegen des hohen Rangs der polizeilichen Aufgaben läßt der Gesetzgeber den Zugriff auf Daten sämtlicher Einwohner und sogar besonders problematische Suchstrategien zu. Als Korrektiv für diese praktisch schrankenlosen Zugriffsmöglichkeiten muß zugleich der zur Verfügung stehende Datenumfang definiert werden. Andernfalls wäre die der Legislative obliegende Abwägung unverhältnismäßig, da sie der Exekutive die wesentliche Entscheidung überlassen würde.

Aus diesen Gründen haben wir auch das Vorgehen der Behörde für Inneres kritisiert, zwar einerseits anzukündigen, daß der Datenumfang auf Wunsch der Polizei erweitert werden soll, andererseits jedoch nicht klarzustellen, welche Daten dies sein sollen, und zugleich die Streichung des Datenkatalogs in § 31 Abs. 4 HmbMG vorzuschlagen. Wenn die Zusatzwünsche der Polizei sachlich begründet sind, spricht nichts dagegen, sie bereits im Rahmen der Behördenabstimmung zu benennen und auch dem Gesetzgeber zu verdeutlichen. Damit können alle Beteiligten den Umfang des polizeilichen Zugriffs auf das Melderegister in voller Kenntnis beurteilen und entscheiden.

13.1.3 Melderegisterauskünfte an Parteien

Grundsätzlich haben die politischen Parteien und Wählergemeinschaften vor Wahlen das Recht, Auskünfte aus dem Melderegister über bestimmte Altersgruppen und Bewohner einzelner Ortsteile zu erhalten. Bei zahlreichen Wahlberechtigten, die die Weitergabe ihrer Anschriften zum Zwecke der Wahlwerbung nicht wünschen, stößt dies immer wieder auf Ablehnung. Es ist daher zu begrüßen, daß der neue Entwurf für das HmbMG erstmalig für Hamburg ein Widerspruchsrecht der Betroffenen enthält, wie es andere Landesmeldegesetze bereits kennen. Die Neuregelung sieht ferner vor, daß die den Parteien zur Verfügung gestellten Unterlagen über wahlberechtigte Einwohner spätestens eine Woche nach der Wahl zu vernichten sind und jede Benutzung für andere als Wahlzwecke untersagt ist. Die Bußgeldandrohung wird dabei auf 50.000 DM erhöht.

Zur Sicherung dieser gesetzlich vorgeschriebenen Zweckbindung haben wir eine Ergänzung der Vorschrift vorgeschlagen: Herkömmlicherweise werden die Auskünfte an die Parteien in Form von Adressenaufklebern erteilt. Bei deren Verwendung verbleibt regelmäßig kein Datenmaterial bei den Versendern. Es ist zwar nicht ausgeschlossen und faktisch nicht auszuschließen, daß die Aufkleber kopiert werden, um sie anderweitig zweckfremd zu verwenden. Dieses Risiko steigt jedoch beträchtlich an, wenn die Auskünfte in Form von automatisierten Dateien (Disketten, Magnetbändern) erteilt werden, wofür die technischen Voraussetzungen bereits existieren. Bei diesen Speichermedien ist das

Kopieren, Zusammenfassen und Auswerten von Adressenmaterial ohne großen Aufwand in nicht mehr kontrollierbarem Umfang möglich.

Wenn – wie bereits bei der letzten Europawahl geschehen – einzelne Parteien Adressenmaterial aus der gesamten Bundesrepublik sammeln und zentral auswerten, wird ihnen mit maschinell lesbaren Datenträgern ein Instrumentarium in die Hand gegeben, das nach der herkömmlichen Form der Erteilung von Auskünften an Parteien kaum vorstellbar war. Da im Zusammenhang mit Wahlen der Gleichbehandlungsgrundsatz höchste Bedeutung hat, würde auch dann, wenn einzelne Parteien die maschinell lesbaren Datenträger nur im Rahmen des Zulässigen unter hohen Sicherheitsstandards verarbeiten, ein Präzendenzfall für andere Wahlbewerber geschaffen, bei denen keine Vermutung für Gesetzestreue besteht. Diesem Risiko kann nur begegnet werden, indem im Meldegesetz die Erteilung der Auskünfte in Form automatisierter Dateien ausdrücklich verboten wird.

13.2 Novellierung des Melderechtsrahmengesetzes

Der Entwurf zur Änderung des Melderechtsrahmengesetzes (MRRG), der bereits im 7. TB (4.10.4) und 9. TB (4.9.1) dargestellt worden war, ist in der letzten Legislaturperiode zwar noch abschließend in den Bundestagsausschüssen beraten worden, jedoch nicht mehr zur Verabschiedung gelangt.

Der Innenausschuß des Deutschen Bundestages hatte eine wesentliche Verbesserung beschlossen. Die rahmenrechtliche Vorgabe für die Länder zur Regelung der Hotelmeldepflicht sollte entfallen. Damit hätte es den Ländern freigestanden, der datenschutzrechtlichen Forderung nach Streichung der Hotelmeldepflicht nachzukommen. Inzwischen liegt ein neuer Referentenentwurf für das MRRG vor, der wiederum an der Hotelmeldepflicht festhält.

Wir haben die in Hamburg beteiligten Behörden aufgefordert, sich im Gesetzgebungsverfahren in dieser Frage zumindest für die Rückkehr zur Beschlußlage des Bundestags-Innenauschusses einzusetzen. Darüber hinaus sieht der Entwurf jedoch noch eine Verschärfung der Hotelmeldepflicht vor, denn ausländische Hotelgäste sollen verpflichtet werden, sich bei der Anmeldung im Hotel auszuweisen. Zur Begründung wird auf Art. 45 des Schengener Zusatzübereinkommens (siehe 9. TB, 4.12.3) verwiesen.

Diese Verschärfung der Hotelmeldepflicht für eine bestimmte Gruppe von Hotelgästen, die auch im Entwurf für das HmbMG vorgesehen ist, halten wir für höchst problematisch. Wenn „nur" Ausländer dazu verpflichtet werden sollen, sich bei Anmeldung im Hotel auszuweisen, bleibt unbeantwortet, wie das Hotelpersonal die Staatsangehörigkeit – ohne die Vorlage von Ausweispapieren – feststellen soll. Deutsche Hotelgäste sind nicht verpflichtet, ihren Ausweis vorzuzeigen, also gibt es in Zweifelsfällen keine Möglichkeit, zuverlässig zwischen beiden Gruppen abzugrenzen. Somit wird von den Leitern von Beherbergungsstätten – sogar mit Bußgeldandrohung – etwas Unmögliches verlangt. Bereits dies ist wegen Verstoß gegen das Verhältnismäßigkeitsgebot verfassungswidrig.

Wenn man darüber hinaus berücksichtigt, daß die Gründe, die gegen die allgemeine Hotelmeldepflicht sprechen (9. TB, 4.9.1), ebenso gegen eine Hotelmeldepflicht für Ausländer sprechen, liegt die Unverhältnismäßigkeit dieser Vorschrift auf der Hand. Denn ebensowenig wie für deutsche gilt für ausländische Hotelgäste die Vermutung, sie stellten eine generelle Gefahr für die öffentliche Sicherheit dar oder seien Straftäter. Wir haben daher die Streichung dieser Vorschrift im Entwurf zum MRRG ebenso wie zum HmbMG gefordert.

14. Ausländerbehörde

14.1 Automation der Ausländerverwaltung

Die Pläne, im Bereich der Ausländerbehörde die technischen Voraussetzungen für eine umfassende automationsunterstützte Abwicklung aller Arbeitsabläufe zu schaffen (9. TB, 4.10.3), haben im Berichtszeitraum konkrete Formen angenommen. Bereits Ende 1990 ist eine Projektorganisation „Automation des Ausländer- und Asylwesens" eingesetzt worden, an deren Lenkungsgruppe auch wir beteiligt sind.

Ziel des Projekts ist es, alle Vorgänge, die nach ausländerrechtlichen Vorschriften durch die Ausländerbehörde bearbeitet werden müssen, im Dialogbetrieb abzuwickeln. Hierzu gehören die Erteilung und Verlängerung von Aufenthaltsgenehmigungen ebenso wie die Beendigung des Aufenthalts bis hin zur Abschiebung, aber auch zahlreiche Fragen des Asylverfahrensrechts, für die die Ausländerbehörden unmittelbar zuständig sind.

Durch das neue Automationsverfahren soll neben der Verbesserung des Services für die Betroffenen und der Arbeitsbedingungen für die Mitarbeiter und Mitarbeiterinnen erreicht werden, daß Aufgaben des Ausländerwesens wirtschaftlicher wahrgenommen werden. Insbesondere erhofft man sich, durch schnellere Verwaltungsabläufe aufgrund des Dialogverfahrens den Aufenthalt zahlreicher Ausländer verkürzen zu können, um somit Kosten einzusparen. Für die Ausländerbehörde im Landeseinwohneramt von Berlin wird ein solches Dialogverfahren demnächst eingeführt. Die Behörde für Inneres hat sich entschlossen, das Berliner Verfahren in den Grundzügen zu übernehmen und gemeinsam mit dem Unternehmen, das die Anwendung für Berlin erstellt und auch mit der technischen Konzeption für das Ausländerzentralregister Erfahrungen im Bereich der Ausländerverwaltung gesammelt hat, in Hamburg zu realisieren.

Das Projekt hat im Schnellverfahren zunächst analysiert, welche Abweichungen vom Berliner Verfahren in Hamburg erforderlich sind, und die Anforderungen in einem Auftrag an das Unternehmen zur Erstellung der Konzeption zusammengefaßt. Es ist nach den Plänen des Projekts ferner vorgesehen, das Verfahren nicht über einen Großrechner bei der Datenverarbeitungszentrale

abzuwickeln, sondern über Abteilungsrechner im Bereich der Ausländerbehörden. Die endgültige Entscheidung hierüber soll nach Auswertungen der ersten Berliner Erfahrungen getroffen werden. Dabei soll die Option offengehalten werden, auch im Falle einer Dezentralisierung ausländerbehördlicher Aufgaben – beispielsweise auf die Bezirke – die zu erstellende Infrastruktur übernehmen zu können. Wir haben unsere Zustimmung zur Nutzung von Abteilungsrechnern davon abhängig gemacht, daß die im 9. TB (3.3) beschriebenen Schwachstellen beim Betrieb von UNIX-Rechnern durch ein umfassendes Datensicherungskonzept aufgefangen werden.

Unmittelbare Schnittstellen zu anderen automatisierten Dateien der hamburgischen Verwaltung zur Datenübermittlung im Online-Verfahren sind nicht vorgesehen. Änderungen im Melderegister über ausländische Bewohner werden der Ausländerbehörde im Stapelverfahren täglich übermittelt und zur Aktualisierung der Ausländerdatei verwendet. Die technischen Möglichkeiten zum Zugriff auf Daten des Ausländerzentralregisters sollen jedoch beträchtlich erweitert werden. Die Ausgestaltung hängt ab vom Gesetz über das Ausländerzentralregister.

Aus datenschutzrechtlicher Sicht stehen neben den Aspekten der Datensicherheit folgende Problembereiche im Vordergrund:

14.1.1 Rechtsgrundlage für die Automation der Ausländerverwaltung

Während für andere Automationsvorhaben der Verwaltung teilweise sehr detaillierte rechtliche Vorgaben bestehen (z.B. Straßenverkehrsgesetz und Fahrzeugregisterverordnung für das Kfz-Zulassungswesen), enthält das neue Ausländergesetz zwar auch Vorschriften zur Datenverarbeitung. Diese betreffen jedoch in erster Linie Übermittlungen an die Ausländerbehörden (siehe unten 14.2). Lediglich § 80 AuslG sieht nach näherer Ausgestaltung durch eine Rechtsverordnung vor, daß jede Ausländerbehörde eine Datei über Ausländer führt, die sich in ihrem Zuständigkeitsbereich aufhalten. Danach dürfen nur die Personalien einschließlich der Staatsangehörigkeit und der Anschrift des Ausländers, Angaben zum Paß, über ausländerrechtliche Maßnahmen und über die Erfassung im Ausländerzentralregister, sowie über frühere Anschriften, die zuständige Ausländerbehörde und die Abgabe von Akten an eine andere Ausländerbehörde erfaßt werden (§ 80 Abs. 1 Satz 3 AuslG).

Die Rechtsverordnung aufgrund § 80 AuslG – die sog. Ausländerdateienverordnung – ist inzwischen erlassen worden. Sie sieht die Einrichtung einer sog. Ausländerdatei A über aktuell im Bezirk der Ausländerbehörde lebende Ausländer und einer Ausländerdatei B über Verstorbene und Fortgezogene vor. Bereits in unserer Stellungnahme zum Entwurf der Rechtsverordnung vor Beginn des Automationsprojekts hatten wir darauf hingewiesen, daß die Regelung den Erfordernissen einer zeitgemäßen Automationsunterstützung für die Ausländerverwaltung nicht entsprechen werde, und eine gründliche Überprüfung unter diesem Gesichtspunkt vorgeschlagen. Dem ist die Behörde für Inneres nicht gefolgt, sie hat vielmehr der Verordnung unverändert zugestimmt.

Bei den Beratungen im Projekt stellte sich dann jedoch schnell heraus, daß der in der Ausländerdateienverordnung festgelegte Datensatz nicht ausreicht. Beispielsweise sind Angaben der Betroffenen über ihre Volkszugehörigkeit oder Religion wesentlich für ausländer- oder asylrechtliche Entscheidungen. Es reicht eben nicht aus zu wissen, ob jemand die türkische oder irakische Staatsangehörigkeit hat, wenn er Kurde ist oder einer verfolgten Religionsgemeinschaft angehört. Diese Daten sind in der Ausländerdateienverordnung nicht vorgesehen.

Damit stand das Projekt vor der Frage, ob die Regelungen in § 80 AuslG und der Verordnung abschließend sind und die Speicherung von zusätzlichen Daten nicht zulassen. Die Behörde für Inneres vertritt nunmehr die Auffassung, daß die ausländerrechtlichen Vorschriften nur die Verpflichtung der Länder zur Führung der genannten Dateien mit dem in der Verordnung geregelten Mindestdatensatz bezweckten. Die Befugnis zur Speicherung weiterer Daten in einem automatisierten Verfahren ergebe sich dagegen aus der Verwaltungshoheit der Länder und richte sich nach den Bestimmungen des Landesdatenschutzgesetzes. Dieser Auffassung haben sich auch die Ausländerrechtsreferenten des Bundes und der Länder angeschlossen.

Wir haben dagegen eingewandt, daß bei dieser Auslegung die Vorschriften von § 80 AuslG und der Ausländerdateienverordnung, wonach nur die festgelegten Daten gespeichert werden dürfen, sinnlos werden. Es ist auch nicht schlüssig, zwischen der bundesrechtlichen Verpflichtung zur Einrichtung eines Mindestdatensatzes und der angeblichen landesrechtlichen Befugnis zu dessen Erweiterung zu differenzieren, da die Verordnung selbst zwischen einem Grunddatensatz und einem erweiterten Datensatz unterscheidet. Die Regelung über den erweiterten Datensatz nimmt sogar direkt Bezug auf besondere technische Voraussetzungen, d.h. auf ein automatisiertes Verfahren, um ausländerrechtliche Entscheidungen zu treffen.

Ein Rückgriff auf die Verwaltungshoheit der Länder als Befugnis zur Speicherung personenbezogener Daten stellt in Wahrheit einen Rückfall in Argumentationsmuster aus der Zeit vor dem Volkszählungsurteil dar. Der Verwaltungshoheit des Landes nach Maßgabe des Hamburgischen Datenschutzgesetzes unterliegen sicherlich die Fragen, ob und in welcher Form ein Textverarbeitungsprogramm integriert wird, welche Wiedervorlagefristen automatisiert festgelegt werden und welche Rechnerkonfigurationen zu beschaffen sind. Die Festlegung des Datensatzes der Datenbank als Kernstück des geplanten Verfahrens hat sich jedoch der Bund in Wahrnehmung seiner Rechtssetzungskompetenz auf dem Gebiet des Ausländerrechts vorbehalten, indem er im Gesetz und in der Verordnung eine ausdrücklich abschließende Regelung getroffen hat. Hierüber kann sich die Landesexekutive nicht einfach hinwegsetzen, auch wenn sie erkennt, daß die Bundesregelung völlig unzureichend ist. Der gebotene Weg ist dann eine Initiative zur Änderung des Bundesrechts. Andernfalls setzt sich Hamburg dem Vorwurf aus, zwar einerseits Neuregelungen des Aus-

länderrechts zu Lasten der Betroffenen durchzusetzen, andererseits selbst die ausländerrechtlichen Vorschriften zu mißachten.

Auf die Frage, welchen Zweck die Regelung in der Ausländerdateienverordnung überhaupt noch habe, fällt bei der Auslegung der Behörde für Inneres eine Antwort schwer. Sie ist der Auffassung, daß die Verordnung lediglich festlege, welche Daten unter Nutzung der Datei und welche unter Hinzuziehung weiterer Unterlagen an andere Stellen übermittelt werden dürfen. Dagegen ist festzustellen, daß es keinen Unterschied macht, ob Daten übermittelt werden, nachdem man einen Blick in eine Datei oder in eine Akte geworfen hat, solange es sich um dieselben Angaben handelt und nicht zusätzliche – etwa in der Datei nicht gespeicherte – Informationen, die sich nur aus der Akte ergeben, heranzuziehen sind. Letztlich bleiben als wirksamer Regelungsgegenstand der Verordnung nur noch die dort festgelegten Fristen übrig, die Anhaltspunkte für die Fristen des automatisierten Verfahrens geben können. Die bei weitem überwiegende Zahl der einschlägigen Regelungen in § 80 AuslG und der Ausländerdateienverordnung laufen dagegen leer.

14.1.2 Weitere Probleme

Die Kontroverse über die Frage der Rechtsgrundlage wäre dann eher theoretischer Natur, wenn im Hamburger Verfahren nur solche zusätzlichen, in der Verordnung nicht erwähnten Daten erfaßt werden sollten, deren Erforderlichkeit auf der Hand liegt und die letztlich im Interesse der Betroffenen gespeichert werden (wie z.B. Angaben über Volks- und Religionszugehörigkeit, wenn sie auf eigenen Angaben der Betroffenen beruhen). Dies ist jedoch nicht der Fall.

Vielmehr soll das Verfahren beispielsweise auch ermöglichen, Listen über Personen auszudrucken, die nach dem Asylverfahrensgesetz von Hamburg in andere Bundesländer zu verteilen sind, sich aber noch hier aufhalten. Man wird zwar angesichts der Regelungen über das Verteilungsverfahren die Erforderlichkeit derartiger Listen bejahen können. Dennoch wird hier deutlich, daß nicht nur eine Datenbank zur Unterstützung der internen Verwaltungsabläufe in der Ausländerverwaltung geschaffen werden soll, sondern auch ein Instrument zur Überwachung und Verhängung von Zwangsmaßnahmen gegen die Betroffenen.

Noch kritischer wäre die Registrierung von Verstößen gegen ausländerrechtliche Vorschriften, die im Einzelfall als Ordnungswidrigkeiten geahndet werden können. Dies wird erwogen, weil die Einzelverstöße im Wiederholungsfall Straftatbestände sind und die Speicherung somit die Möglichkeit bietet, vom Ordnungswidrigkeitenverfahren zur Einleitung von Strafverfahren überzugehen. Damit hätte das Verfahren die Funktion einer Datei zur vorbeugenden Bekämpfung von Straftaten.

Es ist inzwischen allgemein anerkannt, daß Datenspeicherungen zu diesem Zweck einer ausdrücklichen gesetzlichen Grundlage bedürfen. Im Gesetz über

die Datenverarbeitung der Polizei werden derartige Speicherungen jedoch an die Voraussetzung geknüpft, daß ein strafrechtliches Ermittlungsverfahren eingeleitet worden ist. Die Einleitung von Ordnungswidrigkeitenverfahren reicht in keinem Fall aus. Auch im Bereich der Verkehrsordnungswidrigkeiten besteht Übereinstimmung darüber, daß Speicherungen über sog. Mehrfachtäter außerhalb des Verkehrszentralregisters unzulässig sind (siehe 9. TB, 4.11.4). Somit wird deutlich, daß Erweiterungen des Datensatzes im geplanten Hamburger Verfahren gegenüber den bundesrechtlichen Vorgaben teilweise massive Eingriffe bedeuten würden, die in keinem Fall auf die Verwaltungshoheit des Landes gestützt werden können. Wir haben daher den Erweiterungen insgesamt und insbesondere der Speicherung von abgeschlossenen Ordnungwswidrigkeitenverfahren widersprochen.

14.2 Datenübermittlungen an die Ausländerbehörde nach dem neuen Ausländergesetz

Welche enormen datenschutzrechtlichen Probleme sich aus der Regelung von § 76 des neuen Ausländergesetzes ergeben, der alle öffentlichen Stellen zur Mitteilung von Ausweisungsgründen an die Ausländerbehörde verpflichet, war bereits im 9. TB (4.10.1) dargestellt worden. Inzwischen haben sich die beteiligten Fachbehörden mit unserer Beteiligung auf Hinweise zur Anwendung dieser Vorschrift verständigt, die den Versuch unternehmen, ansatzweise eine dem Verhältnismäßigkeitsgrundsatz entsprechende Einschränkung der uferlosen Mitteilungspflichten zu gewährleisten.

Danach sollen nur solche Umstände übermittelt werden, die die öffentliche Stelle im Rahmen der Erfüllung ihrer Amtsgeschäfte erfahren hat. Daten, die Bedienstete außerhalb ihrer dienstlichen Zuständigkeit erfahren, sind dagegen nicht mitzuteilen. Ferner sind jeweils nur die Stellen mitteilungspflichtig, bei denen die mitzuteilenden Daten institutionell anfallen, weil die öffentliche Stelle insoweit fachlich zuständig ist. So ist z.B. nur das Sozialamt verpflichtet, den Bezug von Sozialhilfe zu melden, nicht jedoch das Finanzamt, das hiervon erfährt. Einer Unterrichtung über den Sozialhilfebezug bedarf es gar nicht, wenn die Sozialhilfeleistungen nur als Vorschuß für einen anderen Leistungsträger (z.B. die Bundesanstalt für Arbeit) erbracht werden. 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 von Hilfen 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 ist. Dies gilt auch für minderjährige Ausländer, wenn ihre Eltern über den verfestigten Aufenthaltsstatus verfügen.

Mit der verwaltungsinternen Regelung für Hamburg ist jedoch nur ein Teil der durch § 76 Abs. 2 AuslG umfaßten Informationsflüsse zwischen öffentlichen Stellen und der Ausländerbehörde angesprochen. Im Rahmen der bundeseinheitlichen Verwaltungsvorschrift, die vom Bundesminister des Innern mit Zustimmung des Bundesrates erlassen wird, soll die Anwendung der Datenverarbeitungsvorschriften insgesamt geregelt werden. Der Bundesinnenminister hat im Frühjahr einen ersten Entwurf für diese Verwaltungsvorschrift vorgelegt. Bereits der Umfang dieses Regelungsvorschlags, der ausdrücklich keinen Anspruch auf Vollständigkeit erhebt, macht die Problematik der Vorschriften zur Datenverarbeitung nach dem Ausländergesetz deutlich : allein die Hinweise zu den §§ 76 und 77 umfassen 44 Seiten! Zusammen mit dem Bundesbeauftragten für den Datenschutz und anderen Landesbeauftragten haben wir Vorschläge zur Verbesserung erarbeitet und die beteiligten Fachbehörden aufgefordert, diese bei den weiteren Beratungen zu berücksichtigen. Sie betreffen vor allem die folgenden Punkte:

Die Verwaltungsvorschrift sollte bereichsspezifisch nach den für Übermittlungen an die Ausländerbehörde relevanten öffentlichen Stellen gegliedert werden, mit dem Ziel, die in Betracht kommenden Stellen abschließend zu benennen. Nur so können die derzeitigen Rechtsunsicherheiten, welche Stelle welche Sachverhalte zu übermitteln hat, abgebaut werden.

Der Auffassung des Bundesinnenministers, wonach nicht zu prüfen sei, ob die Übermittlungen im Einzelfall verhältnismäßig sind, haben wir widersprochen. Der Verhältnismäßigkeitsgrundsatz folgt unmittelbar aus den Grundrechten und gilt demnach für die gesamte öffentliche Verwaltung. Durch Verwaltungsvorschriften können öffentliche Stellen nicht von der Pflicht, sich grundrechtskonform zu verhalten, freigeschrieben werden.

Die bisherigen Bemühungen in Hamburg, vorläufige Anwendungshinweise für die Praxis herauszugeben, sollten diesem Gesichtspunkt Rechnung tragen. Die Regelungen der Verwaltungsvorschrift sollten daher in keinem Fall hinter den für Hamburg vereinbarten Anwendungshinweisen, die sowohl für die Belange der Ausländerbehörde als auch für die übermittelnden Stellen akzeptabel gewesen sind, zurückbleiben. Es müssen Einschränkungen der Übermittlungen insbesondere beim Sozialhilfebezug sowohl hinsichtlich des Status von Betroffenen als auch hinsichtlich Art und Umfang der Leistungen erfolgen.

Es ist auch daran festzuhalten, daß Übermittlungen auf der Grundlage von § 76 Abs. 2 AuslG immer nur dann erfolgen können, wenn tatsächlich ein konkreter, auf den Einzelfall bezogener Ausweisungsgrund vorliegt. Dies bedeutet, daß über Personen, die besonderen Ausweisungsschutz nach § 48 AuslG, den Fürsorgeabkommen oder Minderjährigenschutzabkommen genießen, nur solche Sachverhalte mitgeteilt werden dürfen, die auch nach diesen speziellen Vorschriften die Ausweisung ermöglichen. Dies sind schwerwiegende Gründe der öffentlichen Sicherheit und Ordnung, z. B. die serienmäßige Begehung nicht unerheblicher vorsätzlicher Straftaten, keinesfalls der bloße legale Bezug

von Leistungen der Sozial- oder Jugendhilfe. Es bleibt auch kein Raum für Verwaltungsvorschriften, nach denen in diesen Fällen eine Übermittlung nur unterbleiben kann und nicht zu unterbleiben hat. Das Bundesinnenministerium und auch die Behörde für Inneres vertreten jedoch die Auffassung, daß die Ausländerbehörde auch in den Fällen mit besonderem Ausweisungsschutz etwaige Ausweisungsgründe kennen müsse. Diese könnten zwar nicht zu aufenthaltsbeendenden Maßnahmen führen, seien jedoch bei anderen ausländerrechtlichen Entscheidungen zu berücksichtigen.

Dies würde nach unserer Auffassung auf eine Datenspeicherung auf Vorrat hinauslaufen, bei der weder der Zweck der Übermittlung noch der der Speicherung von vornherein feststeht. Wenn im Ausländergesetz die Pflicht zur Übermittlung beim Vorliegen von Ausweisungsgründen festgelegt wird, ist dies wegen der Weite der Ausweisungstatbestände schon für sich allein bedenklich. Eine Erweiterung auf Sachverhalte, die irgendeine ausländerrechtliche Relevanz haben könnten, findet dagegen weder im Gesetz eine Stütze noch ist sie verhältnismäßig.

In Einzelfällen sind die Regelungsabsichten des Bundes allerdings restriktiver als die der Behörde für Inneres. Obwohl § 76 Abs. 4 AuslG nur Mitteilungen über Ordnungswidrigkeiten, die mit einem Bußgeld von bis zu 1000 DM geahndet werden können, zuläßt, hielt sie Übermittlungen für erforderlich, wenn im Zeitraum von drei Jahren mehrfach gegen eine mit geringerem Bußgeld bewehrte Vorschrift verstoßen wurde. Somit wäre zweimaliges Falschparken in den letzten 3 Jahren mitzuteilen gewesen, mit dem Ziel, den Ausländer auszuweisen. Wir haben mehrfach zunächst erfolglos auf die absurden Konsequenzen, die eine solche Praxis gehabt hätte, hingewiesen. Erst auf die entsprechende Argumentation des Bundesministers des Innern hat die Behörde für Inneres hierauf verzichtet.

Wegen der überaus komplexen Materie konnte die weitere Beratung dieses Teils der Verwaltungsvorschrift noch nicht abgeschlossen werden.

15. Verkehrswesen

15.1 Prüfung der polizeilichen Praxis bei Direktabrufen aus dem Zentralen Fahrzeugregister

Alle in den 11 „alten" Ländern der Bundesrepublik zugelassenen Kraftfahrzeuge werden sowohl bei den örtlich zuständigen Zulassungsstellen als auch zentral beim Kraftfahrt-Bundesamt in Flensburg registriert. Seit 1. Januar 1991 kommen die mit neuen amtlichen Kennzeichen versehenen Fahrzeuge aus den „neuen" Bundesländern hinzu. Das Zentrale Fahrzeugregister ist damit eine der größten Sammlungen von personenbezogenen Daten in der öffentlichen Verwaltung. Es dient der Identifizierung von Fahrzeugen sowie von Personen in ihrer Eigenschaft als Halter von Fahrzeugen.

Durch das Straßenverkehrsgesetz (StVG) haben die Polizeibehörden des Bundes und der Länder die Möglichkeit eingeräumt bekommen, nach näherer Ausgestaltung durch die Fahrzeugregister-Verordnung (FRVO) auf den Datenbestand des Zentralen Fahrzeugregisters und außerdem auf Daten über Versagung und Entziehung von Fahrerlaubnissen, die im Verkehrszentralregister gespeichert werden, direkt (im Online-Verfahren) zuzugreifen. Dieses Zentrale Verkehrs-Informationssystem (ZEVIS) ist somit in erster Linie ein polizeiliches Datenverarbeitungssystem.

Nachdem die Rechtsgrundlagen für den Online-Abruf der Polizei geschaffen worden sind und die Einführungsphase von ZEVIS abgeschlossen ist, erschien es uns geboten, einen Überblick über die Praxis des Abrufs von Kfz-Halterdaten im automatisierten Verfahren zu gewinnen. Im Vordergrund der Prüfung standen daher Querschnittsfragen der ZEVIS-Nutzung.

15.1.1 Entwicklung und derzeitiger Stand der Nutzung des Zentralen Verkehrs-Informationssystems (ZEVIS) durch die Polizei

Die Hamburger Polizei benutzt zum ZEVIS-Abruf die vorhandenen POLAS-Terminals. Dem Kraftfahrt-Bundesamt sind 166 abrufberechtigte Terminals gemeldet worden, von denen 143 über die Möglichkeit zum Abruf verfügen. Monatlich werden im Durchschnitt mehr als 30 000 Abrufe von diesen Terminals getätigt (1990 376 335 insgesamt), wovon die weit überwiegende Anzahl Anfragen mit Kennzeichen nach Kfz-Haltern (sog. K-Anfragen) betrifft. Der Anteil der sog. P-Anfragen, mit denen festgestellt werden kann, welche Fahrzeuge auf eine Person zugelassen sind, liegt im einstelligen Prozentbereich. Im Vergleich mit anderen Ländern liegt Hamburg im Mittelfeld der Nutzer (höher als Schleswig-Holstein oder Hessen). Wie in den anderen Ländern ist auch in Hamburg der Gesamtumfang der ZEVIS-Nutzung kontinuierlich angestiegen (Vergleichszahlen 1988 : 239 071 und 1989: 325 477).

15.1.2 Einzelne Problemfelder

§ 36 Abs. 5 Nr. 1 Straßenverkehrsgesetz erlaubt die Einrichtung von Anlagen zum ZEVIS-Abruf im automatisierten Verfahren nur inswoweit, als die automatisierte Übermittlung unter Berücksichtigung der schutzwürdigen Belange des Betroffenen und der Aufgabe des Empfängers angemessen ist. Dies bedeutet, daß Polizeidienststellen, die über abrufberechtigte Terminals verfügen, auch Aufgaben erfüllen müssen, die die Abfrage von Kfz-Halterdaten in Sekundenschnelle für die Kontrolle der Fahrzeuge und der Fahrzeugpapiere, für die Verfolgung von Verkehrsordnungswidrigkeiten und Straftaten sowie für Vollzug und Vollstreckung von Strafen oder zur Gefahrenabwehr erfordern.

Nicht zulässig wäre dagegen die Annahme, daß alle polizeilichen Zuständigkeiten die Installation von abruffähigen Terminals und die Nutzung von ZEVIS-Anfragen erfordern. Im Rahmen der Prüfung war es nicht möglich, alle relevanten Dienststellen daraufhin zu untersuchen, ob diese Voraussetzungen erfüllt

werden. Die Erforderlichkeit wird jedoch ständig durch die Landespolizeiverwaltung überprüft. So wurde z.B. bei der Verlegung eines POLAS-Terminals die ZEVIS-Berechtigung entzogen.

Gewisse Anhaltspunkte für die Relevanz von ZEVIS-Anfragen für die Dienststellen ergeben sich aus dem tatsächlichen Abfrageverhalten. Drei Dienststellen tätigten in den ersten 10 Monaten 1990 weniger als 30 Abfragen. Einer Dienststelle ist die ZEVIS-Berechtigung inzwischen entzogen worden, da diese nicht im obigen Sinne erforderlich war. Die beiden anderen (Lagedienst und Dienststelle der Grenzpolizei am Hafenrand) greifen lagebedingt auf ZEVIS zu, was akzeptiert werden kann.

§ 36 Abs. 5 Nr. 2 StVG schreibt Maßnahmen zur Sicherung gegen Mißbrauch vor. Hierzu gehört insbesondere die Vergabe von Kennungen, deren Eingabe erforderlich ist, um das POLAS-Terminal für den ZEVIS-Abruf zu aktivieren (§ 13 Abs. 1 Satz 1 FRVO). Wenn mehr als zweimal die 10-stellige Kennung der abrufberechtigten Dienststelle unrichtig eingegeben wird, führt dies zur Sperrung der Möglichkeit zum ZEVIS-Abruf durch dieses Endgerät (§ 13 Abs. 2 FRVO).

Das Kraftfahrt-Bundesamt (KBA) sendet in diesen Fällen eine Mitteilung an die Landespolizeiverwaltung (1990: über 270). Diese Fehlerbriefe enthalten z.T. Angaben über den konkreten Anlaß, der zur Sperrung führte. Nach den bisherigen Erfahrungen handelt es sich fast durchgehend um Fälle, in denen die Kennung versehentlich falsch eingegeben wurde (Zahlendreher etc.).

Die Kennungen von Terminals, die zwar gegenüber dem KBA als ZEVIS-berechtigt gemeldet worden sind, an denen jedoch nach polizeiinterner Auffassung keine Abrufe aus ZEVIS vorgenommen werden müssen, werden bei der Landespolizeiverwaltung unter Verschluß gehalten. Dieses Verfahren ist sachgerecht, da sie den erforderlichen Überblick hat und laufende Überprüfungen vornehmen kann, während das KBA hierzu schon rein faktisch nicht in der Lage wäre.

15.1.3 Abruf von Echtdaten zu Schulungszwecken

Zunächst wurde uns mitgeteilt, daß über die Terminals der Landespolizeischule auch Echtdaten zu reinen Schulungszwecken abgerufen wurden. Dies wurde damit begründet, daß die Schulungsdatei beim KBA noch nicht alle relevanten Abfragemöglichkeiten erfasse. Im Laufe der Prüfung hat die Landespolizeischule diese Praxis überdacht und mitgeteilt, daß nunmehr in der Regel nur mit den Testdaten der hierfür vorgesehenen Schulungsdatei gearbeitet wird. Die prompte Bereitschaft der Polizei zur Korrektur in dieser Frage haben wir begrüßt. Durch eine Überprüfung anhand von Abfragen im Mai 1991 haben wir uns davon überzeugt, daß keine Echtdaten mehr zu Schulungszwecken abgerufen werden.

15.1.4 Prüfung von Einzelabfragen anhand der Protokolle

Wir haben zu den im November und Dezember 1990 zu protokollierenden Anfragen einzelner Terminals bei einer Polizeidirektion, einem Polizeirevier und einer Dienststelle des Landeskriminalamts teilweise die Vorgänge herangezogen bzw. die Anfragen mit den zuständigen Bediensteten erörtert. Wegen des Querschnittscharakters der gesamten Prüfung sollte die Überprüfung einzelner Abfragen einen Eindruck über den alltäglichen Umgang mit dem Instrument ZEVIS vermitteln.

Fälle von Mißbrauch der ZEVIS-Anfragen (außerdienstliche Zwecke) wurden bei der Prüfung nicht festgestellt. In zwei Fällen beim Polizeirevier war der Anlaß der Abfragen nach den Erläuterungen des Revierführers nicht zu rekonstruieren; nach den protokollierten Daten spricht jedoch viel dafür, daß es sich um Schulungs- bzw. Testanfragen mit Daten von Kollegen handelte, so daß aus hiesiger Sicht eine weitere Aufklärung nicht erforderlich schien.

Vom oben definierten „Mißbrauch" wären Fälle zu unterscheiden, in denen Anfragen zwar zu polizeilichen Zwecken erfolgen, die Voraussetzungen von § 36 Abs. 2 und 3 StVG jedoch nicht vorliegen oder die aus anderen Gründen (z.B. mangelnde Erforderlichkeit oder Verhältnismäßigkeit) unzulässig sind. Abgesehen vom oben erörterten Echtdatenabruf zu Schulungszwecken haben wir Fälle des offenkundig unzulässigen Abrufs nicht festgestellt. Hierzu ist allerdings zu bemerken, daß die Zulässigkeitsvoraussetzungen des StVG so weit sind, daß – außer der Schulung – kaum polizeiliche Zwecke denkbar sind, die nicht abgedeckt wären.

In einigen Fällen lagen die Abfragen jedoch an der Grenze der Erforderlichkeit und Verhältnismäßigkeit. So wurden z.B. zur Fahndung nach einem entflohenen Strafgefangenen auch Anfragen nach den Fahrzeugen von Personen vorgenommen, die ihn in der Vergangenheit in der Haft besucht hatten, wozu auch ein Minderjähriger gehörte. Nach unserem Eindruck ist in derartigen Fällen die Gewinnung von weiteren Erkenntnissen durch die Anfrage, welche Fahrzeuge auf die (minderjährige) Kontaktperson zugelassen sind, zwar nicht restlos ausgeschlossen, jedoch eher theoretischer Natur.

Unabhängig von derartigen Einzelfällen kommen Bedenken gegen die Verhältnismäßigkeit der ZEVIS-Anfragen insbesondere bei Kontaktpersonen dann auf, wenn man sich die mögliche weitere Verwendung der Kfz-Halterdaten vergegenwärtigt. Nach geltendem Recht ist eine Ausschreibung von Kontaktpersonen und deren Fahrzeugen zur Fahndung nach mit Haftbefehl gesuchten oder flüchtigen Personen nicht vorgesehen. Die Entwürfe zur Novellierung der Strafprozeßordnung beschränken die Ausschreibung von Kontaktpersonen bzw. deren Kfz-Kennzeichen zur Fahndung entweder auf die Fälle von Straftaten erheblicher Bedeutung (§ 163e StPO im Entwurf des Gesetzes zur Bekämpfung der organisierten Kriminalität); der Entwurf für ein Strafverfahrensänderungsgesetz bezieht dagegen Kontaktpersonen nicht in die Fahndungsbefugnisse nach § 163e StPO ein, sondern setzt voraus, daß das Fahrzeug regelmäßig vom Beschuldigten (bzw. Flüchtigen) benutzt wird.

Wenn jedoch nach geltendem und zukünftigem Recht die Verwendungsmöglichkeit von Kfz-Halterdaten auf bestimmte Konstellationen eingegrenzt ist, muß dies Konsequenzen für die Frage der Erforderlichkeit von ZEVIS-Anfragen haben. Wir haben daher gefordert, daß vermehrt darauf geachtet wird, ob die abgerufenen Daten auch zulässigerweise für weitere Maßnahmen genutzt werden können, da die ZEVIS-Auskunft selbst in der Mehrzahl der Fälle keine unmittelbar weiterführenden Erkenntnisse vermittelt, sondern allenfalls Ansatzpunkte für ein weiteres gezieltes Vorgehen liefern kann. Für ZEVIS wie für andere Online-Verfahren auch gilt, daß Routineanfragen ohne vorhergehende Überlegung, was mit den erwarteten Daten angefangen werden soll und darf, den möglichen Nutzen des Systems überschätzen und wegen mangelnder Erforderlichkeit unverhältnismäßig sein können.

15.2 Modellversuch Anwohnerparken

Anläßlich der Zustimmung zur Änderung des HVV-Tarifs von 1990 hat die Bürgerschaft ein Sofortprogramm über Maßnahmen zur Verbesserung des Leistungs- und Service-Angebots beim öffentlichen Personennahverkehr beschlossen. Darin war auch die „Einführung von lizensierten Stellplätzen im Straßenraum in citynahen Verdichtungsgebieten unter Berücksichtigung der Interessen von Bewohnern und Betrieben" vorgesehen. Daraufhin ist im Mai 1991 in einem Teil der Neustadt ein Modellversuch zum sog. Anwohnerparken initiiert worden.

Danach gilt in dem Versuchsgebiet ein grundsätzliches Parkverbot, von dem nur für Anwohner wie deren Besucher Ausnahmen erteilt werden. Die Anwohner müssen beim zuständigen Bezirksamt einen maximal 2 Jahre und 3 Monate gültigen Anwohnerparkausweis beantragen, ihre Besucher können beim örtlichen Polizeirevier einen Ausweis erhalten, der sie zum Parken während des Besuchs berechtigt.

Nach der Einführung dieser Regelung ist es insbesondere über die datenschutzrechtlichen Fragen dieses Verfahrens zu öffentlichen Diskussionen gekommen. Wir haben erst durch die Presseberichterstattung davon erfahren, daß und wie dieser Modellversuch durchgeführt werden soll. Obwohl die datenschutzrechtliche Problematik auf der Hand lag, hat niemand daran gedacht, auch uns in die Planung mit einzubeziehen.

Zunächst war vorgesehen, daß die Besucher die Durchschrift eines ausführlichen Antragsformulars mit Angaben über Besucher, Besuchte und Zeitraum des Besuchs an der Windschutzscheibe ihrer Fahrzeuge deutlich sichtbar anbringen sollten. Man hat jedoch schnell erkannt, daß den Betroffenen damit zugemutet wurde, allen interessierten Passanten und Nachbarn zu offenbaren, wer wann wen wie lange besucht.

Auf Initiative des Polizeireviers wurde dann ein anonymer Besucherausweis ausgegeben, der nur noch den Gültigkeitszeitraum und das Kfz-Kennzeichen enthielt. Die Daten über Besucher, Besuchte und den Zeitraum wurden jedoch nach wie vor im Polizeirevier auf der Durchschrift des Ausweises erfaßt und solange aufbewahrt, wie der Ausweis gültig war.

Diese Erfassung und Speicherung von Daten über Besucher und Besuchte in einem überschaubaren Stadtteil haben wir kritisiert, da die Sammlung von Ausweisdurchschriften hochsensible Daten enthielt, die außerhalb von Haftanstalten nirgends sonst erhoben und gespeichert werden.

Inzwischen ist das Verfahren weiter vereinfacht worden. Es wird auch im Polizeirevier nur noch die Gültigkeitsdauer und das Kennzeichen festgehalten, jedoch nicht mehr, wer besucht wird. Wir haben uns mehrfach unangemeldet davon überzeugt, daß die Durchschriften der Ausweise unmittelbar nach Ablauf der Gültigkeit vernichtet werden. Damit ist letztlich eine aus unserer Sicht befriedigende Lösung erreicht worden.

Ursprünglich hatten wir auch Zweifel an der Erforderlichkeit der Aufbewahrung der Anträge für Anwohnerparkausweise beim Bezirksamt geäußert, diese jedoch im Lauf der weiteren Diskussion zurückgestellt. Die Möglichkeit, die Unterlagen zu Kontrollen oder zum Nachweis des Mißbrauchs zu benutzen, ist zwar eher theoretischer Natur. Im Rahmen eines Modellversuchs erscheint die Aufbewahrung zu diesen Zwecken jedoch zunächst vertretbar. Die Auswertung des Modellversuchs wird sich auch auf die Fragen beziehen, ob der Aufwand beim Antragsverfahren und der Umfang der Datenspeicherung aus diesem Anlaß erforderlich sind.

16. Polizei

16.1 Projekt zur computerunterstützten Vorgangsbearbeitung bei der Polizei (COMVOR)

Im 9. TB (4.12.9) waren die Pläne zur Entwicklung eines umfassenden Verfahrens zur „Computerunterstützten Vorgangsbearbeitung (COMVOR)" bei der Polizei dargestellt worden. Im Berichtszeitraum ist die Diskussion hierüber intensiv fortgesetzt worden. Es wird bereits jetzt deutlich, daß in den nächsten Jahren die wesentlichen datenschutzrechtlichen Fragen im Bereich der Polizei im Rahmen dieses Projektes entschieden werden. COMVOR wird daher den Schwerpunkt unserer Aufmerksamkeit bei der Datenverarbeitung der Polizei bilden.

Auch außerhalb Hamburgs findet eine intensive Diskussion um die automatisierte Vorgangsverwaltung und -bearbeitung im Bereich der Polizei statt. In einzelnen Ländern (z.B. Saarland) stehen umfassende Vorgangsverwaltungs- und -bearbeitungssysteme vor der Realisation. Es läßt sich bereits heute feststellen, daß diese Systeme eine neue Stufe bei der polizeilichen Datenverarbeitung

darstellen werden. Daher erscheint es zunächst sinnvoll, sich Klarheit darüber zu verschaffen, was sich hinter den Begriffen verbirgt und wie das neue Gesetz über die Datenverarbeitung der Polizei hierzu Stellung nimmt.

16.1.1 Vorgangsverwaltung und Vorgangsbearbeitung

Bei der sogenannten Vorgangsverwaltung geht es allein um die Frage, wo ein Schriftstück, eine Akte oder ein Gegenstand, der im Verwaltungsablauf eine bestimmte Bedeutung hat, aufzufinden ist. Dies ist ein Problem, daß sich in allen Bereichen der Verwaltung stellt. Daneben steht die Aufbewahrung zur Dokumentation, um auch nach Abschluß eines Verwaltungsverfahrens noch Nachweise über bestimmte Tatsachen erbringen zu können.

Im neuen Gesetz über die Datenverarbeitung der Polizei heißt es denn auch lapidar, daß die Polizei personenbezogene Daten in Akten und Dateien speichern, verändern und nutzen darf, soweit dies zur Erfüllung ihrer Aufgaben, einschließlich einer zeitlich befristeten Dokumentation, oder der Vorgangsverwaltung erforderlich ist (§ 16 Abs. 1). In der Gesetzesbegründung wird dazu ausgeführt: „Die Speicherung von Daten zur Vorgangsverwaltung und zur Dokumentation ist ein untrennbarer Bestandteil der polizeilichen Aufgabenerfüllung." Die besondere Hervorhebung geschehe nur aus Gründen der Klarheit.

Betrachtet man dagegen die für COMVOR erarbeitete Gliederung des geplanten Datensatzes, ergibt sich ein ganz anderes Bild. Danach ist bisher vorgesehen, im sog. Verfahren zur Vorgangsbearbeitung Daten über Personen in insgesamt 16 verschiedenen Rollen zu speichern, von denen nur die letzte zur eigentlichen Vorgangsverwaltung gehört: Beschuldigter, Person mit Kriminalakte, Verdächtiger, angehaltene Person, beobachtete Person, Kontaktperson, Betroffener im Ordnungswidrigkeitenverfahren, Beteiligter bei Maßnahmen der Gefahrenabwehr, Vermißter, unbekannter Toter, unbekannte hilflose Person, Anzeigeerstatter, Geschädigter, Zeuge, Antragsteller und schließlich die sog. Verwaltungsperson. Das heißt, alle denkbaren Rollen, in denen Bürger der Polizei oder die Polizei Bürgern gegenübertreten können, werden unter dem Begriff Vorgangsbearbeitung zusammengefaßt.

Vorgangsverwaltung und Vorgangsbearbeitung bezeichnen daher grundverschiedene Sachverhalte. Die Vorgangsbearbeitung faßt die gesamte polizeiliche Tätigkeit in allen Facetten unter einem Schlagwort zusammen. Während der Begriff der Vorgangsverwaltung im Gesetz über die Datenverarbeitung der Polizei nur ganz am Rande ohne Anspruch auf eigenständige Bedeutung auftaucht, wird der der Vorgangsbearbeitung nur verständlich, wenn man alle gesetzlichen Grundlagen für polizeiliche Tätigkeit, also das Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung (SOG), das Gesetz über die Datenverarbeitung der Polizei, die Strafprozeßordnung, das Ordnungswidrigkeitengesetz, das Straßenverkehrsgesetz und zahlreiche andere Rechtsvorschriften zusammen betrachtet.

Das geplante Verfahren zur automatisierten Vorgangsbearbeitung sollte nach den ursprünglichen – inzwischen modifizierten – Plänen die gesamte polizeiliche Datenverarbeitung strukturieren. Dabei sollten die genannten Rollen Überschriften für lange Kataloge von personenbezogenen Daten darstellen.

Es war geplant, die Möglichkeit zu schaffen, Personen abhängig von ihrer jeweiligen Rolle nach folgenden Kategorien zu erfassen: rechtmäßige Personalien, zu denen neben der Staatsangehörigkeit auch die Volkszugehörigkeit gehören sollte; Alias-Personalien; Sterbeangaben; Fähigkeiten wie Beruf und spezielle Kenntnisse; äußere Erscheinung mit Gestalt, Größe und besonderen Merkmalen; Sprache einschließlich Mundart und Fremdsprachen; Bekleidung mit Schuhgrößen und mitgeführten Gegenständen; Lichtbilder, Fingerabdrücke und Handschriftenmaterial; Aktennachweise; Hinweise auf sog. Tätertypen und Gruppenzugehörigkeiten (sog. „personenbezogene Hinweise") und schließlich Adressenangaben und Telefonnummern. Im Herbst 1990 enthielt dieser Katalog 75 mögliche Stichworte, im Mai 1991 bereits 101.

Doch damit war das Bild noch nicht vollständig, vielmehr konnten sich unter den einzelnen Stichworten lange Listen von sogenannten Katalogwerten verbergen. So wurde z.B. das Datenelement „Äußere Erscheinung" mit folgenden Bezeichnungen weiter untergliedert: „asiatisch, negroid, nordländisch, orientalisch, südländisch, slawisch, indianid". Die Liste der möglichen körperlichen Merkmale war zu lang, um hier wiedergegeben werden zu können, sie reichte von „Adamsapfel" über „Brille", „hoppsender Gang" und „Linkshänder" bis zur „Warze". Wenn all dies in einem automatisierten Verfahren zentral für die gesamte hamburgische Polizei gespeichert würde, wäre es gelungen, den „gläsernen Menschen" zu schaffen.

16.1.2 Ist COMVOR überhaupt praktikabel?

Beim Durchsehen dieser Listen stellte sich für uns ebenso wie für polizeiliche Praktiker sehr schnell die Frage, ob dies alles überhaupt realisierbar und für die praktische Arbeit der Polizei sinnvoll ist. Eine sehr genaue Beschreibung unbekannter Toter ist sicherlich für die Dienststelle erforderlich, die einen Mord aufklären muß; die Schuhgröße kann bei der Suche nach Einbrechern hilfreich sein, die Fußspuren hinterlassen haben, und die Stimme und Sprache bei der Identifikation eines Erpressers. Doch was sollen derartige Angaben beim Ladendieb oder bei jemandem, der unter Alkoholeinfluß einen Verkehrsunfall verursacht?

Wenn somit die Erforderlichkeit der Erhebung, Speicherung und Nutzung vom Einzelfall abhängt und die Zuordnung von Aufgaben im Bereich der Polizei hochdifferenziert ist, ergibt eine Zusammenstellung aller denkbaren Daten für alle möglichen polizeilichen Aufgaben notwendigerweise ein schiefes Bild. Wir haben daher die Herangehensweise des Projekts kritisiert, das zunächst die Anforderungen aller Polizeidienststellen entgegengenommen hat, um dann einen umfassenden Gesamtdatenbestand zu erarbeiten. Uns wurde zunächst

entgegengehalten, daß die Planung eines Verfahrens zur Bearbeitung von polizeilichen Vorgängen aller Art eine umfassende Informationsstrukturanalyse erfordere; die Differenzierung, wer auf welche Daten zu welchen Zwecken zugreifen soll (die sog. Funktionsstrukturanalyse), könne erst im zweiten Schritt erfolgen.

16.1.3 Speicherung aller polizeilichen Daten in einem zentralen Bestand?

Die Erstellung einer umfassenden Datenstruktur ungeachtet der differenzierten Aufgabenstellungen in der Polizei war jedoch nicht nur Folge der Anwendung bestimmter Methoden der Datenverarbeitungs-Planung (DV-Planung). Sie folgte vielmehr der Maßgabe, einen einheitlich strukturierten Datenbestand für die gesamte Polizei zu schaffen. Eine zwingende Begründung für die Erforderlichkeit dieser zentralen Datenhaltung gibt es nicht. Technisch bestünde auch die Möglichkeit, aus dezentralen Dateien die Informationsflüsse innerhalb der Polizei abzuwickeln.

Den spezifischen Anforderungen der einzelnen Dienststellen wie auch des Datenschutzes könnte dadurch einfacher Rechnung getragen werden. Es bestünde auch nicht im gleichen Maße die Abhängigkeit aller polizeilichen Funktionen von der Leistungsfähigkeit des einheitlichen Systems. Aus datenschutzrechtlicher Sicht bestehen die Risiken darin, daß somit – wenigstens potentiell – alle Daten, über die die Polizei verfügt, gleichermaßen recherchierbar sind, ganz gleich, ob es sich um Angaben über Schwerverbrecher oder Geschädigte, um Anzeigenerstatter oder Anmelder von Demonstrationen handelt. Rechtlich bestehen kaum noch Grenzen. Im Zusammenspiel der Vorschriften von § 16 und § 14 des Gesetzes über die Datenverarbeitung der Polizei ist die Nutzung fast aller Daten zu fast allen Zwecken erlaubt. Lediglich bei Daten, die mit besonderen Erhebungsmethoden beschafft worden sind, gibt es Schranken. Offen ist jedoch, ob bei einer Zusammenführung auch dieser Daten in einem zentralen Bestand technische Maßnahmen möglich sind, die die Einhaltung der rechtlichen Einschränkungen gewährleisten.

16.1.4 Die neue Konzeption

Zweifel an der Realisierbarkeit einer umfassenden Neustrukturierung der polizeilichen Informationsverarbeitung haben zusammen mit unseren Vorbehalten dazu beigetragen, daß das COMVOR-Konzept völlig neu überdacht worden ist. Als Ergebnis ist ein in drei Stufen unterteiltes und – zumindest in der ersten geplanten Realisierungsstufe – wesentlich reduziertes Modell entworfen worden. Die wichtigste Änderung besteht darin, die Systeme COMVOR zur Vorgangsbearbeitung und POLAS/INPOL als polizeiliches Informations- und Auskunftssystem getrennt zu betrachten. Mit dieser Herangehensweise wird eine Reihe von datenschutzrechtlichen Bedenken gegen die bisherigen Planungen für COMVOR entschärft.

Eine Erfassung im Kriminalaktennachweis als Kernstück von POLAS/INPOL setzt den Verdacht auf eine Straftat und Wiederholungsgefahr, für das bundes-

weite INPOL-System auch besondere Schwere und überregionale Bedeutung voraus (siehe hierzu unten 16.3). Eine Zusammenführung dieser Daten mit ganz anders strukturierten Vorgangsverwaltungs- und -bearbeitungsdaten in einem gemeinsamen Bestand von COMVOR hätte die Gefahr hervorgerufen, daß die Voraussetzungen für die Speicherung in POLAS/INPOL verwässert worden wären. Die oben beschriebenen enormen Datenkataloge sind im wesentlichen auf INPOL-Anforderungen zurückzuführen, ferner enthält der INPOL-Datenkatalog höchst problematische personenbezogene Hinweise (z.B. über Freitodgefahr), die in Hamburg auf Ersuchen der Bürgerschaft von 1986 nicht gespeichert werden dürfen (5. TB, 5.6.8). Bei der Schaffung einer Datenstruktur für COMVOR, die diejenige von INPOL voll übernommen hätte, wären diese Hinweise „durch die Hintertür" wieder möglich geworden.

Für weitere Realisierungsschritte, die für den Zeitraum 1994 bis 1995 nach Abschluß der ersten Stufe vorgesehen sind, ist zwar auch nach der neuen Konzeption zunächst eine Schnittstelle zwischen COMVOR und POLAS und schließlich auch die Benutzung der COMVOR-Oberfläche für POLAS/INPOL-Abfragen und auch für Änderungen des POLAS/INPOL-Bestandes geplant. Insbesondere letzteres ist als problematisch anzusehen, zur Zeit jedoch noch nicht aktuell.

Das neue Konzept sieht für die erste Realisierungsstufe – die 1993 abgeschlossen sein soll – vor, die Datenerfassung zunächst im Zusammenhang mit der Aufnahme von Anzeigen über Straftaten in den Polizeirevieren neu zu strukturieren. Dabei soll die bereits bestehende automatisierte Tagebuchverwaltung der Polizeidirektionen als Grundlage dienen (siehe hierzu unten 16.2). Der Datensatz dieses Verfahrens soll zwar erweitert werden, jedoch in der ersten Stufe längst nicht den ursprünglich geplanten, oben beschriebenen Umfang erhalten. Im wesentlichen soll die Rolle der Person im jeweiligen Sachverhalt (z.B. Geschädigter, Zeuge, Verdächtiger, Beschuldigter) mit den Identifizierungsdaten und ggf. Angaben über Aliaspersonalien und zur Erreichbarkeit erfaßt werden. Als Sachverhaltsdaten sind Ort, Art und Zeitpunkt des Ereignisses sowie Angaben zum Tatobjekt vorgesehen. Den Zweck der Vorgangsverwaltung im engeren Sinne sollen Aktenzeichen, Angaben zur Dienststelle und zum Sachbearbeiter, zu dazugehörigen Vorgängen anderer Dienststellen bzw. zur Abgabe an die Staatsanwaltschaft erfüllen.

Ziel dieser ersten Stufe ist es, die derzeit benutzten Formulare und Vordrucke für die verschiedensten Berichte und Meldungen aus Anlaß der Strafverfolgung computerunterstützt auszufüllen und zu versenden. Aus unserer Sicht ist dabei vor allem die Frage von Interesse, welche Verknüpfungen zwischen personenbezogenen Datensätzen, die aus verschiedenen Anlässen gespeichert sind, möglich sein werden, ob Zugriffe auf Daten zu einem bestimmten Sachverhalt von anderen Dienststellen zugelassen werden sollen, und welche Wege für elektronische Übermittlungen eröffnet werden können. Die Diskussion hierüber hat erst begonnen, so daß zur Zeit noch keine abschließende Bewertung möglich ist.

16.2 Automatisierte Tagebuchdateien in den Polizeidirektionen

Seit Anfang 1990 verfügen die Polizeidirektionen über sog. „automatisierte Tagebücher". Dies sind Vorgangsverwaltungs- und -bearbeitungsdateien, die auf Abteilungsrechnern geführt werden. Sie sind nicht direktionsübergreifend vernetzt. Nach der Zweckbeschreibung in der Errichtungsanordnung sollen diese Dateien das Auffinden polizeilicher Vorgänge, die Terminüberwachung und Aussagen über den Verbleib eines Vorgangs – also Vorgangsverwaltung im engeren Sinn – ermöglichen. Außerdem sollen sie zur Darstellung der Kriminalitätslage, zur Feststellung von Zusammenhängen, zum Erkennen von Kriminalitätsbrennpunkten und zur Gewinnung von Erkenntnissen für kriminaltaktisches Vorgehen dienen.

Damit sind Zwecke angesprochen, die über die bloße Vorgangsverwaltung hinausgehen und die materiellen Aufgaben der Polizei insbesondere bei der Strafverfolgung betreffen. Gedacht waren die Vorgangsverwaltungssysteme als Ersatz für die herkömmlichen manuellen Indexkarteien und Tagebücher. Andere polizeiliche technikgestützte Anwendungen wie Textverarbeitung, Abruf aus Dateien und Informationssystemen sind zwar noch nicht integriert, die Einführung der Vorgangsverwaltungsysteme soll jedoch ein erster Schritt in Richtung auf die mit COMVOR geplante umfassende, IuK-unterstützte polizeiliche Sachbearbeitung sein (siehe 16.1).

Neben den Angaben zur Person und zur Rolle als Beschuldigte, Verdächtige, Geschädigte, Anzeigenerstatter und für auswärtige Dienststellen vernommene Zeugen werden das polizeiliche Aktenzeichen und Angaben zur Straftat, zum Eingangs- und Wiedervorlagedatum und zuständigen Sachbearbeiter sowie zur Stelle, an die der Vorgang abgegeben wurde (Staatsanwaltschaft oder auswärtige Polizeidienststelle), erfaßt.

Die Auswertungsmöglichkeiten sind nach bestimmten Funktionen differenziert. Zum einen ermöglichen die Dateien die Überwachung, welche Sachbearbeiter welche Vorgänge wie lange bearbeiten, andererseits können die Sachbearbeiter selbst erkennen, welche Personen zu einem Vorgang gehören oder wieviele Vorgänge einer Person zugeordnet werden können. Darüber hinaus sind sogenannte Globalauswertungen möglich, die anzeigen, wieviele Delikte einer bestimmten Kategorie im Zuständigkeitsbereich der Polizeidirektion oder eines Reviers innerhalb eines bestimmten Zeitraums aufgetreten sind.

16.2.1 Technische Mängel der Dateien

Um uns ein Bild von der Praxis beim Umgang mit diesen Dateien zu verschaffen, haben wir bei einer Polizeidirektion insbesondere die Einhaltung der gesetzlich und in der Errichtungsanordnung geregelten Vorgaben zur Datensicherheit geprüft. Hierbei mußten wir Mängel konstatieren, die deshalb besonders gravierend waren, weil es sich bei der eingesetzten Technik um das Standardprodukt in der hamburgischen Verwaltung handelt und die Schwachstellen ebenso bekannt sind wie die Maßnahmen, um sie zu verhindern.

Vor allem war die nach § 8 Abs. 2 Nrn. 3 und 4 HmbDSG vorgesehene Speicher- und Benutzerkontrolle unzureichend gewährleistet. Die Einrichtung, Löschung und Sperrung von Benutzern waren unzureichend dokumentiert und ließen sich daher nicht lückenlos nachvollziehen. Insbesondere war nicht erkennbar, welche Benutzerkennungen wann von welchem Systemverwalter eingerichtet worden sind.

Besonders kritisch war, daß unter einer Standardkennung mit dem vom Hersteller ausgelieferten und allgemein bekannten Paßwort ein LOGIN in das Standardmenüsystem möglich war. Ein solches – unberechtigtes – LOGIN würde (anders als die rechtmäßigen Systembenutzungen und fehlgeschlagene Versuche, sich als Superuser einzuloggen) nicht protokolliert. Mit den unter der Standardkennung verfügbaren Mitteln war es möglich, die Paßwortdatei und andere Dateien mit vielen sicherheitsrelevanten Informationen zu lesen und dabei insbesondere zu erkennen, welche Benutzer kein Paßwort hatten.

Nicht weniger als 14 Benutzerkennungen waren nicht paßwortgeschützt. Darunter befand sich auch eine Systemverwalterkennung. Dieser Mangel wurde auch nicht dadurch relativiert, daß Benutzer ohne Paßwort automatisch nach dem ersten LOGIN dazu aufgefordert wurden, ein Paßwort einzugeben. Praktisch hätte sich jeder Systembenutzer unter einer nicht paßwortgeschützten Kennung einloggen und nach Vergabe des Paßwortes in die Identität desjenigen schlüpfen können, für den die Kennung eingerichtet wurde. Da das System gerade auch die Kontrolle ermöglichen soll, ob Bedienstete Vorgänge, für die sie zuständig sind, unzulässig lang behalten, war dies eine besonders empfindliche Lücke.

Da eine nicht mit Paßwort geschützte Kennung Systemverwalterrechte hatte, konnten unter dieser Kennung weitere Benutzer eingerichtet werden. Da eine lückenlos nachvollziehbare Dokumentation der Rechtevergabe fehlte und die Kennungen generell zunächst ohne Paßwort eingerichtet wurden, ließ sich auch nicht mit der erforderlichen Sicherheit feststellen, ob tatsächlich alle aktuell mit Paßwort ausgestatteten Kennungen auch von ihren rechtmäßigen Benutzern oder von anderen nicht berechtigten Personen benutzt wurden.

Die Polizei hat diese Mängel bei der betroffenen Dienststelle und auch bei anderen, die ähnliche Defizite aufwiesen, umgehend abgestellt. Die Standardkennung mit dem vom Hersteller vergebenen Paßwort sowie die ungeschützten Benutzerkennungen wurden gelöscht. In Zukunft soll nach jedem Einrichten einer Benutzerkennung nur noch so verfahren werden, daß zwangsweise ein individuelles Paßwort vergeben wird.

16.2.2 Speicherung von Anhaltemeldungen

Neben diesen inzwischen bereinigten technischen Mängeln haben wir eine Änderung der Praxis zur Speicherung sog. Anhaltemeldungen gefordert. Anhaltemeldungen werden dann gefertigt, wenn einem Polizeibeamten eine

Person aufgrund ihres Verhaltens auffällig erscheint, ohne daß jedoch bereits ein Verdacht auf eine Straftat vorliegt (Beispiel: an einem Ort, an dem in der Vergangenheit bereits mit Drogen gehandelt wurde, aber auch bandenmäßige Raubüberfälle auf Passanten verübt wurden, halten sich Jugendliche auf; es gibt jedoch keine konkreten Anhaltspunkte dafür, daß sie im Besitz von Drogen sind, Überfälle begangen haben oder begehen wollen).

Der Polizeibeamte kann nach § 4 Abs. 1 des Gesetzes über die Datenverarbeitung der Polizei die Personalien feststellen. Da er jedoch keine Veranlassung für die Einleitung eines Strafermittlungsverfahrens oder andere polizeiliche Maßnahmen hat, fertigt er lediglich eine sog. Anhaltemeldung. Diese hat den Zweck, aufgrund weiterer Erkenntnisse, die der Polizei bereits vorliegen, festzustellen, ob die angehaltenen Personen einer bekannten Straftat mit unbekannten Tätern als Verdächtige oder Beschuldigte zugeordnet werden können, oder ob die Informationen in eine bestehende Kriminalakte (siehe 16.3) aufgenommen werden können.

Für diese Prüfung ist polizeintern eine Aufbewahrungsdauer von drei Monaten vorgesehen; läßt sich die Anhaltemeldung in dieser Frist keinem anderen Vorgang zuordnen, ist sie zu vernichten. Diese Regelung gilt seit 1983 (2. TB, 3.10.2.2). In den Vorgangsverwaltungsdateien sollten jedoch angehaltene Personen ein Jahr lang gespeichert werden. Auf Grund unserer Forderung wurde die Frist für angehaltene Personen, die keinem anderen Vorgang als Verdächtige oder Beschuldigte zugeordnet werden können, auf drei Monate verkürzt.

16.3 Prüfung der Kriminalaktenhaltung

Im Berichtszeitraum war es uns erstmalig möglich, die Kriminalaktenhaltung beim Landeskriminalamt im Wege einer Querschnittsprüfung systematisch zu untersuchen.

Kriminalakten sind nicht, wie die Bezeichnung nahelegt, die Ermittlungsakten in einem Strafverfahren oder Handakten, die die Kriminalpolizei in konkreten Ermittlungsverfahren führt. Vielmehr wird aus diesen Unterlagen eine kurze Zusammenfassung über den strafrechtlichen Vorwurf gegen eine Person erstellt und von der ermittelnden Dienststelle als Merkblatt an LKA 511, die kriminalaktenführende Dienststelle der Polizei, übersandt. Dort wird die Person mit den Grunddaten und Kurzangaben zum Delikt im Kriminalaktennachweis (KAN) des polizeilichen Auskunfts- und Informationsystems POLAS erfaßt.

POLAS ermöglicht damit die sofortige Kurzauskunft, ob die Polizei in einer Kriminalakte Erkenntnisse zu einer Person hat. POLAS/KAN und die Kriminalaktenhaltung sind das Rückgrat der polizeilichen Datenspeicherung zum Zwecke der Vorsorge für künftige Strafverfolgung. Kriminalakten und entsprechende Nachweise – sei es in Form von Indexkarteien oder automatisierten Dateien – führt die Polizei schon seit langem.

Erst mit Inkrafttreten des Gesetzes über die Datenverarbeitung der Polizei (DVPolG) am 1. August 1991 hat diese Form polizeilicher Datenverarbeitung eine gesetzliche Grundlage erhalten. Nach § 16 Abs. 2 Satz 3 ist eine suchfähige Speicherung von Daten, die die Polizei im Rahmen der Verfolgung von Straftaten gewonnen hat, zum Zwecke der Gefahrenabwehr bei Personen zulässig, gegen die ein strafrechtliches Ermittlungsverfahren eingeleitet worden ist und bei denen wegen der Art, Ausführung oder Schwere der Tat und der Persönlichkeit des Betroffenen die Besorgnis der Begehung weiterer Straftaten besteht.

Diese Formulierung ist den Richtlinien zur Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien) entnommen, die für Detailfragen auch nach wie vor von Bedeutung sind. Sie wurde ursprünglich vom Bundesverwaltungsgericht im Zusammenhang mit der Befugnis zur Anfertigung und Aufbewahrung von Lichtbildern und Fingerabdrücken zu sog. Zwecken des Erkennungsdienstes nach § 81 b 2. Alternative StPO geprägt.

Der Bezug zu erkennungsdienstlichen (ed-) Unterlagen besteht in der Praxis nach wie vor, denn in den Kriminalakten werden ed-Unterlagen aufbewahrt. Bereits anhand des Aktenzeichens ist erkennbar, ob Kriminalakten ed-Unterlagen enthalten: Wenn Lichtbilder und Fingerabdrücke vorliegen, wird eine sogenannte feste Akte angelegt, die durch den Buchstaben „F" am Ende des Aktenzeichens erkennbar ist; wenn (noch) keine ed-Unterlagen vorhanden sind, werden sog. Sammelakten geführt, mit „S" am Ende. In Sammelakten werden in der Regel bis zu fünf Merkblätter über einzelne Ermittlungsverfahren abgelegt, spätestens ab dem sechsten Delikt wird beim nächsten Aufgreifen des Betroffenen die erkennungsdienstliche Behandlung zur vorbeugenden Bekämpfung von Straftaten angeordnet und die Sammelakte in eine feste Akte überführt. Die Absicht, eine feste Akte anzulegen, führt jedoch allein nicht zu einer erkennungsdienstlichen Behandlung.

Die hamburgische Polizei verfügt z.Zt über ca. 156 000 Kriminalakten und entsprechende Eintragungen in POLAS/KAN. Die Hälfte davon enthält erkennungsdienstliche Unterlagen. Bereits diese Zahl macht deutlich, daß es nicht möglich ist, die Kriminalaktenhaltung insgesamt oder auch nur anhand einer prozentualen Auswahl durchzugehen. Wir haben insgesamt 268 Akten und die dazugehörenden POLAS-Auszüge überprüft. Dabei konnten wir in insgesamt 105 Fällen wiederkehrende Probleme feststellen, die teilweise Schlußfolgerungen auf die gesamte Aktenhaltung zuließen.

16.3.1 Struktureller Mangel bei der Fristberechnung

Nach § 16 Abs. 2 Satz 5 DVPolG sind für Kriminalakten Prüfungstermine festzusetzen, die bei Erwachsenen zehn und bei Jugendlichen fünf Jahre nicht überschreiten dürfen. Diese Fristen werden in den KpS-Richtlinien näher konkretisiert. Danach gilt auch bei Erwachsenen in Fällen von geringerer Bedeutung (z.B. Hausfriedensbruch, Beleidigung, Ladendiebstahl durch Kunden etc.)

regelmäßig eine Frist von fünf Jahren. Die Prüfungsfristen sind als Regel-Löschungsfristen ausgestaltet, d.h. es müssen besondere Gründe vorliegen, um eine Aufbewahrung über die Fristen hinaus im Einzelfall zu rechtfertigen.

Positiv hervorzuheben ist, daß wir keinen Fall festgestellt haben, in dem die festgelegten Fristen überschritten waren. Als äußerst problematisch war jedoch die Art und Weise anzusehen, wie die Fristen berechnet wurden. Die Regelungen im Gesetz und in den KpS-Richtlinien sind eindeutig: Danach beginnt in den Fällen, in denen keine Haftzeiten zu berücksichtigen sind, die Frist an dem Tag, an dem das letzte Ereignis eingetreten ist, das zur Speicherung der Daten geführt hat. Dies ist in den meisten Fällen der Tag der Tat, wegen der das strafrechtliche Ermittlungsverfahren eingeleitet worden ist, bei Taten, die sich über einen Zeitraum erstrecken, der letzte Tag dieses Zeitraums. Es kann auch der Tag sein, an dem eine Person, über die bereits eine Kriminalakte vorliegt, unter einschlägigen Umständen angetroffen wird, ohne daß es zur Einleitung eines Ermittlungsverfahrens kommt. Doch nur in Einzelfällen war die Frist ab dem Ereignistag bemessen. Vielmehr war es in aller Regel der Tag der Eingabe der Daten in POLAS.

Dieser Zeitpunkt der Erfassung hängt von Zufälligkeiten (z.B. Zeitpunkt der Anzeigenerstattung) oder polizeiinternen Abläufen ab und ist für die Berechnung von Fristen völlig ungeeignet. Nach unseren Feststellungen wich er durchschnittlich einen bis drei Monate vom Tattag ab, in 28 der überprüften Fälle jedoch mehr als sechs Monate bis zu einigen Jahren. Dies hat zu einer unzulässigen und bei Abweichungen über mehrere Monate auch völlig unverhältnismäßigen Fristverlängerung geführt.

Ursache hierfür war die programmtechnische Anbindung des durch POLAS vorgegebenen Prüfdatums an die POLAS-Erfassung bzw. -Aktualisierung. Wir haben gefordert, dieses Verfahren zu ändern. Dem ist die Polizei gefolgt; Anknüpfungspunkt für die Fristberechnung ist in Zukunft ausschließlich der Tag des Ereignisses, das zur Anlegung der Kriminalakte geführt hat. Zu diesem Zweck wird im neuen POLAS-Verfahren (siehe unten 16.4) ein besonderes Datenfeld „Ereigniszeit" eingeführt, das als absolutes Bezugsdatum für die Berechnung des Prüfdatums dient. Damit wird für die Zukunft eine wesentliche Verbesserung geschaffen.

Die von uns festgestellten Fälle mit unzutreffender Fristberechnung sind bereinigt worden. Besonders zu begrüßen ist es, daß die Polizei sich auch für den gesamten Altbestand der Kriminalakten um eine Lösung dieses Problems bemüht. Im neuen POLAS-Verfahren werden alle Laufzeiten von mehr als fünf Jahren überprüft. Dadurch sollen alle Datensätze mit einer Laufzeit von mehr als zehn Jahren festgestellt und ausgedruckt werden, um sie zu bereinigen und sukzessive den vom Gesetz vorgesehenen Zustand zu erreichen.

In 42 der überprüften Fälle war darüber hinaus statt der unserer Auffassung nach gebotenen 5-Jahres-Frist die 10-Jahres-Frist eingegeben. Nach der

Rechtsprechung des Bundesverwaltungsgerichts und nunmehr § 16 Abs. 2 Satz 3 DVPolG ist insbesondere die Schwere der Tat maßgeblich für die Anlegung und Aufbewahrung von Kriminalakten. Soweit die geringe Bedeutung der Tat nicht bereits grundsätzlich gegen deren Anlegung spricht, ist die Schwere bei der Festlegung der Fristen zu berücksichtigen. Die KpS-Richtlinien geben hierfür praktikable Anhaltspunkte. Daneben ist insbesondere der Verfahrensausgang zu berücksichtigen. Bei Einstellungen nach § 153 Abs.1 StPO (Bagatellsachen) oder den entsprechenden Vorschriften des Jugendgerichtsgesetzes liegen staatsanwaltschaftliche oder gerichtliche Wertungen vor, die eindeutig gegen die 10-Jahres-Frist sprechen. Ferner ist bei Verurteilungen zu Geldstrafen bis zu 50 Tagessätzen von Fällen geringer Bedeutung auszugehen.

Die relativ große Anzahl von Fällen, die als Bagatellsachen mit 10-Jahres-Fristen versehen wurden, ist nach unserem Eindruck darauf zurückzuführen, daß Rückmeldungen über den Ausgang des Verfahrens in erster Linie zur Prüfung der weiteren Aufbewahrung der Unterlagen, jedoch nicht zur Prüfung der Änderung der Aufbewahrungsfrist führten.

Die fehlende Festlegung von 5-Jahres-Fristen bei Fällen, die in den KpS-Richtlinien ausdrücklich genannt sind, wurde anscheinend dadurch verursacht, daß die 10-Jahres-Frist programmtechnisch vorgegeben war. Sofern nicht erkannt wurde, daß die Tat zum Katalog der Fälle geringer Bedeutung gehört, die sachbearbeitende Dienststelle den hierzu vorgesehenen Vermerk nicht angebracht hat oder dieser bei der Eingabe übersehen wurde, erfolgte automatisch die Festlegung der zu langen 10-Jahres-Frist.

Diesen strukturellen Mangel kann man nur dadurch abstellen, daß die 5-Jahres-Frist programmtechnisch vorgegeben wird und die Festlegung der 10-Jahres-Frist ggf. manuell erfolgt. Da es sich um Prüffristen handelt und in keinem Fall eine automatische Löschung erfolgt, wären „zu kurze" Fristen unschädlich und einfach zu korrigieren. An stark verkürzten Prüffristen scheint ohnehin ein fachliches Interesse zu bestehen: So haben wir eine relativ große Anzahl von Kriminalakten über Rauschgiftabhängige festgestellt, in denen Prüffristen von einem oder zwei Jahren verfügt waren. Diese Vorgehensweise ist grundsätzlich zu begrüßen – vorausgesetzt, die 5- bzw. 10-Jahres-Frist wird in der Summe nicht überschritten.

Auch hier ist die Polizei unserem Vorschlag gefolgt und wird in Zukunft für alle Fälle eine Laufzeit von zunächst fünf Jahren unabhängig von der Schwere des Delikts festlegen. In Fällen, in denen eine längere Speicherfrist zulässig ist, wird sie nach der Entscheidung des Sachbearbeiters auf maximal zehn Jahre verlängert.

Die von uns festgestellten Einzelfälle mit falschem Fristbeginn oder zu langer Frist wurden von der Polizei geprüft und bereinigt.

16.3.2 Weitere Probleme

In 7 Fällen war zweifelhaft, ob überhaupt ein hinreichender Anlaß für die Anlegung der Kriminalakten vorlag. Einen Schwerpunkt in diesem Problembereich

bildeten ausländerrechtliche Sachverhalte. So fanden sich Unterlagen über Asylantragsteller mit erkennungsdienstlichen Unterlagen aus dem Asylverfahren in Kriminalakten, die bisweilen Verdachtsmomente auf illegale Einreise, aber teilweise keinerlei Hinweise auf die Einleitung strafrechtlicher Ermittlungsverfahren oder deren Ausgang enthielten. In einigen Fällen sind inzwischen Löschungen erfolgt bzw. Hinweise auf Asylverfahren in den Akten oder POLAS getilgt worden, in anderen Fällen haben wir nach näherer Darlegung durch die Polizei die Aufbewahrung der Kriminalakten akzeptiert.

Grundsätzlich ist festzustellen, daß erkennungsdienstliche Behandlungen nach AuslG oder AsylVfG nur zu den Zwecken gespeichert werden können, die in den einschlägigen Vorschriften genannt sind (Identitätsfeststellung, Durchführung von ausländerrechtlichen Verfahren), nicht jedoch zur vorbeugenden Bekämpfung von Straftaten. Eine schlichte „Umwidmung" der nach anderen Vorschriften erhobenen ed-Unterlagen ist nur zulässig, wenn die Erhebungsvorschrift auch den Zweck der vorbeugenden Bekämpfung von Straftaten umfaßt (§ 41 Abs. 3 AuslG: Fälle der Paßfälschung oder Verdacht auf erneute illegale Einreise; § 86 Abs. 2 Satz 2 Strafvollzugsgesetz bei Strafgefangenen). Ferner können erkennungsdienstliche Unterlagen auch dann „umgewidmet" werden, wenn die ed-Behandlung zwar nach einer anderen – nicht präventivpolizeilichen – Vorschrift durchgeführt wurde, sie jedoch auch zur vorbeugenden Bekämpfung von Straftaten zulässig wäre, um eine zweite, den Betroffenen zusätzlich belastende ed-Behandlung zu vermeiden. Anhaltemeldungen (Feststellung der Personalien) können die Anlegung von Kriminalakten nicht begründen.

Auch in Fällen, in denen Personen lediglich als vermißt gemeldet wurden, haben wir Kriminalakten vorgefunden. Wenn besondere Umstände vorliegen, die zum Wiederauffinden der vermißten Personen beitragen können, kann auch die Anlegung von Kriminalakten aus diesem Grund in Betracht kommen (z.B. die vermißte Person hält sich immer wieder nach ihrem Verschwinden an bestimmten Orten auf). Wenn jemand jedoch 2 Stunden nach der Vermißtenanzeige in einer Gaststätte wiederaufgefunden wird, rechtfertigt dies nicht die Anlegung und Aufbewahrung einer Kriminalakte mit einer Frist von fünf Jahren. Diese Akte wurde gelöscht.

Nach § 16 Abs. 2 Satz 4 DVPolG sind Daten, die nach Einleitung eines Ermittlungsverfahrens in Kriminalakten und POLAS gespeichert werden, zu löschen, wenn der dem Verfahren zugrunde liegende Verdacht entfällt. Diese aus rechtsstaatlichen Grundsätzen zwingende Regelung kann nur dann eingehalten werden, wenn die Polizei das Ergebnis des staatsanwaltschaftlichen oder gerichtlichen Verfahrens erfährt. Die Rückmeldung über den Verfahrensabschluß ist auch für die Frage, welche Daten gespeichert werden können und wie die Frist zu bemessen ist, von Bedeutung.

Seit Jahren ist zwischen Staatsanwaltschaft und Polizei ein Verfahren vereinbart, in dem formularmäßig das Ergebnis des Verfahrens nach Abschluß mitge-

teilt wird. Dies hat zwar zu wesentlichen Verbesserungen geführt, ist aber nach unseren Feststellungen immer noch nicht frei von Mängeln. In 36 der überprüften Akten fehlten die Rückmeldungen über den Verfahrensausgang. Hierbei haben wir solche Fälle nicht aufgenommen, in denen die polizeiliche Sachbearbeitung erst 1991 abgeschlossen wurde, da hier damit gerechnet werden kann, daß noch Rückmeldungen eintreffen. In einer Reihe der 36 Fälle sind inzwischen Löschungen erfolgt. In anderen hat der Verfahrensausgang die polizeiliche Prognose bestätigt.

Wir haben die Prüfung zum Anlaß genommen, das Problem erneut mit der Staatsanwaltschaft, die für das Rückmeldeverfahren die Verantwortung trägt, zu erörtern, um durch organisatorische Maßnahmen Verbesserungen zu erreichen. Die Erörterungen hierüber sind noch nicht abgeschlossen.

Die Anlegung von Kriminalakten setzt grundsätzlich voraus, daß eine sog. Negativprognose über die betroffene Person abgegeben werden kann. § 16 Abs. 2 Satz 3 DVPolG stellt dies nunmehr ausdrücklich fest: „... bei denen wegen Art, Ausführung oder Schwere der Tat und der Persönlichkeit des Betroffenen die Besorgnis der Begehung weiterer Straftaten besteht."

Im Rahmen der Querschnittsprüfung war es nicht möglich, alle bei der polizeilichen Sachbearbeitung heranzuziehenden Gesichtspunkte aus dem Ermittlungsverfahren und dessen Ausgang zu berücksichtigen. Grundsätzlich kann jedoch festgestellt werden, daß die Schilderung der Tat in den Merkblättern durchweg aussagekräftig war und die Negativprognosen nachvollziehbar machte. In 10 Fällen traf dies jedoch nicht ohne weiteres zu. Sie betrafen im wesentlichen Freisprüche, Verfahrenseinstellungen und die Ablehnung der Eröffnung des Hauptverfahrens durch das Gericht, zu denen die entsprechenden Entscheidungstexte nicht vorlagen, so daß wegen der nicht eindeutigen Darstellung durch die polizeilichen Sachbearbeiter die Negativprognose nicht offenkundig war. Die Mehrzahl dieser Akten wurde inzwischen gelöscht, in zwei Fällen hält die Polizei die weitere Aufbewahrung aufgrund ihrer Prognose für erforderlich.

16.3.3 Schlußfolgerungen aus der Prüfung

Entsprechend der Häufigkeit in der Kriminalstatistik bezog sich eine große Anzahl der überprüften Akten auf Delikte wie einfacher Ladendiebstahl durch Kunden, Erschleichen von Leistungen („Schwarzfahren") und auch Straftaten nach dem Ausländergesetz, die mit einer Höchststrafe von 1 Jahr bedroht sind. Nach dem erwähnten § 16 Abs. 2 Satz 3 DVPolG ist die Anlegung von Kriminalakten insbesondere von den Kriterien „Art, Ausführung und Schwere" der Tat abhängig. Die Speicherung der Daten muß ferner zur Aufgabenerfüllung der Polizei erforderlich sein. Wir diskutieren mit der Polizei, ob und unter welchen Kriterien bei den oben genannten Bagatell- und Massendelikten die Anlegung von Kriminalakten überhaupt der Aufgabenerfüllung der Polizei dienen kann. Die Erörterungen hierüber sind noch nicht abgeschlossen.

16.4 Einführung eines Systems zur Überprüfung von Zugriffsberechtigungen für das POLAS/INPOL-System

Die seit langem überfällige Einführung eines wirksamen Verfahrens zur Prüfung der Zugriffsberechtigung für das automatisierte polizeiliche Auskunftssystem POLAS-Hamburg und das bundesweite INPOL-System (9. TB, 4.12.4) ist auch im Berichtszeitraum immer noch nicht abgeschlossen worden. Wie dringend erforderlich die vom Hamburgischen Datenschutzgesetz vorgeschriebenen technischen und organisatorischen Maßnahmen zur Zugriffssicherung sind, wird zum einen deutlich, wenn man sich den unter 16.3 geschilderten Datenumfang von POLAS vergegenwärtigt; zum anderen ist auch erneut deutlich geworden, daß Hilfskonstruktionen eine unmittelbar am Datenendgerät wirksame technische Prüfung der Zugriffsberechtigung nicht ersetzen können.

Im 9. TB (a.a.O) ist beschrieben worden, daß durch die Einführung eines Protokollbuchs versucht wurde, wenigstens bei Direktabfragen aus dem Melderegister für eine Übergangsphase den gesetzlichen Anforderungen zu entsprechen. Die Erwartungen, die wir und die Polizei gleichermaßen hiermit verbunden hatten, konnten nicht erfüllt werden. Zwar hat die Mehrzahl der Beamten die Mühe auf sich genommen, ihre Melderegisterabfragen in den vorgeschriebenen Protokollbüchern handschriftlich einzutragen. Bei Stichproben zeigten sich im Vergleich mit den Maschinenprotokollen jedoch erhebliche Lücken. Im Ergebnis wurden daher die sorgfältig arbeitenden Beamten mit zusätzlichem Aufwand belastet; die weniger sorgfältigen, die die Eintragungen unterließen und bei denen schon deshalb Anlaß zur Kontrolle besteht, waren jedoch nicht feststellbar. Wir haben daher unserer Forderung nach möglichst rascher Einführung des geplanten automatisierten Verfahrens zur Berechtigungsprüfung erneut Nachdruck verliehen.

Auf Nachfrage ist uns zugesagt worden, daß das Verfahren jedenfalls bis Ende dieses Jahres eingeführt werde. Bei Redaktionsschluß war das Verfahren allerdings noch nicht so weit fortgeschritten, daß eine datenschutzrechtliche Prüfung möglich gewesen wäre.

16.5 Akten über politische Organisationen beim polizeilichen Staatsschutz

Im Rahmen einer datenschutzrechtlichen Prüfung von Speicherungen legte die Staatsschutzabteilung beim Landeskriminalamt Ende 1990 verschiedene Unterlagen vor. Hierzu gehörte auch eine Personenakte, in der sich aus dem Jahre 1983 insgesamt 10 Merkblätter sowie eine listenmäßige Zusammenfassung über diese Unterlagen befanden. Sie enthielten Angaben darüber, daß die betroffene Person 1983 z.T. allein und z.T. mit anderen Personen Demonstrationen, Mahnwachen und Informationsstände von „amnesty international" angemeldet hatte. Die Demonstrationen etc. richteten sich damals hauptsächlich gegen Menschenrechtsverletzungen in Südamerika. Irgendwelche Hinweise auf Verstöße gegen Tatbestände des Strafgesetzbuchs oder anderer Gesetze

waren im Unterschied zu weiteren in der Akte enthaltenenen Vorgängen aus späteren Jahren, die sich nicht auf „amnesty international" bezogen, nicht verzeichnet.

Aus allen diesen Merkblättern aus dem Jahr 1983 mit dem Hintergrund rechtmäßiger Demonstrationen ging hervor, daß sie einer Fallakte über „amnesty international" entnommen waren. Auch diese Fallakte wurde eingesehen. Sie enthielt ein Vorblatt mit einer allgemeinen Beschreibung der Zielsetzung von „amnesty international" aus dem Jahr 1966 mit Angaben über die damaligen Gründungsmitglieder. Ferner waren in ihr ein Flugblatt, Merkblätter mit Hinweisen auf Demonstrationen – zuletzt vom September 1990 – sowie auf eine in Hamburg veranstaltete Jahresversammlung der Organisation abgelegt. Die in der Personenakte abgelegten Merkblätter waren nicht in der Fallakte enthalten. Querverweise auf diese oder andere Personenakten waren nicht ersichtlich. In der Fallakte wurden keinerlei Vorgänge über strafrechtlich relevante Sachverhalte festgestellt. Entgegen in den Medien geäußerten Vermutungen ließ die Akte auch keinerlei Rückschlüsse auf eine systematische Beobachtung oder gar den Einsatz verdeckter Ermittlungsmethoden zu. Sie stellte eher ein unstrukturiertes „Sammelsurium" dar.

Die Herkunft der Merkblätter über Demonstrationen etc. erläuterten die Mitarbeiter der Staatsschutzabteilung dadurch, daß die Abteilung bei allen Anmeldungen nach dem Versammlungsgesetz zur Lagebeurteilung beteiligt wird.

Unmittelbar nach diesen Feststellungen wurde im Dezember 1990 aus datenschutzrechtlicher Sicht gegenüber dem Polizeipräsidenten und der Behörde für Inneres deutlich gemacht, daß die Anlegung und Führung dieser Fallakte über „amnesty international" nicht zulässig ist. Dabei wurde davon ausgegangen, daß es nicht zu den Aufgaben der Polizei gehört, Organisationen, die den Schutz der Vereinigungsfreiheit genießen und deren Mitglieder von ihrem Grundrecht auf Meinungs- und Versammlungsfreiheit Gebrauch machen, nach polizeilichen Kriterien zu erfassen. Ansatzpunkt für polizeiliche Tätigkeit und Datenspeicherung kann nur die Abwehr von Gefahren und Verfolgung von Straftaten im Einzelfall sein. Akten im Bereich des polizeilichen Staatsschutzes können nur diesen Zwecken dienen.

Die Fallakte über „amnesty international" konnte diese Zwecke jedoch in keiner Weise erfüllen. Von der Organisation gehen keine Gefahren für die öffentliche Sicherheit oder Ordnung aus, sie ist auch strafrechtlich von keinerlei Interesse. Die gleichen Überlegungen gelten auch für Personenakten. Die Anmeldung einer rechtmäßigen Versammlung kann daher auch kein Anlaß für die Anlegung einer polizeilichen Akte sein.

Selbst wenn eine Beteiligung des Landeskriminalamtes bei der Anmeldung von Versammlungen nach dem Versammlungsgesetz erforderlich sein sollte, um im Vorfeld zu klären, ob Gefahren von dieser Versammlung ausgehen können

oder für sie drohen, rechtfertigt dies keine Speicherung der betreffenden Vorgänge in einer polizeilichen Akte. Entsprechende Meldungen werden vielmehr nach Abschluß der Versammlung nicht mehr benötigt und sind zu vernichten, es sei denn, daß die Versammlung strafbar verlaufen ist oder Anlaß für polizeiliches Einschreiten gegeben hat.

Der festgestellte Vorgang hat deutlich gemacht, daß die Speicherung entsprechender Meldungen in polizeilichen Akten auch geeignet ist, die betroffene Organisation insgesamt zu diskreditieren. In der anfangs erwähnten Personenakte war ein Fernschreiben einer Polizeidienststelle außerhalb Hamburgs enthalten, in dem nach Erkenntnissen zur betroffenen Person aus Anlaß von strafrechtlichen Ermittlungen ohne jeden Bezug zu „amnesty international" gefragt wurde. Hierauf antwortete die Staatsschutzabteilung in Hamburg mit einem Fernschreiben, daß die betroffene Person 1983 als Anmelderin von Veranstaltungen der Organisation „amnesty international" gegen das Verschwinden von Personen in Südamerika amtsbekannt sei. Diese Angaben seien nicht gerichtsverwertbar. Weitere Erkenntnisse lägen nicht vor. Das Fernschreiben war an verschiedene Polizeidienststellen eines anderen Bundeslandes, das dortige Innenministerium sowie das Bundeskriminalamt gerichtet. Somit wurde gegenüber zahlreichen Stellen aufgrund der ohne relevanten Anlaß angelegten Personenakte ein Zusammenhang zwischen der Organisation „amnesty international" und strafbaren Vorgängen hergestellt, der tatsächlich überhaupt nicht bestand.

Wir haben gefordert, die Fallakte über „amnesty international" und etwaige Hinweise hierauf in Aktennachweisen und Vorgangsverwaltungsdateien unverzüglich zu vernichten und die auf Veranstaltungen von „amnesty international" bezogenen Merkblätter in der Personenakte sowie alle auf diese Vorgänge bezogenen Hinweise in dieser Akte auszusondern und zu löschen. Dies ist nach einer Entscheidung des Präses der Behörde für Inneres geschehen.

Darüber hinaus haben wir folgende Forderungen aufgestellt: Sofern weitere Fallakten über vergleichbare Organisationen bestehen, bei denen ebenfalls keine strafrechtliche Relevanz vorliegt, sind auch diese unverzüglich zu vernichten. Sofern in sonstigen Unterlagen der Polizei Hinweise auf die oben genannten zu löschenden Unterlagen festgestellt werden, sind auch diese Hinweise zu löschen. Hierzu hat uns die Behörde für Inneres mitgeteilt, daß unsere Feststellungen zum Anlaß genommen worden seien, Form und Inhalt der Führung solcher Fallakten einer genaueren Prüfung zu unterziehen. Dies berühre jedoch grundlegendere Fragen der Aktenhaltung und des Arbeitsablaufs, die nicht kurzfristig zu klären seien.

Nachdem Monate später in den Medien über die Akte zu „amnesty international" berichtet worden war, wurde bekannt, daß auch Akten zu Organisationen wie „Greenpeace" oder „Robin Wood" bestehen. Wir haben daraufhin um Stellungnahme in Form eines Zwischenberichts gebeten, über welche Organisationen, gegen die kein Verdacht von strafbaren Handlungen nach dem 1.-5.

Abschnitt des Besonderen Teils des Strafgesetzbuchs (d.h. wegen Staatsschutzdelikten) oder wegen Bildung einer kriminellen oder terroristischen Vereinigung besteht, Fallakten beim Staatsschutz vorliegen bzw. bis in letzte Zeit vorgelegen haben und welche Kriterien für die Führung derartiger Akten aus Sicht der Polizei zugrunde gelegt werden.

Hierauf haben wir erfahren, daß die organisationsbezogene Sammlung bei der Staatsschutzabteilung der Polizei mehrere hundert Fallakten umfaßt hat, wobei es sich bei einer erheblichen Anzahl um politische Vereinigungen oder um Institutionen z. B. aus dem Medienbereich handelte, die im öffentlichen Leben nicht ernsthaft als Gefahr für die öffentliche Sicherheit oder als strafrechtlich relevant angesehen werden können.

Uns ist dann von der Behörde für Inneres mitgeteilt worden, eine erste Bestandsaufnahme habe ergeben, daß bereits ein Viertel des Aktenbestandes vernichtet worden sei, da die Unterlagen für die Aufgabenbewältigung ungeeignet waren. Diese Aussage ist allerdings bemerkenswert, als einerseits eingeräumt wird, daß ein großer Teil der in diesem Zusammenhang gespeicherten Informationen für die gesetzlichen Aufgaben der Polizei ohne Bedeutung und daher unzulässig war, andererseits jedoch unbeantwortet bleibt, warum und aus welchen Anlässen die Sammlungen überhaupt angelegt worden sind und welche Organisationen und Institutionen hier betroffen waren. Nach Auskunft der Behörde für Inneres von Anfang Dezember 1991 wird weiter mit Nachdruck an dem Thema gearbeitet. Es ist nunmehr beabsichtigt, möglichst im 1. Quartal 1992 das neue Konzept für die Aktenhaltung in diesem Bereich vorzulegen.

Da Ausgangspunkt der Anlegung von organisationsbezogenen Fallakten nach unseren Feststellungen und Äußerungen der Polizei in den Medien insbesondere die Anmeldung von Demonstrationen, Info-Ständen etc. ist, haben wir ferner gefordert, das Verfahren bei der polizeilichen Anmeldung von Versammlungen und die daraus folgenden Informationsflüsse zu überprüfen. Dies betrifft vor allem die sog. Meldungen wichtiger Ereignisse (WE-Meldungen), die offenbar alle Arten von Demonstrationen umfassen.

Eine Aufbewahrung von Meldungen über Demonstrationen über einen Zeitraum von 3 Jahren, die derzeit vorgesehen ist, halten wir dann nicht für akzeptabel, wenn sie einen Bezug zu den Veranstaltern oder Teilnehmern der Demonstration enthalten und die Demonstration störungsfrei verlaufen ist. Das Verfahren im Zusammenhang mit der Anmeldung von Versammlungen ist vielmehr nach der Rechtsprechung des Bundesverfassungsgerichts (Brokdorf-Urteil) am Maßstab des Grundrechts nach Art. 8 GG auszurichten und darf nicht zu einer Registrierung und damit Beeinträchtigung der grundsätzlich staatsfreien Ausübung des Grundrechts führen.

Somit können personenbezogene Daten aus Anlaß von Versammlungen weder akten- noch dateimäßig gespeichert werden, es sei denn, daß die Versammlung strafbar verlaufen ist oder Anlaß für polizeiliches Einschreiten gegeben

hat. Nur in diesen Fällen kann eine Speicherung der Personen, gegen die ermittelt wird oder gegen die zur Gefahrenabwehr eingeschritten worden ist, in Ermittlungsakten bzw. zur Dokumentation polizeilichen Handelns erfolgen und – sofern die Voraussetzungen dafür vorliegen – in kriminalpolizeilichen Sammlungen in Betracht kommen.

Die Behörde für Inneres hat hierzu noch nicht Stellung genommen. Sie will dieses Problem unabhängig von der Bereinigung der Fallakten behandeln.

16.6 Speicherung von Kindern in polizeilichen Dateien?

Polizeiliche Dateien sind in aller Regel sog. kriminalpolizeiliche personenbezogene Sammlungen (KpS). Das heißt, es werden Personen erfaßt, gegen die ein strafrechtliches Ermittlungsverfahren eingeleitet worden ist und bei denen wegen der Art, Ausführung oder Schwere der Tat und der Persönlichkeit des Betroffenen die Besorgnis der Begehung weiterer Straftaten besteht (§ 16 Abs. 2 Satz 3 DVPolG). Kinder unter 14 Jahren sind nach § 19 des Strafgesetzbuches schuld- und damit strafunmündig; gegen sie kann kein strafrechtliches Ermittlungsverfahren eingeleitet werden. Somit fehlt grundsätzlich die rechtliche Voraussetzung für die Speicherung von Kindern unter 14 Jahren in kriminalpolizeilichen Sammlungen.

Bisher wurden daher Kinder nicht in polizeilichen Dateien gespeichert. Es besteht jedoch die Absicht, diese Praxis in einzelnen Deliktsbereichen zu ändern. So führt die für Rauschgiftkriminalität zuständige Abteilung des Landeskriminalamtes mit einer besonderen Ermittlungsgruppe seit 1989 an erkannten Brennpunkten des Rauschgifthandels gezielt Maßnahmen gegen die am Handel beteiligten Personen durch. Generell gestaltet sich die Entlarvung der in dieser Szene verwickelten Täter wegen deren Abschottung und dem Mangel an Anzeigen anderer Beteiligter äußerst schwierig. Allerdings hat die Vorlage von Lichtbildern von Tätern, deren genaue Identität nicht immer bekannt war, bei aussagewilligen Personen häufig zur Identifizierung und Aufklärung von Tatkomplexen geführt. Es soll daher eine Lichtbildersammlung als Datei angelegt werden, um diesen Ermittlungsansatz zu unterstützen. In der Errichtungsanordnung ist vorgesehen, auch Kinder unter 14 Jahren zu erfassen.

Hierzu hat die Polizei erläutert, daß im Drogenhandel zunehmend auch Kinder in Erscheinung getreten sind. Nach der Kriminalstatistik waren es 1989 zwei und 1990 sieben Personen unter 14 Jahren. Ferner sei zu berücksichtigen, daß nach den polizeilichen Feststellungen Kinder auch gezielt von Erwachsenen in das Verteilsystem eingebunden werden. Bei dieser Ausgangssituation haben wir der Erfassung von Kindern in der Lichtbilderdatei unter besonderen Voraussetzungen zugestimmt. Wenn durch Speicherungen über die Kinder Ansatzpunkte zur Verfolgung der Hintermänner gefunden werden können, kann nur dieser Zweck die Speicherung von Kindern zur Abwehr von Gefahren – auch für die Kinder selbst – rechtfertigen. Dieser Gesichtspunkt muß daher in der Errichtungsanordnung und der Speicherungspraxis strikt beachtet werden.

Eine Speicherung von Kindern in der bloßen Erwartung, daß ihre Daten nach Erreichen der Strafmündigkeit für Verfahren gegen sie selbst gebraucht werden können, wäre dagegen nach der klaren Wertung des Gesetzgebers in § 19 StGB und in § 16 Abs. 2 Satz 3 DVPolG unzulässig. Wegen des begrenzten Zwecks der Speicherung von Kindern in der hier betroffenen Datei scheidet eine Übernahme der Daten in die Kriminalaktenhaltung und POLAS aus. Wir haben daher folgende Regelung in der Errichtungsanordnung vorgeschlagen:

„Strafunmündige Kinder werden in die Datei nur aufgenommen, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß sie von strafmündigen Personen für Taten eingesetzt werden, zu deren vorbeugender Bekämpfung oder Verfolgung die Daten erforderlich sind. Die Daten der Kinder dürfen nicht in andere Dateien und kriminalpolizeiliche Sammlungen übernommen werden." Dieser Forderung hat die Polizei Rechnung getragen. Ferner haben wir deutlich gemacht, daß mit unserer Zustimmung zur Speicherung von Kindern in dieser Datei kein Präjudiz für andere Dateien verbunden ist.

16.7 Datei Gewalttäter Sport

Die Zunahme von gewalttätigen Ausschreitungen im Zusammenhang mit Fußball- und sonstigen Sportveranstaltungen ist unverkennbar und stellt die Polizei vor schwierige Probleme. Zur Verfolgung von einschlägigen Straftaten verfügt die hamburgische Polizei über die Lichtbilder von Tätern, die hier bereits als Fußball-Rowdies in Erscheinung getreten sind. Sie werden in der Datei junger Gewalttäter gespeichert. Gegen deren Nutzung bestehen – unter dem Vorbehalt, daß die Vorraussetzungen für die Speicherung von erkennungsdienstlichen Unterlagen und die Kriterien der Errichtungsanordnung eingehalten werden, – aus unserer Sicht keine Bedenken (siehe auch 9. TB, 4.12.7).

Die Innenministerkonferenz hat im Mai 1991 beschlossen, eine Datei Gewalttäter Sport einzuführen. Nach den bisherigen Planungen soll sie als automatisierte Verbunddatei beim Bundeskriminalamt geführt werden. Anlaßbezogen sollen alle Länderpolizeien Zugriff auf die Daten erhalten. Es ist vorgesehen, Personen, gegen die Ermittlungsverfahren im Zusammenhang mit Ausschreitungen bei Sportveranstaltungen eingeleitet bzw. Stadionverbote verhängt wurden oder die im Zusammenhang mit Sportveranstaltungen in Gewahrsam genommen oder mit Waffen etc. angetroffen worden sind, in der Datei zu speichern. Folgende Daten sollen aufgenommen werden: Personalien; Hinweis auf evtl. Bildaufzeichnungen; Zugehörigkeit zu bestimmten Störergruppen; Anlässe und Umstände, die zur Aufnahme in die Datei führen; Informationen über Reisewege, Antrefforte und Umstände der Überprüfungen im Zusammenhang mit Sportveranstaltungen.

Ursprünglich hatte die Innenministerkonferenz im Dezember 1990 vorgesehen, die Datenschutzbeauftragten des Bundes und der Länder schon bei der Frage zu beteiligen, ob die Datei eingerichtet werden soll. Hierzu ist es nicht gekommen. Erst nach dem Beschluß der IMK vom Mai 1991 bin ich als Vorsitzender des Arbeitskreises Sicherheit der Datenschutzbeauftragten im Auftrag der Innenministerkonferenz gebeten worden, eine Stellungnahme der Datenschutzbeauftragten herbeizuführen.

Bei den weiteren polizeiinternen Überlegungen zur Einrichtung der Datei hat sich jedoch gezeigt, daß eine Realisierung der Datei als automatisierte Verbunddatei nur möglich ist, wenn auf das bestehende INPOL-System zurückgegriffen werden kann. Das Bundeskriminalamt hat mitgeteilt, daß es derzeit keine INPOL-Anwendung gibt, die den fachlichen Anforderungen der vorgesehenen Datei Gewalttäter Sport entspricht. Die Erarbeitung einer Errichtungsanordnung sei daher verfrüht. Vielmehr seien zunächst die datenverarbeitungstechnischen Realisierungsmöglichkeiten zu prüfen.

Damit sind unsere frühzeitig geäußerten Zweifel an der Realisierbarkeit der Datei und ihrer Geeignetheit zunächst bestätigt worden. Die Konferenz der Datenschutzbeauftragten hat von einer förmlichen Beschlußfassung abgesehen und mitgeteilt, daß sie bislang nicht über hinreichende Informationen verfügt, um sich eine abschließende Meinung zur Geeignetheit und Erforderlichkeit einer solchen Datei bilden zu können. Für den Fall, daß das Projekt weiterverfolgt wird, gehen die Datenschutzbeauftragten davon aus, daß sie in allen wesentlichen Phasen unmittelbar und ständig informiert werden.

Aufgrund des derzeitigen Kenntnisstandes sind von der Konferenz der Datenschutzbeauftragten folgende Problembereiche gesehen worden:

— Auf welche Personen werden die in einer Verbunddatei zu speichernden Daten beschränkt? Nach welchen Kriterien und unter Bezug auf welche konkreten Straftatbestände kann eine Speicherung erfolgen?

— Welche personenbezogenen Merkmale von Betroffenen werden anhand welches festgelegten Datensatzes gespeichert?

— Welche Polizeidienststellen sollen für die jeweiligen Sportveranstaltungen Zugriff auf die entsprechenden Speicherungen haben?

— Welche Speicherungs- bez. Aufbewahrungsfristen sind vorgesehen?

— Wann erfolgt die Löschung?

Die Datenschutzbeauftragten des Bundes und der Länder werden sich im Detail zu dem geplanten Projekt äußern, wenn es zu einem Entwurf einer Errichtungsanordnung kommen sollte. Zu klären wäre dann insbesondere, ob und wie Bundeskriminalamt und Bundesgrenzschutz im Rahmen eines Online-Verfahrens auf die Datei zugreifen dürften, unter welchen Voraussetzungen Übermittlungen an Veranstalter und an Betreiber von Sportstätten in Betracht kommen könnten und ob die Datei zunächst nur vorläufig und befristet eingeführt werden soll, um damit Erfahrungen sammeln zu können.

16.8 Verbessertes Verfahren für die Aufbewahrung von Anträgen auf Auskunft und Löschung

Im 9. TB (4.12.8) war kritisiert worden, daß schriftliche Vorgänge im Zusammenhang mit der Erteilung von Auskünften oder Löschungen polizeilicher Datenspeicherungen bei der dateiführenden Stelle aufbewahrt worden sind und somit auch nach Ablauf von Löschungsfristen als Ersatz für die ursprünglichen dateimäßigen Speicherungen dienen konnten.

Durch ein neues Verfahren ist dieser Mißstand inzwischen weitgehend bereinigt worden. Grundsätzlich werden danach Ersuchen um Auskunft oder Löschung sowie die Stellungnahmen und Bescheide der Polizei hierzu von den Unterlagen in den kriminalpolizeilichen Sammlungen räumlich und organisatorisch getrennt. Diese die Speicherung betreffenden Unterlagen werden ein Jahr nach Löschung in der Datei vernichtet.

Wird bei einer Überprüfung festgestellt, daß dateimäßig gespeicherte Daten zu löschen sind, werden die Daten in der Datei gelöscht; die dazugehörenden aktenmäßigen Unterlagen werden noch 6 Wochen getrennt aufbewahrt, um etwaige Nachfragen beantworten zu können.

Es hat sich inzwischen gezeigt, daß dieses Verfahren praktikabel ist und mehr Klarheit schafft, als die im 9. TB kritisierte frühere Praxis.

16.9 Arbeitsdatei PIOS Innere Sicherheit (APIS)

Im 9. TB (4.12.5.2) war die Prüfung von Speicherungen in der Datei APIS von 1990 beschrieben worden. Nachdem mehr als 15 Monate seit dieser Prüfung vergangen sind, können wir nunmehr endlich über den Abschluß berichten.

Die offenkundigen Fehlspeicherungen, die bemängelt worden waren, sind korrigiert worden. Zu keiner einverständlichen Lösung ist es dagegen in den Fällen gekommen, in denen die Speicherung einer Gruppe von Hausbesetzern wegen Haus- und Landfriedensbruch kritisiert worden war. Die Kritik galt zum einen der Tatsache, daß hier unbegründet eine gegen die Verfassung gerichtete Zielsetzung angenommen wurde, die bei einer APIS-Speicherung vorliegen muß. Zum anderen richtete sie sich gegen die Vermischung der Ereignisse, die den in APIS gespeicherten Hausbesetzern zugerechnet werden konnten, mit den Vorgängen, die sich vor dem Haus ohne Beteiligung dieser Personen abspielten.

Zu den Ausführungen zur APIS-Relevanz im Prüfvermerk vom August 1990 hatte die Behörde für Inneres im November 1990 zunächst mitgeteilt, daß über einige dieser Personen wesentliche weitere Erkenntnisse bei der Polizei vorlägen. Eine sachgerechte Beurteilung der Frage, ob die Fälle tatsächlich die Kriterien der Errichtungsanordnung erfüllen, sei ohne Berücksichtigung dieser Gesichtspunkte nicht möglich. Im Dezember 1990 wurden daraufhin die polizeilichen Akten über diese weiteren Erkenntnisse eingesehen.

Hierbei handelte es sich um Unterlagen über Ermittlungsverfahren, die gegen einige der in APIS gespeicherten Personen bereits früher eingeleitet worden waren. In allen Fällen waren die Aktionen mit Straftaten deutlich erkennbar auf politische Themen bezogen, die unbestreitbar auch von Personen mit extremistischen Zielen und massiv gewalttätigem Vorgehen verfolgt werden. Andererseits werden dieselben politischen Themen (z. B. Atomkraftwerke, Dritte Welt, Wohnraumpolitik) auch von Personen aufgegriffen, die sich hierbei völlig gesetzeskonform im Rahmen der Grundrechte bewegen. Die betroffenen Personen hatten dagegen bereits bei den früheren Aktionen den legalen Rahmen verlassen und Sachbeschädigungen bzw. Hausfriedensbrüche begangen.

Bei der Frage, ob über die gebotene Strafverfolgung hinaus APIS-Relevanz vorliegt, reicht allerdings die Feststellung eines Straftatbestands und einer politischen Zielsetzung nicht aus.

Vielmehr muß es sich um eine gegen die verfassungsmäßige Ordnung gerichtete Zielsetzung handeln. Der Schluß von der politischen Motivation auf die Verfolgung extremistischer Ziele ist vor dem Hintergrund der gesellschaftlichen Realität ebensowenig zwingend wie der auf die Verfolgung verfassungskonformer Ziele. Daher besteht bei Straftaten mit politischem Hintergrund für sich betrachtet noch keine Vermutung auf die Verfolgung von Zielen im Sinne der APIS-Errichtungsanordnung. Es müssen vielmehr hinreichend aussagekräftige Anhaltspunkte hinzukommen, die diese Vermutung rechtfertigen.

In den früheren Fällen wie in dem, der zur APIS-Erfassung geführt hat, waren jedoch eher gegenteilige Anhaltspunkte festzustellen, da die Betroffenen offen aufgetreten sind. Typisch für extremistisches Verhalten wäre dagegen anonymes („vermummtes") Vorgehen.

Vor dem Hintergrund der älteren Unterlagen ließ sich im Fall der Hausbesetzung, die zur APIS-Erfassung geführt hatte, lediglich konstatieren, daß die Betroffenen bereits früher – und z. T. ebenfalls gemeinsam – unter vergleichbaren Begleitumständen in Erscheinung getreten waren. Dies reicht für die Aufnahme in Kriminalakten aus (siehe 16.3), nicht jedoch für eine APIS-Erfassung.

Wir haben uns bei dieser Bewertung vor allem an den Kriterien Schwere der Tat und überörtliche Bedeutung orientiert. Dabei war zum einen die Aussage der Behörde für Inneres maßgebend, wonach Hamburg sich vor allem deshalb weiterhin am bundesweiten Verbundsystem APIS beteilige, um die Polizeien anderer Bundesländer nicht von relevanten Informationen aus Hamburg abzuschneiden.

Zum anderen entspricht dies auch der Diskussion, die wir über das Problem der APIS-Relevanz mit anderen Datenschutzbeauftragten des Bundes und der Länder geführt haben. In Schleswig-Holstein ist zwischen dem dortigen Landesbeauftragten, dem Innenministerium und der Polizei eine ergänzende Regelung zur APIS-Errichtungsanordnung entworfen worden. Danach dürfen

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 1000 DM.

Die Fälle der hier relevanten Hausbesetzung erfüllten diese Kriterien nicht. Das Ereignis war allenfalls von lokaler Bedeutung. Bei Geldstrafen zu 20 Tagessätzen bzw. der Einstellung der Verfahren gegen Zahlung von geringfügigen Geldbußen kann nicht von schweren Taten ausgegangen werden. Keiner der Hausbesetzer war gewalttätig gegen Personen vorgegangen, auch wegen Sachbeschädigung war gegen sie kein Ermittlungsverfahren eingeleitet worden. Eine andere Person, die nicht zu den Hausbesetzern gehörte, hatte dagegen bei einem polizeilichen Einsatz eine gefährliches Schlagwerkzeug mit sich geführt. Wir hatten zunächst Zweifel an der APIS-Relevanz dieses Falls geäußert. Unter Zugrundelegung der oben genannten Kriterien haben wir diese jedoch fallen gelassen.

Lange Zeit nach unserer weiteren Stellungnahme haben wir nichts von der Behörde für Inneres gehört. Erst im Oktober 1991 erhielten wir eine Antwort, worin mitgeteilt wurde, daß die von uns kritisierten APIS-Speicherungen bestehen blieben. Man folge zwar unserer Bewertung der früheren Ereignisse weitgehend. Diese seien für die APIS-Erfassung jedoch nicht maßgeblich gewesen. Bei der Beurteilung der gegen die freiheitliche demokratische Grundordnung gerichteten Motivation der Täter sei die Situation des politisch motivierten „Kampfes für selbstbestimmtes Leben und gegen die Umstrukturierung in den Vierteln" zu berücksichtigen. Diese Thematik beherrsche seit längerer Zeit einen Großteil des linksextremistischen Spektrums in Hamburg. Die polizeiliche Bewertung, daß die Taten von einer gegen die freiheitliche demokratische Grundordnung gerichteten Motivation getragen worden seien, sei daher nicht zu kritisieren.

Damit wird erneut die Problematik von APIS deutlich: Maßgeblich für die Speicherung sind letztlich Bewertungen einer politischen Motivation, nicht jedoch kriminalistische Fakten. Eine datenschutzrechtliche Auseinandersetzung über derartige Wertungen erscheint aussichtslos.

Von der zuständigen Staatsanwaltschaft ist uns bestätigt worden, daß gegen keine der betroffenen Personen ein Ermittlungsverfahren wegen Landfriedensbruchs eingeleitet worden ist, sondern die Taten allein unter dem Gesichtspunkt des Hausfriedensbruchs verfolgt worden sind. Somit war die Speicherung in APIS wegen Landfriedensbruchs nach dem Gesetz über die Datenverarbeitung der Polizei und der APIS-Errichtungsanordnung unzulässig. Uns ist nach unserer Anfrage bei der Staatsanwaltschaft von der Polizei mitgeteilt worden, daß die Speicherung wegen Landfriedensbruchs getilgt worden ist.

17. Datenschutz im Rettungsdienst

Mit dem Hamburgischen Rettungsdienstgesetz (HmbRDG) sollen die Notfallrettung und der Krankentransport durch den öffentlichen Rettungsdienst – also durch die Feuerwehr und das Deutsche Rote Kreuz, die Johanniter Unfallhilfe, den Malteser Hilfsdienst und den Arbeiter Samariter Bund – gesetzlich geregelt werden. Das Gesetz soll auch für die in Zukunft neu zuzulassenden privaten Betreiber von Krankentransportunternehmen gelten. Wir haben bei der Behördenabstimmung des Entwurfs den Vorschlag der Behörde für Inneres unterstützt, mit einer bereichspezifischen Vorschrift für alle Träger von Notfallrettung und Krankentransport einheitlich die Verarbeitung von Daten, die bei Einsätzen zur Notfallrettung oder zum Krankentransport anfallen, zu regeln.

Nach § 5 des Gesetzentwurfs dürfen aus diesen Anlässen grundsätzlich Daten nur erhoben, gespeichert, genutzt und übermittelt werden, soweit dies erforderlich ist

1. zur Ausführung oder Abrechnung des Einsatzes,
2. zum Nachweis seiner ordnungsgemäßen Ausführung,
3. zur weiteren medizinischen Versorgung des Patienten oder
4. zur Unterrichtung eines Angehörigen, soweit der Patient nicht seinen gegenteiligen Willen kundgetan hat oder sonstige Anhaltspunkte dafür bestehen, daß eine Übermittlung nicht angezeigt ist.

Damit ist die Datenverarbeitung aus Anlaß von Notfallrettung und Krankentransport grundsätzlich auf den Umfang begrenzt, der unmittelbar im Zusammenhang mit den entsprechenden Einsätzen steht. Die jeweiligen Daten dürfen nach dem Kriterium der Erforderlichkeit nur bezogen auf den konkreten Verwendungszweck verarbeitet werden. Insbesondere ist bei der Datenverarbeitung sicherzustellen, daß Angaben zur weiteren Versorgung des Patienten (medizinische Daten) nicht etwa zu Abrechnungszwecken genutzt und übermittelt werden.

Allerdings war auch zu berücksichtigen, daß es oftmals nicht ausreicht, nur den Rettungseinsatz durchzuführen, sondern daß Daten der Betroffenen auch benötigt werden, um den Eintritt weiterer Schäden zu verhindern. Daher dürfen nach der neuen Vorschrift des § 5 HmbRDG Daten auch übermittelt werden, soweit der Anlaß des Einsatzes (z.B. Verkehrsunfall) zugleich eine Gefahr für die öffentliche Sicherheit darstellt oder sie erst auslöst. Voraussetzung ist jedoch immer, daß die Daten zur Abwehr der Gefahr erforderlich sind und die zuständige Behörde (insbesondere Polizei oder Feuerwehr) hierum ersucht. Der Rettungsdienst darf dagegen keine Daten ohne konkretes Ersuchen zur Gefahrenabwehr – auf Vorrat – an die Polizei übermitteln. Soweit in anderen Spezialgesetzen Pflichten zur Erteilung von Auskünften für bestimmte Zwecke festgelegt werden, bleiben sie unberührt. Diese Regelung war schon deshalb erforderlich, weil bundesgesetzlich geregelte Auskunftspflichten durch ein Landesgesetz nicht eingeschränkt werden können.

Allgemeine Übermittlungsbefugnisse nach den Datenschutzgesetzen reichen hierfür jedoch nicht aus, es muß sich vielmehr immer um ausdrückliche Auskunftspflichten handeln. Eine solche Pflicht besteht insbesondere bei strafrechtlichen Ermittlungen der Staatsanwaltschaft und ihrer Hilfsbeamten nach § 161 Satz 1 StPO. Das heißt, zur Verfolgung von Straftaten dürfen Daten, die im Zusammenhang mit der Notfallrettung und dem Krankentransport anfallen, übermittelt werden. Allerdings sind hier strikt die Zeugnisverweigerungsrechte nach der Strafprozeßordnung zu beachten, die auch für die Besatzungen von Rettungs- und Krankenwagen gelten.

18. Verfassungsschutz

18.1 Stand der Gesetzgebung

Im 9. TB (4.13.19) war die Vorlage eines Entwurfs eines hamburgischen Verfassungsschutzgesetzes angemahnt worden, damit auch das hamburgische Landesamt für Verfassungsschutz seine Arbeit endlich auf einer gesetzlichen Grundlage praktizieren könne, die den verfassungsrechtlichen Vorgaben entspricht.

Während die Mehrzahl der alten Bundesländer inzwischen neugefaßte Gesetze über den Verfassungsschutz besitzt oder zumindest Entwürfe in den parlamentarischen Beratungen sind, liegt in Hamburg bislang nur ein Referentenentwurf vor. Da der Entwurf noch nicht in die Behördenabstimmung gegeben war, konnten wir zum Entwurf noch keine Stellung nehmen.

Die Zeitverzögerung ist um so erstaunlicher, als das Landesamt für Verfassungsschutz bereits im Sommer 1990 mitgeteilt hatte, daß noch im Laufe des Jahres 1990 ein Referentenentwurf in die Behördenabstimmung gehen werde.

Bei Betrachtung des derzeitigen Tempos kann mit einer Verabschiedung eines novellierten Gesetzes, welches das inzwischen völlig unzureichende Gesetz aus dem Jahre 1978 ablösen wird, kaum vor 1993 gerechnet werden.

Damit wäre das Ende des „Übergangsbonus", der den Gesetzgeber zur Korrektur nicht verfassungskonformer Gesetze an die verfassungsrechtlichen Anforderungen eingeräumt ist, endgültig erreicht.

18.2 Eckdaten für eine Novellierung des Hamburgischen Verfassungsschutzgesetzes

Im 8. TB (3.9.1.1) waren die Anforderungen an ein verfassungsrechtlich einwandfreies Gesetz ausführlich dargelegt worden.

Auf dem Hintergrund der neueren Diskussion anläßlich der Novellierung verschiedener Landesverfassungsschutzgesetze und des Bundesverfassungsschutzgesetzes ergeben sich folgende Eckdaten für eine Novellierung:

1. Es bedarf einer abschließenden Definition der Aufgabenfelder am Maßstab der Normenklarheit.

2. Es bedarf einer abschließenden Definition der Befugnisse des Landesamtes für Verfassungsschutz, d.h. insbesondere der zulässigen „nachrichtendienstlichen Mittel". Der Katalog dieser „nachrichtendienstlichen Mittel" sollte möglichst restriktiv gefaßt werden. Auch die Voraussetzungen für den Einsatz „nachrichtendienstlicher Mittel" bedürfen näherer Konkretisierung.

   Insbesondere klargestellt werden müßte, daß im Zusammenhang mit dem Einsatz nachrichtendienstlicher Mittel keine Straftaten begangen werden dürfen (vgl. jetzt § 8 Abs. 3 Satz 1 des schleswig-holsteinischen Verfassungsschutzgesetzes).

3. Es bedarf präziser Regelungen für die zulässige Speicherung, Änderung und Nutzung personenbezogener Daten. Insbesondere muß klargestellt sein, daß Speicherungen nur dann gerechtfertigt sind, wenn in der Person des Betroffenen selbst tatsächliche Anhaltspunkte für den Verdacht von verfassungsfeindlichen Bestrebungen, terroristischen Handlungen oder Spionagetätigkeiten liegen.

4. Es bedarf präziser Regelungen für die Übermittlung zwischen Verfassungsschutz und Sicherheitsbehörden unter Berücksichtigung des Trennungsgebotes. Insbesondere ist eine Einschränkung der Datenflüsse zwischen Polizei und Verfassungsschutz anzustreben. Eine erfreuliche Klarstellung bringt hier § 9 des schleswig-holsteinischen Verfassungsschutzgesetzes: „Polizeiliche Befugnisse stehen der Verfassungsschutzbehörde nicht zu; sie darf die Polizei auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, zu denen sie selbst nicht befugt ist."

5. Ebenfalls gesetzlicher Regelung bedarf die Einsicht in amtliche Register durch das Landesamt für Verfassungsschutz, da es sich hier um eine Zweckänderung der gespeicherten Daten handelt. Hier sind insbesondere zu nennen das Melderegister, das Personalausweis- und das Paßregister. Auf keinen Fall kann die Einrichtung von Online-Anschlüssen in Betracht kommen.

6. Das Auskunftsrecht von Betroffenen gegenüber dem Landesamt für Verfassungsschutz sollte präzisiert und erweitert werden. In diesem Zusammenhang wäre der Vorschlag eines „Datenkonto-Auszugs" überlegenswert, in dem z.B. jährlich entsprechende „Buchungen" aufgelistet und den Auskunftssuchenden zugänglich zu machen wären.

7. Zur zumindest ansatzweisen Kompensation der Eingriffsbefugnisse müßten efektive Instrumente der Kontrolle des Verfassungsschutzes bereitgestellt werden: Die Arbeit des parlamentarischen Kontrollausschusses sollte durch ein „Selbstbefassungsrecht" sowie die Ausdehnung der Kontrollrechte – etwa durch erweiterte Einsichtsrechte – verbessert werden.

Nachzudenken wäre schließlich über die Schaffung eines unabhängigen Beauftragten für den Verfassungsschutz, der – wie in § 27 des schleswig-hol-

steinischen Verfassungsschutzgesetzes vorgesehen – im Einzelfall vom parlamentarischen Kontrollausschuß bestellt werden könnte.

18.3 Automatisierung der Referatsarbeitskartei (RAK)

Das Landesamt für Verfassungsschutz ist derzeit dabei, die bislang manuell geführte Referatsarbeitskartei „Extremismus" zu automatisieren. Zur Klärung der datenschutzrechtlichen Aspekte hat sich das Landesamt an uns gewandt. In der Referatsarbeitskartei werden biographische und sonstige Angaben über Personen aus dem gesamten Arbeitsfeld des Bereichs „Extremismus" zusammengeführt.

Hierzu zählen Personen, deren Bestrebungen gegen die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung von Mitgliedern verfassungsmäßiger Organe des Bundes oder eines Landes zum Ziel haben. Außerdem zählen hierzu Personen einschließlich Ausländer, deren Bestrebungen durch Anwendung von Gewalt auswärtige Belange der Bundesrepublik Deutschland gefährden. Dazu gehören Verdachtsfälle und akute Fälle sowie frühere, noch nicht gelöschte Fälle. Der derzeitige Datenbestand umfaßt Angaben zu etwa 11 000 Personen.

Die Daten werden nach Maßgabe des Erfassungskatalogs für NADIS gespeichert. Im Regelfall werden diese Daten ferner im nachrichtendienstlichen Informationssystem NADIS selbst gespeichert. Im Unterschied zu NADIS dient die Referatsarbeitskartei bereits in ihrer jetzigen konventionellen Form nicht bloß als Nachweissystem, sondern sie enthält auch inhaltliche Angaben über die in Erscheinung getretenen Personen.

Während NADIS ein Verbundsystem ist, an dem das Bundesamt für Verfassungsschutz und die Landesämter angeschlossen sind, ist die Referatsarbeitskartei eine speziell auf Hamburger Daten zugeschnittene Sammlung. Zu Personen, die in der Referatsarbeitskartei mit einigen wesentlichen Angaben gespeichert sind, existiert gelegentlich eine Akte, wenn eine bestimmte Menge an Erkenntnissen über sie vorliegt.

Nach unserem Eindruck stellt die geplante Automatisierung der Referatsarbeitskartei ein Pilotprojekt dar, welches insoweit bundesweit Vorreiterfunktionen wahrnehmen würde. Die Automatisierung soll in Form eines lokalen Netzwerkes konfiguriert werden.

Der Datensatz soll umfassen die biographischen Grunddaten (Name, Anschrift, Geburtsdatum usw.) sowie die Felder Beruf, Familienangehörige, Bankverbindung. Die Erkenntnisdaten sollen jeweils zusätzlich gekoppelt werden mit den Datenfeldern Quelle, taktische Zeit, Aktenzeichen und Zeitpunkt der Eintragung.

Zu jedem gespeicherten Datensatz soll ein „Überwachungsdatum" eingetragen sein, das als Zeitpunkt der Wiedervorlage für die Erforderlichkeitsprüfung einer

weiteren Speicherung genutzt werden soll. Das Überwachungsdatum soll automatisiert auf 4 Jahre seit der letzten Zuspeicherung von Daten zu einer Person festgesetzt werden. Jede erneute Datenspeicherung zu einer Person führt mithin zu einer verlängerten Speicherung der bereits vorhandenen Daten. Die – manuelle – Vergabe kürzerer Fristen soll möglich sein. Die vorgesehene 4-Jahres-Frist korrespondiert mit der Wiedervorlagefrist von 4 Jahren, die im Bereich NADIS praktiziert wird.

Besonders bemerkenswert ist zusätzlich, daß im Datenbestand völlig frei recherchierbar sein soll, also die Suche nach beliebigen, auch kombinierbaren Kriterien möglich sein soll.

Das System soll als Netzwerk gestaltet werden. Dabei soll ein Unix-Server mit Workstations, die unter dem Betriebssystem DOS laufen, verbunden werden. Datenhaltung soll zentral auf dem Unix-Server erfolgen, wobei die Daten – auf Anforderung der Sachbearbeiter – auf die Workstations übertragen werden können, um sie dort weiterverarbeiten oder auch ausdrucken zu können. Um das unkontrollierte Kopieren der Daten oder die Benutzung nichtautorisierter Software zu unterbinden, sollen ausschließlich Workstations ohne bzw. nur mit gesperrten Diskettenlaufwerken eingesetzt werden.

Da vorgesehen ist, die vorhandenen Karteikarten, soweit technisch möglich, über einen Scanner in das System einzulesen, bestünde zum Zeitpunkt des Einlesens nicht die Möglichkeit einer Erforderlichkeitsprüfung bezüglich der bereits jetzt auf den Karteikarten gespeicherten Informationen. Bei einer stichprobenartigen Überprüfung des bisherigen manuellen Systems haben wir uns davon überzeugt, daß zumindest der Bestand an Informationen überzogen erscheint, zumal wenn man bedenkt, daß jede Karteikarte nur eine Kurzzusammenfassung der ohnehin zusätzlich geführten Akte darstellt. Das Landesamt meint, alle zu einer Person gespeicherten Informationen seien notwendig, um den „Werdegang" rekonstruieren zu können.

Im Hinblick auf die geplante Volltextrecherchemöglichkeit im System hatten wir dem Landesamt bereits vorab unsere Bedenken deutlich gemacht und darauf hingewiesen, daß – wenn eine solche Verknüpfung nach verschiedenen Suchkriterien überhaupt praktiziert werden sollte – die Datensicherungsanforderungen des § 8 Abs. 2 Nr. 3 HmbDSG (Speicherkontrolle) die Protokollierung bereits beabsichtigter bzw. durchgeführter Verknüpfungen im Datenbestand verlangen. Es wurde vereinbart, daß entsprechende Protokolldaten monatlich ausgedruckt werden, die Protokolldatei dann gelöscht wird und der Ausdruck der monatlichen Ausdrucke maximal 1 Jahr aufbewahrt werden kann. Damit sind zumindest stichprobenartige interne Kontrollen auf die entsprechenden Verknüpfungsmöglichkeiten genauso gegeben wie die Möglichkeit der externen Kontrolle durch uns.

Eine abschließende datenschutzrechtliche Bewertung läßt sich erst nach Prüfung der vollständigen Unterlagen vornehmen. Diese liegen uns noch nicht vor.

Aus Sicht des Landesamtes für Verfassungsschutz soll der Echtzeitbetrieb im Frühjahr 1992 beginnen.

19. Justiz

19.1 Stand der Gesetzgebung

19.1.1 Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG)

Bereits in der vergangenen Legislaturperiode des Deutschen Bundestages war von seiten einiger Bundesländer über den Bundesrat ein entsprechender Gesetzentwurf eingebracht worden. Unsere Kritik daran ist im 9. TB. (4.14.1.2) wiedergegeben. Mit dem Ende der letzten Legislaturperiode des Bundestages war dieser Entwurf erfreulicherweise der Diskontinuität zum Opfer gefallen.

Im Frühjahr 1991 hat dann der Bundesrat (auf Initiative der Länder Baden-Württemberg und Bayern) erneut einen entsprechenden Entwurf präsentiert, der inzwischen nach Stellungnahme der Bundesregierung in die Beratungen des Deutschen Bundestages eingebracht worden ist.

Der Entwurf wird motiviert mit der „Herausforderung für Staat und Gesellschaft", zu der sich die organisierte Kriminalität entwickelt habe. Sie konzentriere sich auf "... Deliktsbereiche, die hohe kriminelle Gewinne garantieren und bei denen zugleich das Risiko der Entdeckung dadurch vermindert wird, daß es entweder keine unmittelbaren Opfer gibt oder die Opfer nicht bereit sind, Anzeige zu erstatten und vor den Strafverfolgungsbehörden auszusagen" (Entwurf, Seite 1). Durch eine Verbesserung des Ermittlungsinstrumentariums solle den Strafverfolgungsbehörden ermöglicht werden, „in den Kernbereich der kriminellen Organisationen einzudringen" (Entwurf, Seite 1). Der Entwurf dokumentiert folgerichtig eine vorwiegend präventive Stoßrichtung.

Diese Zielrichtung verändert auch den Stellenwert des Ermittlungsverfahrens gegen den einzelnen Tatverdächtigen grundlegend. Nicht mehr die Aufklärung und Ahndung einzelner Straftaten steht im Vordergrund, sondern die „Zerschlagung" der Strukturen der organisierten Kriminalität, deren Abgrenzung zur sonstigen Kriminalität im übrigen nicht klar geregelt wird.

Die datenschutzrechtlich relevanten Inhalte des Gesetzentwurfs sind folgende:

— gesetzliche Regelung des Einsatzes verdeckter Ermittler,

— gesetzliche Regelung des Einsatzes akustischer und optischer Überwachungsgeräte innerhalb und außerhalb von Wohnungen,

— gesetzliche Regelungen über die Rasterfahndung und die polizeiliche Beobachtung,

— polizeiliche Überwachung und Aufzeichnung des Fernmeldeverkehrs zu Zwecken der Gefahrenabwehr.

Die geplanten Maßnahmen werden im Fall ihrer Realisierung schwerwiegende Eingriffe in die Bürgerrechte darstellen.

Erhebliche Bedenken bestehen dagegen, daß Eingriffe in die Privatsphäre durch den Einsatz von Peilsendern, Richtmikrophonen und Wanzen schon möglich sein sollen, wenn die Strafverfolgungsbehörden „Straftaten von erheblicher Bedeutung" für gegeben erachten.

Mit diesem schwammigen Begriff wird der Einsatz solcher geheimer Ermittlungsmethoden weit über den Bereich der organisierten Kriminalität hinaus ausgedehnt. Diese Mittel werden dann nämlich für alle Fälle außerhalb der Bagatell- und Kleinkriminalität verfügbar. Es ist ebenfalls nicht hinnehmbar, daß so schwerwiegende Eingriffe wie der Einsatz verdeckter Ermittler nicht grundsätzlich vom Richter angeordnet werden müssen, sondern weitgehende Eilkompetenzen für Polizei und Staatsanwaltschaft vorgesehen werden. Nach dem Gesetzentwurf ist für die Bürger nicht mehr einschätzbar, ob geheime Ermittlungsmethoden auch gegen sie eingesetzt werden.

Auch über völlig unbeteiligte Personen sollen heimlich Bild- und Filmaufnahmen hergestellt werden können, wenn es „der Erforschung des Sachverhalts" oder der „Aufenthaltsermittlung des Täters" dient. Gegen unverdächtige Personen sollen Wanzen und Peilsender eingesetzt werden können, wenn eine „Verbindung" mit dem Täter vermutet wird. Das nichtöffentliche, im Beisein eines verdeckten Ermittlers gesprochene Wort des Verdächtigen, evtl. Begleitpersonen und zufällig mitbetroffener Dritter soll heimlich abgehört und aufgezeichnet werden können. Die Verwendung der Informationen, die durch den Einsatz geheimer Ermittlungsmethoden gewonnen werden, wird in besorgniserregendem Umfang für andere Zwecke zugelassen.

Offen bleibt insbesondere, ob die gewonnenen Erkenntnisse der Polizei für eine jahrelange Speicherung zur „vorbeugenden Straftatenbekämpfung" überlassen werden dürfen. Dies sieht der Gesetzentwurf nicht nur für Tatverdächtige, sondern sogar für andere Personen wie Begleiter oder zufällig betroffene Dritte vor. Besonders bedenklich erscheint die vorgesehene Ausweitung der Telefonüberwachung, die erstmals schon ohne Vorliegen eines konkreten Tatverdachts möglich sein soll.

Sollte der Gesetzentwurf geltendes Recht werden, so würde für die Bekämpfung der organisierten Kriminalität ein hoher Preis zu zahlen sein: Der polizeiliche Handlungsspielraum würde gegenüber der derzeitigen Rechtslage weit in das Vorfeld strafrechtlich relevanter Handlungen ausgedehnt werden mit der Folge, daß persönlichste Lebensverhältnisse einer Vielzahl unbeteiligter Personen Gegenstand staatlicher Kontrolle werden könnten.

Ein weiterer bedeutsamer Effekt des vorgesehenen Einsatzes verdeckter Ermittlungsmethoden könnte aber auch darin liegen, daß sich die bisherige Rollenverteilung zwischen Exekutive und Gerichten grundlegend verändert. War bislang die Sperrung von Beweismitteln nur unter engen Voraussetzungen

(des § 96 StPO) zugelassen, so sehen § 101 Abs. 1 und 4 StPO (Art. 4 Nr. 7 des Entwurfs) und § 110 d Abs. 2 StPO (Art. 4 Nr. 8 des Entwurfs) vor, daß „Entscheidungen und sonstige Unterlagen" über den verdeckten Einsatz technischer Mittel und den verdeckten Ermittler grundsätzlich bei der Staatsanwaltschaft verwahrt werden sollen. Zu diesen Entscheidungen gehört auch beispielsweise die Anordnung einer Abhörmaßnahme in der Wohnung des Betroffenen gemäß § 100 b Abs. 1 StPO.

Nach der Intention des Gesetzentwurfs werden solche Maßnahmen erst dann dem Beschuldigten und dem später zur Entscheidung in der Hauptverhandlung berufenen Gericht offenbart werden, wenn die „öffentliche Sicherheit" oder die weitere Verwendung eines verdeckten Ermittlers nicht mehr gefährdet ist. Angesichts der Tatsache, daß die Verwendung eines verdeckten Ermittlers in der Regel auf Dauer konzipiert ist, ist also davon auszugehen, daß entsprechende Entscheidungen nie oder nur sehr selten offenbart werden. Welche Akten das Gericht erhält und welche Dossiers ihm vorenthalten werden, entscheidet künftig also die von polizeilichen Präventionsstrategien geleitete Exekutive.

19.1.2 Gesetzgebungsvorhaben zum Schuldnerverzeichnis

Im 9. TB (4.14.1.4) war der an sich erfreuliche Ansatz, die Vorschriften über Auskünfte aus dem Schuldnerverzeichnis im Hinblick auf das informationelle Selbstbestimmungsrecht neu zu regeln, ausdrücklich begrüßt worden. Zugleich waren die erheblichen Schwachstellen des Gesetzentwurfs dargestellt worden, die auch vom Bundesrat und vom Bundesbeauftragten für den Datenschutz kritisiert worden waren.

Der Gesetzentwurf wurde in der vergangenen Legislaturperiode nicht mehr verabschiedet. Er wurde inzwischen von der Bundesregierung in unveränderter Form erneut eingebracht (BT-Drucks. 12/193). Der Bundesrat hat am 1. März 1991 seine frühere Stellungnahme zu den Mängeln des Gesetzes bestätigt. Auch der Bundesbeauftragte für den Datenschutz hält an seiner in der letzten Legislaturperiode geäußerten Auffassung fest.

Trotz des fortgeschrittenen Standes des Gesetzgebungsverfahrens halten wir es für möglich und erforderlich, durch entsprechende Stellungnahmen auf den Fortgang des Verfahrens Einfluß zu nehmen (zu privaten bundesweiten Schuldnerverzeichnissen vgl. 27.).

19.1.3 Noch kein Justizmitteilungsgesetz

Seit Jahren wird von den Datenschutzbeauftragten bemängelt, daß die Übermittlung personenbezogener Daten aus den Verfahren der Zivil- und Strafgerichtsbarkeit nicht gesetzlich legitimiert ist, sondern auf der Grundlage einfacher Verwaltungsvorschriften erfolgt, obwohl solche Mitteilungen schwerwiegende Folgen für die Betroffenen haben können.

Von daher ist zu begrüßen, daß der Bundesjustizminister nun einen überarbeiteten Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz, Stand 23. August 1991) vorgelegt hat.

Allerdings berücksichtigt der Entwurf noch immer nicht wesentliche datenschutzrechtliche Kritikpunkte der früheren Diskussionen:

1. Nach wie vor wird am Konzept der „Zwei-Stufigkeit" festgehalten, d.h. es sollen Regelungen einerseits im Gesetz (speziell im Einführungsgesetz zum Gerichtsverfassungsgesetz) und Regelungen in Verwaltungsvorschriften nebeneinander bestehen. Die Grundsätze der Normenklarheit und des Gesetzesvorbehalts verlangen aber vorrangig eine eingehende gesetzliche Regelung.
2. Es fehlen noch immer konkrete Angaben zu den Empfängern von Übermittlungen.
3. Die Übermittlungsbefugnisse für Gerichte und Staatsanwaltschaften sind zu weit gefaßt; § 13 (des Gesetzentwurfs) läßt die Übermittlung nicht nur dann zu, wenn die Einwilligung des Betroffenen vorliegt oder eine besondere Rechtsvorschrift dies vorsieht (insoweit mit § 5 HmbDSG deckungsgleich), sondern auch in einer Reihe von weiteren Fällen. Dies führt dazu, daß die Einwilligung des Betroffenen geradezu zur Ausnahme wird.
4. Auch die Regelung zur Übermittlung personenbezogener Daten der Beschuldigten in Strafsachen (§ 14) stößt jedenfalls da auf Bedenken, wo sie für dienstrechtliche Maßnahmen und/oder arbeitsrechtliche Maßnahmen zugelassen wird.

   Es sollte klargestellt werden, daß nur dann Mitteilungen erfolgen dürfen, wenn das für den Betroffenen geltende Dienst-, Arbeits- oder Berufsrecht eine Speicherung der Informationen in der Personalakte zuläßt und an festgestellte Verfehlungen Rechtsfolgen knüpft.

   Steht die Straftat des Betroffenen nicht in unmittelbarem Zusammenhang mit seinen dienstlichen Aufgaben, sollte eine Datenübermittlung nur im Fall erheblicher Rechtsverletzungen zulässig sein. Unter dem Gesichtspunkt der Normenklarheit wäre die Aufnahme eines Straftatenkatalogs hilfreich.

   Bezüglich des Zeitpunkts der Übermittlungen sollte klargestellt werden, daß sie jedenfalls nicht vor Erhebung der öffentlichen Klage erfolgen dürfen.
5. Über die ohnehin schon weitreichenden Übermittlungsbefugnisse hinaus erklärt § 17 Nr. 2 die Übermittlung auch dann für zulässig, wenn sie „zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit" erforderlich sei. Mit Hilfe dieser Generalklausel könnte die im Gesetzentwurf teilweise, wenn auch unzureichend eingeschränkte Übermittlungsbefugnis konterkariert werden.

6. Grundsätzlich sollte die Übermittlung in Form einer „Auskunftserteilung" an die empfangenen Stellen erfolgen. Nur soweit es unerläßlich ist, sollte die Übermittlung durch Übersendung der Akte oder von Unterlagen erfolgen (§ 18 Abs. 3).

7. Statt der in § 21 vorgesehenen gleichzeitigen Unterrichtung der Betroffenen mit der Übermittlung sollte die Unterrichtung grundsätzlich vor der Übermittlung erfolgen, um den Betroffenen Gelegenheit zu geben, ihre schutzwürdigen Belange geltend zu machen.

8. Bedenken bestehen schließlich gegen die vorgesehene Regelung, die Pflicht zur Unterrichtung über Datenübermittlungen an die Betroffenen in bestimmten Fällen entfallen zu lassen (§ 21 Abs. 2). Eine solche Ausnahme von der Unterrichtungspflicht sollte auf schwerwiegende Fälle beschränkt sein. Dafür bietet § 21 Abs. 5 jedoch bereits ausreichende Regelungen an. Wenn eine Unterrichtung des Betroffenen unterbleibt, müßte der Betroffene darauf hingewiesen werden, daß er sich an den zuständigen Datenschutzbeauftragten wenden kann (§ 21 Abs. 6).

9. Der Entwurf sollte ergänzt werden durch Bestimmungen, die festlegen, wann die übermittelten Daten zu löschen sind. Anderenfalls bestünde die Gefahr, daß die Speicherfristen nach dem Bundeszentralregistergesetz umgangen werden könnten.

19.2 Kontrollzuständigkeit des Datenschutzbeauftragten bei den Gerichten

Im Jahre 1988 hatten sich bei der Überprüfung der Datenverarbeitung beim Verwaltungsgericht erhebliche Mängel ergeben (7. TB, 4.13.2.2). Bei dieser Überprüfung waren vom Verwaltungsgericht Zweifel an der Kontrollzuständigkeit des Hamburgischen Datenschutzbeauftragten geäußert worden, weil es im damals geltenden § 20 Abs. 1 HmbDSG hieß, daß die Gerichte der Datenschutzkontrolle nur unterliegen, soweit sie in Verwaltungsangelegenheiten tätig werden. Im inzwischen novellierten Hamburgischen Datenschutzgesetz vom 5. Juli 1990 ist die entsprechende Regelung im § 23 Abs. 1 Satz 2 enthalten.

Die Justizbehörde war der Auffassung des Verwaltungsgerichts beigetreten. Nachdem im 8. TB (3.10.2) die Problematik erneut dargestellt worden war, hat die Bürgerschaft auf der Grundlage der Stellungnahme des Senats zum 8. TB das Problem erörtert und in ihrer Mitteilung vom 13./14. März 1991 an den Senat das Ersuchen gerichtet

„— im Rahmen der verfassungsrechtlichen Möglichkeiten eine Datenschutzkontrolle bei den Gerichten sicherzustellen,

— möglichst im Einvernehmen mit dem Hamburgischen Datenschutzbeauftragten Regelungen zu entwickeln, die die offene Frage der Kontrollbefugnis des Hamburgischen Datenschutzbeauftragten bei den Gerichten, insbesondere bei den Geschäftsstellen klären,

— der Bürgerschaft hierüber baldmöglichst zu berichten."

Leider ist es noch nicht gelungen, ein entsprechendes Einvernehmen herzustellen, da die Justizbehörde bisher nicht zu einer abschließenden Regelung bzw. einem entsprechenden Vorschlag gekommen ist.

Von meiner Seite war angeregt worden, zur Klärung der Frage eine Auflistung der gerichtlichen Tätigkeiten nach Verwaltungsangelegenheiten einerseits und spruchrichterlichen Tätigkeiten andererseits vorzunehmen. Mit einbezogen werden soll auch die Tätigkeit der Gerichtsvollzieher (vgl. 8. TB, 3.10.5). In der Zwischenzeit hat die Justizbehörde damit begonnen, eine entsprechende Auflistung durch Erhebungen bei den verschiedenen Gerichtszweigen vorzubereiten.

Wir haben zur Unterstützung verschiedene Unterlagen beigesteuert, insbesondere einschlägige Teile aus den Analysen zur Organsiation der Verwaltungsgerichte und zur Organisation der Amtsgerichte, die im Rahmen des Forschungsprojekts „Strukturanalyse der Rechtspflege" erstellt worden sind.

Unabhängig von der noch ausstehenden Klärung der Frage des Umfangs der Kontrollzuständigkeit bei den Gerichten haben wir die Justizbehörde auf die Regelung in § 24 Abs. 2 des Berliner Datenschutzgesetzes hingewiesen, in der es heißt: „Setzen Gerichte zur Erfüllung ihrer gesetzlichen Aufgaben automatische Datenverarbeitungsanlagen ein, so unterliegt unbeschadet der richterlichen Unabhängigkeit die Ordnungsmäßigkeit und Rechtmäßigkeit der Verfahren der Kontrolle des Datenschutzbeauftragten."

Im Rahmen einer voraussichtlich im Jahr 1992 anstehenden Novellierung des Hamburgischen Datenschutzgesetzes würde es sich anbieten, eine entsprechende Regelung in das hamburgische Gesetz aufzunehmen.

20. Strafvollzug

20.1 Stand der Gesetzgebung

Der dringende Bedarf an datenschutzrechtlichen Ergänzungen des Strafvollzugsgesetzes (vgl. 9. TB, 4.15.1) hat sich während des Berichtszeitraums in einem Referentenentwurf eines 4. Gesetzes zur Änderung des Strafvollzugsgesetzes (Stand: 25. März 1991) niedergeschlagen.

Er enthält wichtige Ergänzungen, und zwar

1. zur Besuchsregelung (§ 24),
2. zur Überwachung des Schriftverkehrs (§ 29) und
3. zur Handhabung erkennungsdienstlicher Maßnahmen (§ 86).

1. Aus Gründen der Anstaltssicherheit soll ein Besuch auch davon abhängig gemacht werden können, daß der Besucher der Einholung von Auskünften

über ihn bei anderen Behörden zustimmt. Problematisch wäre die vorgesehene Regelung dann, wenn allein wegen der Nichtzustimmung des Besuchers der Besuch verweigert werden könnte. Statt dessen sollte ein Erkenntnisdefizit, das eventuell durch die Verweigerung der Zustimmung entsteht, nur ein Kriterium unter verschiedenen für die Entscheidung über die Zulässigkeit des Besuchs sein.

2. Von der Überwachung des Schriftverkehrs sollen über die bisherige Regelung hinaus (§ 29 Abs. 2) „Schreiben an die Datenschutzbeauftragten des Bundes und der Länder" ausgenommen sein. Diese Regelung ist zu begrüßen.

   Ergänzungsbedürftig ist die Regelung in § 29 Abs. 3, derzufolge der übrige Schriftwechsel überwacht werden darf. Es sollte klargestellt werden, daß die Überwachung des Schriftverkehrs jeweils auf die konkrete Person des Strafgefangenen hin geprüft werden muß und eine Entscheidung, die nur auf die gesamte Anstalt und ihre Insassen abstellt, nicht ausreichend ist.

3. Die vorgesehene Regelung über die zulässige Handhabung erkennungsdienstlicher Maßnahmen läßt eine Regelung über Löschung bzw. Vernichtung der entsprechenden Unterlagen vermissen. Hier ist zu fordern, daß solche Maßnahmen, auch wenn sie zulässig gewesen sind, spätestens bei Abschluß der Strafvollstreckung zu vernichten sind. Darüber hinaus wäre zu prüfen, ob und unter welchen Voraussetzungen Personen, die eine Ersatzfreiheits- oder eine Kurzstrafe verbüßen, überhaupt erkennungsdienstlich behandelt werden müssen.

Wichtige Neuregelungen sind unter der Überschrift „Datenschutz" in den §§ 127 bis 128 f des Entwurfs enthalten. Hier sind insbesondere hervorzuheben

1. die Regelung über die Datenerhebung (§ 127),
2. Verarbeitung und Nutzung (§ 128),
3. Schutz besonderer Informationen (§ 128 b),
4. Aufbewahrungsfristen (§ 128 c Abs. 3).

1. Bedenken bestehen dagegen, daß Daten über Personen, die Nichtgefangene sind, auch ohne ihre Mitwirkung bei Personen oder Stellen außerhalb der Anstalt erhoben werden dürfen, wenn dies für die Sicherheit in der Anstalt unerläßlich sein soll. Statt dessen sollte enumerativ aufgeführt werden, unter welchen Voraussetzungen die Datenerhebung zulässig ist. Ebenfalls sollte konkret und abschließend geregelt werden, welche Auskünfte die Justizvollzugsanstalt bei welchen Stellen einholen darf.

2. Bedenken richten sich auch gegen die Regelung in § 128 des Entwurfs, der die weitere Verarbeitung und Nutzung personenbezogener Daten zu regeln beansprucht. Insbesondere sollte hier eine spezielle Regelung über die Führung der Gefangenenpersonalakte getroffen werden. Hier wäre festzulegen, welchen Inhalt diese Akte haben kann und wie sie geführt werden muß. Dabei wäre anzustreben, daß die Gefangenenpersonalakte aufgespalten wird in unterschiedliche Teilakten, um zu verhindern, daß für jede Bearbeitung die gesamte Akte herangezogen werden muß.

   Schließlich bestehen Bedenken auch gegen die Regelung (§ 128 Abs. 4), nach der Daten von Personen, die Nichtgefangene sind, zur Abwehr jeder unmittelbar drohenden Gefahr für die öffentliche Sicherheit genutzt werden können. Aufgrund dieser Bestimmung würde die Weitergabe von Daten über Personen, die selbst nicht Gefangene sind, schon bei Anhaltspunkten für Verletzungen jeglicher öffentlich-rechtlicher Normen erlaubt sein, obwohl es sich hierbei nicht einmal um Ordnungswidrigkeiten handeln muß.

   Schließlich sollte verlangt werden, daß Auskünfte über Gefangene nur auf schriftliche Anfrage hin erteilt werden (§ 128 Abs. 5 des Entwurfs). Damit wäre die Identitätsfeststellung des Anfragenden einigermaßen präzise feststellbar. Statt der vorgesehenen nachträglichen Mitteilung über die Information an Dritte sollten die Gefangenen vor Erteilung der Auskunft gehört werden.

   Bedenken bestehen auch gegen die in § 128 Abs. 6 vorgesehene Weitergabe der Gefangenenpersonalakte im Normalfall an andere Vollzugsbehörden oder an andere öffentliche Stellen. Im Interesse des Persönlichkeitsschutzes der Gefangenen muß darauf verzichtet werden, die Personalakte zu übersenden. Statt dessen sollte die Datenübermittlung, soweit sie denn erforderlich ist, primär in Form der Auskunft zum jeweils konkreten Thema gehandhabt werden.

3. Ebenfalls Bedenken bestehen gegen die in § 128 b Abs. 2 vorgesehene Regelung, derzufolge der Anstaltsarzt „für die in diesem Gesetz geregelten Aufgaben der Vollzugsbehörde oder zur Abwehr gegenwärtiger Gefahren für Leib oder Leben" von der ärztlichen Schweigepflicht gegenüber dem Anstaltsleiter entbunden ist. Eine Befugnis zur Durchbrechung der ärztlichen Schweigepflicht sollte nur bei erheblichen Gefahren in Betracht kommen und im Gesetz konkret und abschließend aufgezählt werden. Besonders hoch sollte die Schwelle für die Durchbrechung der ärztlichen Schweigepflicht da angesetzt werden, wo lediglich eine Gefahr für den Gefangenen selbst besteht. In diesem Fall sollte es in der Regel dem Gefangenen selbst überlassen bleiben, ob er besondere Hilfe wünscht.

4. Erhebliche Bedenken bestehen gegen die vorgesehenen Aufbewahrungsfristen von 30 Jahren im Fall der Personalakten, Gesundheitsakten und Krankenblätter sowie von 50 Jahren im Fall der Gefangenenbücher (§ 128 c Abs. 3). Hier sind erheblich kürzere Fristen angebracht, bei denen nach der Länge der Strafen differenziert wird.

Wenngleich zusammenfassend zu begrüßen ist, daß mit dem Referentenentwurf der Versuch gemacht wird, die datenschutzrechtlich defizitäre Situation im Bereich des Strafvollzuges den Anforderungen des Grundrechts auf informationelle Selbstbestimmung entsprechend neu zu strukturieren, weist dieser Versuch deutliche Mängel auf, die im Gesetzgebungsverfahren noch korrigiert werden sollten. Das von einer Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder ausgearbeitete Grundsatzpapier zu Fragen des Datenschutzes im Strafvollzug könnte hier als Material zur weiteren Bearbeitung genutzt werden.

20.2 Überwachung des Schriftverkehrs

In Anstalten besonderen Sicherheitsgrades, z.B. in der Justizvollzugsanstalt Fuhlsbüttel (II), wird bislang eine generelle Postüberwachung in Form einer Inhaltskontrolle praktiziert. Ausgenommen von dieser Überwachung sind lediglich die in § 29 Abs. 1 und Abs. 2 des Strafvollzugsgesetzes genannten Institutionen sowie darüber hinaus der Schriftwechsel mit dem Hamburgischen Datenschutzbeauftragten. Das Strafvollzugsamt stützt seine Auffassung auf einen Beschluß des Hanseatischen Oberlandesgerichts vom 7. Januar 1991, in dem diese Praxis für rechtens erklärt wurde.

Gleichwohl bestehen gegen diese Praxis erhebliche Bedenken: Gemessen an den Anforderungen des Grundrechts nach Art. 10 GG (Brief-, Post- und Fernmeldegeheimnis) und des aus den Grundrechten nach Art. 1 Abs. 1 und 2 Abs. 1 GG abgeleiteten Rechts auf informationelle Selbstbestimmung wird der undifferenzierte Schluß von der Sicherheitslage in einer Anstalt auf die Befugnis zur Einschränkung der Grundrechte einzelner Strafgefangener dem Individualcharakter der einschlägigen Grundrechte nicht genügend gerecht.

In diesem Sinne haben wir im Rahmen der Stellungnahme zum Referentenentwurf eines 4. Gesetzes zur Änderung des Strafvollzugsgesetzes eine Ergänzung des § 29 Abs. 3 vorgeschlagen, derzufolge es bezüglich der Briefkontrolle einer Entscheidung im Einzelfall bedarf. Mit dieser Ergänzung würde der Streit über die Frage ausgeräumt werden können, ob die Überwachung, bezogen auf die jeweilige Anstalt, alle Gefangenen umfassen kann oder jeweils von der konkreten Person des Gefangenen abhängig zu machen ist.

Unsere Auffassung ist aber auch durch Informationen anläßlich eines Besuches in der Justizvollzugsanstalt Fuhlsbüttel (II) gestärkt worden. Dort werden seit längerem auf Grund einer neueren Belegungspraxis auch Strafgefangene aufgenommen, die nur Kurzstrafen bis zu 2 Jahren verbüßen. Der prozentuale Anteil dieser Kurzzeitgefangenen fällt mit 10 bis 20 % im Verhältnis zu den übrigen Gefangenen nicht unerheblich ins Gewicht. Von einer generellen Schriftverkehrsüberwachung sind auch diese Strafgefangenen betroffen. Zumindest für diesen Personenkreis stellt eine generelle Schriftverkehrsüberwachung sich als unverhältnismäßig dar und müßte durch Einzelfallentscheidungen ersetzt werden.

Es kommt ein weiteres hinzu: Angesichts der Tatsache, daß diese Strafvollzugsanstalt mittlerweile großzügig mit Telefonzellen ausgestattet wurde, die es den Gefangenen ermöglicht, unbeschränkt und ohne Überwachung zu telefonieren und dadurch unbegrenzt Informationen nach außen gelangen zu lassen, erscheint die bisher praktizierte generelle Schriftverkehrsüberwachung ohnehin fragwürdig. Aus diesen Gründen wird im Bereich der Postüberwachung nur noch eine Sichtkontrolle, jedoch keine Inhaltskontrolle mehr angemessen zu sein.

21. Gesundheitswesen

21.1 Datenschutz im Krankenhaus

21.1.1 Prüfung im AK Altona

Ob der Umgang mit Patientendaten in hamburgischen Krankenhäusern entsprechend den datenschutzrechtlichen Vorgaben und unter Beachtung der ärztlichen Schweigepflicht sowie einschlägiger Dienstanweisungen erfolgt, kann immer nur stichprobenartig überprüft werden. Im Berichtsjahr fiel die Wahl auf das AK Altona, das mit über 20.000 stationär behandelten Patienten eines der größten Krankenhäuser des Landesbetriebs ist. Gegenstand der datenschutzrechtlichen Prüfung war die Verwaltung der Krankengeschichten im Archiv und die dezentrale Verarbeitung von Patientendaten in Einzelplatzsystemen und Lokalen Netzen.

Bei der Prüfung der Krankengeschichtenverwaltung wurde festgestellt, daß im Krankengeschichtenarchiv die Krankenakten und die Röntgenbilder nach Aufenthaltsjahr, Geburtsdatum und Anfangsbuchstaben des Nachnamens geordnet aufbewahrt werden. Nach 3 Jahren werden die Krankenakten vollständig mikroverfilmt und anschließend vernichtet.

Die Prüfung des Archivs ergab, daß das Hinzuziehen neuer und das Anlegen bereits vorhandener Krankenakten anders gehandhabt wird, als dies die Dienstanweisung des Landesbetriebs Krankenhäuser über die Führung und Herausgabe von Krankenakten und Röntgenbildern in der Fassung vom 3. November 1987 vorschreibt. Diese Dienstanweisung, die seinerzeit mit dem Hamburgischen Datenschutzbeauftragten abgestimmt wurde, schreibt zur Sicherstellung des Patientendatenschutzes vor, daß bei jeder Aufnahme eines Patienten ein Blatt mit seinen persönlichen Daten anzufertigen und seine schriftliche Einwilligung zur Beiziehung eventuell schon vorhandener Krankenakten einzuholen ist. Im Archiv ist dann unverzüglich eine Akte anzulegen bzw. bei Einwilligung des Patienten eine vorhandene Krankenakte wie eine neu angelegte Krankenakte weiterzuführen.

Diese Regelung, die zur Wahrung des informationellen Selbstbestimmungsrechts eine schriftliche Einwilligung des Patienten in die Beiziehung bereits vorhandener Daten festlegt, wird im AK Altona nicht eingehalten. Vielmehr werden

die Krankenakten von der behandelnden Station angelegt, die auch bereits bestehende Krankenakten im Archiv anfordert. Durch dieses Verfahren ist nicht sichergestellt, das dem Patienten sein Selbstbestimmungsrecht hinsichtlich der Hinzuziehung bereits vorhandener Daten bewußt gemacht wird.

Bei Erstaufnahmen erhält das Archiv erstmals bei Entlassung des Patienten durch Übersendung einer Karteikarte Kenntnis vom Aufenthalt dieses Patienten. Die Krankenakte gelangt erst nach Abfassung und Versendung des Arztbriefes an das Archiv. Eine Terminüberwachung über die Verweildauer von Akten auf der Station zwischen Entlassung und Arztbriefschreiben wird nicht vorgenommen.

Eine ordnungsgemäße Archivierung der Krankenunterlagen innerhalb der dafür vorgeschriebenen Fristen wäre aber im Interesse des Datenschutzes und der Einhaltung der ärztlichen Schweigepflicht erforderlich. Die Aufbewahrung der Krankenakten auf der Station nach Abschluß der Behandlung ist nur in engem Rahmen bis zur Abfassung des Arztbriefes zulässig. Hierfür schreibt die Dienstanweisung eine Frist von 6 Wochen vor. Organisatorisch ist das AK Altona zu einer Terminüberwachung über die Verweildauer der Akten auf der Station nach seiner eigenen Stellungnahme derzeit nicht in der Lage. Voraussetzung wäre der Anschluß des Krankengeschichtenarchivs an die Patientendatenverwaltung, so daß 6 Wochen nach Entlassung des Patienten nicht vorhandene Krankenakten bei der Station angemahnt werden könnten.

Die Prüfung der dezentralen Datenverarbeitung bezog sich ausschließlich auf Systeme, die in krankenhauseigener Verantwortung abgewickelt werden: Dies sind Einzelplatz-PC als auch ein Lokales Netz, das hauptsächlich in den einzelnen Stationen zum Schreiben von Arztbriefen genutzt wird. Bei der Prüfung wurde das Sicherungskonzept des HmbDSB für Einzelplatz-PC (9. TB, 3.2) und Lokale Netze (3.5) als Grundlage herangezogen.

Neben Regelungsdefiziten war bei der Prüfung der dezentralen Systeme insbesondere mangelnde Datensicherheit zu beobachten. Zum einen entspricht die Sicherheit der Einzelplatzsysteme nicht dem von uns geforderten Standard: So ist beispielsweise nicht durchgängig für sämtliche im Einsatz befindlichen Geräte ein sogenannter Boot-Schutz realisiert. Dies liegt nicht zuletzt daran, daß die vom AK Altona selbst entwickelte Sicherungssoftware auf herstellerspezifischen Besonderheiten aufbaut, die nur für wenige PC-Hersteller gilt. Diese Besonderheit birgt zusätzlich die Gefahr, daß das Sicherungskonzept möglicherweise bereits bei geringfügigen Hardwareveränderungen untauglich werden kann. Zum anderen sind beim Lokalen Netz u.a. unzureichende Kontrollen des Netzverwalters aufgrund fehlender Protokollierung, unzureichende Trennung von lokaler und Netzanwendung sowie die fehlende Möglichkeit, den Anschluß netzfremder PC zu erkennen, bemängelt worden.

Aufgrund der Sicherheitsmängel haben wir das AK Altona aufgefordert, das bei Einzelplatz-PC eingesetzte Sicherungssystem durch ein herstellerunabhängiges und zugleich umfassenderes Konzept zu ersetzen und den Sicherheitsstandard des Lokalen Netzes durch zusätzliche Sicherungsmaßnahmen zu verbessern.

Bei der Prüfung der dezentralen Datenverarbeitung im AK Altona wurde festgestellt, daß für die automatisierte Datenverarbeitung im Krankenhaus immer noch eine Dienstanweisung des Landesbetriebs Krankenhäuser fehlt. Die Behörde für Arbeit, Gesundheit und Soziales wurde deshalb nochmals aufgefordert, in ihrem Verantwortungsbereich die automatisierte Verarbeitung von Patientendaten allgemeinverbindlich zu regeln und umgehend Vorschriften über die Zulässigkeit der Datenverarbeitung, über Zuständigkeiten, Zugriffsbefugnisse und anzuwendende Datensicherungsmaßnahmen zu erlassen. Inzwischen liegt uns ein erster Entwurf des Landesbetriebs für ein Verfahren zur datenschutzgerechten Gestaltung von IuK-Vorhaben in den Krankenhäusern vor.

21.1.2 Dienstanweisung Universitäts-Krankenhaus Eppendorf

Bei der stichprobenartigen Prüfung der Patientendatenverarbeitung im Universitäts-Krankenhaus Eppendorf im Jahre 1989, die im 8. TB (3.13) ausführlich behandelt wurde, hatte sich unter anderem ein Mangel an verbindlichen Regelungen für den Umgang mit Patientendaten herausgestellt. Zwar gab es eine alte Dienstanweisung über die Führung und Herausgabe von Krankengeschichten aus dem Jahre 1973, die aber nicht mehr dem geltenden Recht entsprach und deshalb dringend überarbeitet werden mußte. Für die automatisierte Verarbeitung von Patientendaten auf Personalcomputern und anderen dezentralen Datenverarbeitungsanlagen gab es überhaupt keine auf die Verhältnisse des Universitäts-Krankenhauses zugeschnittene Regelung, obwohl diese Geräte von einzelnen Ärzten und Fachabteilungen zunehmend zur Unterstützung der Behandlung und für Forschungszwecke eingesetzt wurden.

Nach mehreren Abstimmungsrunden und häufigen Mahnungen wegen des langwierigen Verfahrens ist im Juli 1991 eine Dienstanweisung für das Universitäts-Krankenhaus Eppendorf in Kraft gesetzt worden, die aus datenschutzrechtlicher Sicht die Verarbeitung von Patientendaten umfassend und zufriedenstellend regelt. Im ersten Teil der Dienstanweisung über die Führung und Herausgabe von Krankenunterlagen und Röntgenbildern werden Verantwortlichkeiten und Zugriffsbefugnisse festgelegt, die Auskunfterteilung, Einsichtnahme und Überlassung von Krankenunterlagen an Patienten sowie an andere Personen und Institutionen geregelt, ferner Aufbewahrungsfristen und die geordnete Vernichtung von Krankenunterlagen vorgeschrieben.

Der zweite Teil über den Patientendatenschutz konkretisiert insbesondere die Regelungen des Hamburgischen Krankenhausgesetzes, das inzwischen in Kraft getreten ist. Von besonderer Bedeutung sind hier für das Universitäts-Krankenhaus die rechtlichen Grundlagen für die Nutzung von Patientendaten zu Forschungszwecken.

Der dritte Teil der Dienstanweisung enthält Regelungen für den Einsatz dezentraler Kleinrechner im Universitäts-Krankenhaus. In Anbetracht der besonderen Schutzbedürftigkeit von personenbezogenen Patientendaten sind hohe Anforderungen zu stellen, um eine unberechtigte Kenntnisnahme und eine mißbräuchliche Verwendung mit größtmöglicher Sicherheit auszuschließen. Dazu gehören nicht nur Forderungen nach einer ausreichenden räumlichen Sicherung der Anlagen, sondern auch nach Einsatz von Sicherungsprogrammen, die einen Paßwortschutz und eine Verschlüsselung der Daten gewährleisten.

Wir werden die Datenverarbeitung im Universitäts-Krankenhaus Eppendorf im Auge behalten und zur gegebenen Zeit überprüfen, ob die Dienstanweisung im täglichen Umgang mit Patientendaten umgesetzt und so das Geheimhaltungsinteresse der Patienten beachtet wird.

21.2 Forderungen aus der Prüfung des Bernhard-Nocht-Instituts

Über die datenschutzrechtliche Prüfung des Bernhard-Nocht-Instituts, eines Forschungsinstituts der Behörde für Arbeit, Gesundheit und Soziales mit angeschlossener klinischer Abteilung, wurde im 9. TB (4.16.3) berichtet.

Die Umsetzung der Verbesserungsvorschläge zur Sicherstellung des Patientendatenschutzes ist noch nicht abgeschlossen, vor allem im Bereich des technischen Datenschutzes haben bis vor kurzem noch Probleme bestanden. So war die für das Institut zuständige Fachbehörde lange Zeit der Meinung, daß die auf den PC installierten Sicherungsmaßnahmen auch ohne die von uns geforderte Datenverschlüsselung ausreichend seien. Bei einem PC sollte mit der Umsetzung datensicherungstechnischer Maßnahmen bis zur vorgesehenen Installation eines Netzwerks gewartet werden.

Diese Einschätzung haben wir nicht geteilt. Zum einen konnte der bisherige Sicherungsschutz leicht umgangen und somit auf sehr sensible medizinische Daten zugegriffen werden. Zum anderen sind an einen vernetzten PC vergleichbare Anforderungen zur Sicherstellung des Datenschutzes zu stellen wie an Einzelplatz-PC.

Mittlerweile hat die zuständige Fachbehörde zugesagt, die geforderte Verschlüsselung der Daten umzusetzen. Die Zusage erfolgte allerdings erst, nachdem von uns angekündigt worden war, demonstrativ aufzuzeigen, daß die bestehenden Sicherungsmaßnahmen mittels Schraubenzieher und Systemdiskette umgangen werden können.

Die bislang unzureichenden technischen Maßnahmen zur Sicherstellung des Patientendatenschutzes können jedoch nicht allein dem Bernhard-Nocht-Institut zur Last gelegt werden. Die zuständige Fachbehörde hat es bisher versäumt, die Rahmenbedingungen für die automatisierte Datenverarbeitung festzulegen, obwohl in ihrem Bereich besonders schützenswerte Daten zunehmend automatisiert verarbeitet werden. Aus unserer Sicht reicht es allerdings nicht aus, wie in einem Rohentwurf vorgeschlagen, allgemein auf die Geltung

von Datenschutz und Krankenhausgesetz, von Freigabe- und Dokumentationsrichtlinien und Hinweise des Senatsamts für die Verarbeitung personenbezogener Daten auf PC zu verweisen.

Erforderlich ist vielmehr eine bereichsspezifische Anpassung dieser Regelungen an die Art der zu verarbeitenden Daten und die Nutzungsbedürfnisse der speichernden Stellen. Auch im Hinblick auf das Krankenhausgesetz ist es notwendig, Konkretisierungen für die automatisierte Datenverarbeitung vorzunehmen, z.B. zu regeln, unter welchen näheren Voraussetzungen Krankheitsregister, Patientendatenbanken oder Vernetzungen von Anwendungen betrieben werden dürfen. Neben solchen rechtlichen Fragen sind Aspekte der technischen Datensicherung zu klären, z.B. daß Patientendaten, die auf PC verarbeitet werden sollen, zu verschlüsseln sind, wie Datenträger gegen den Zugriff Unbefugter geschützt werden müssen und welche räumlichen Mindestanforderungen zu stellen sind. Die Behörde für Arbeit, Gesundheit und Soziales hat zugesagt, in diesem Sinne eine Dienstanweisung auf der Grundlage der Dienstanweisung des Universitäts-Krankenhauses Eppendorf (21.1.2) zu erarbeiten und mit uns abzustimmen.

21.3 Patientendokumentationsprogramm Klinisch-medizinisches Analyse-Computer-System (KLIMACS)

Im Rahmen des Sofortprogramms zur AIDS-Bekämpfung stellte die Bundesregierung ausgewählten Kliniken und Instituten, in denen schwerpunktmäßig HIV-infizierte Personen behandelt werden, PC's und die Computerprogramme „KLIMACS" und „KLINAIDS" für eine automatisierte Krankendokumentation von HIV-Patienten zur Verfügung. In Hamburg nahmen das AK St.Georg und das Bernhard-Nocht-Institut diese Fördermittel in Anspruch. Bei der Entwicklung des Konzepts für die Krankendokumentation und der Programme waren allerdings datenschutzrechtliche Gesichtspunkte nur sehr unzureichend berücksichtigt worden, so daß mit den Programmen im klinischen Bereich – jedenfalls in Hamburg – bisher nicht gearbeitet werden konnte.

Dem Mangel der Dokumentationsprogramme soll nun durch nachgeschobene Datensicherungskonzepte abgeholfen werden, über die aber bisher – nach mittlerweile mehr als zwei Jahren nach Auslieferung der Computer und der ersten Programmversion – kein Einvernehmen hergestellt werden konnte. Zur datenschutzrechtlichen Bewertung lag im Berichtsjahr eine Ausarbeitung durch das Bundesarbeitsministerium über die „Datenschutzanforderungen an KLIMACS und seine Anwender" vor. Das Konzept geht davon aus, daß die Patientendaten grundsätzlich zu Behandlungszwecken im Rahmen des Behandlungsvertrags verarbeitet werden. Zur Sicherung der Patientendaten gegen unberechtigten Zugriff ist ein Paßwortschutz und eine Verschlüsselung vorgesehen.

Offen bleibt allerdings die wichtige Frage, ob die Identifikationsmerkmale des Patienten und der medizinischen Daten getrennt oder zusammen gespeichert werden sollen.

An Stellen außerhalb des Krankenhauses, insbesondere an das zuständige Ministerium, dürfen nur anonymisierte Daten für statistische Zwecke herausgegeben werden. Den Benutzern des Programms wird empfohlen, das Konzept mit den für sie zuständigen Landesdatenschutzbeauftragten abzustimmen und die Patienten über die Speicherung ihrer Daten zu Behandlungszwecken zu informieren.

Aus hamburgischer Sicht bedarf das Konzept einiger Änderungen und Anpassungen an die Datenverarbeitungsbedingungen der hiesigen potentiellen Benutzer. Zum einen hat sich in Beratungsgesprächen mit ihnen herausgestellt, daß das Dokumentationsprogramm nicht ausschließlich für Behandlungszwecke, sondern vor allem für Forschungsvorhaben genutzt werden soll. Das hat unmittelbare Auswirkungen auf die Rechtsgrundlage der Datenverarbeitung. Maßgeblich ist nicht der Behandlungsvertrag, sondern die Regelung im Krankenhausgesetz über die Forschung mit Patientendaten.

Angesichts der Befürchtungen, die von Betroffenen mit der dateimäßigen Speicherung von HIV-Infizierten verbunden werden können, und wegen der im Regelfall langen Speicherungszeit bei Dauerbehandlungsfällen ist davon auszugehen, daß durch die Datenverarbeitung die Belange der Betroffenen berührt werden. Daher steht ihnen zumindest ein Widerspruchsrecht gegen die automatisierte Speicherung ihrer Daten zu, auch wenn die Informationen nur innerhalb der Klinik personenbezogen genutzt werden. Wenn über die zur Behandlung erforderlichen Daten hinaus eigens Daten zu Forschungszwecken erhoben werden sollen, ist sogar die Einwilligung des Betroffenen erforderlich. Die vorgesehene Patienteninformation ist daher sowohl hinsichtlich des Verarbeitungszwecks der Daten als auch um einen Hinweis auf das Widerspruchsrecht bzw. das Erfordernis der Einwilligung zu ergänzen.

Im Hinblick auf die erforderlichen technischen und organisatorischen Datensicherungsmaßnahmen und das geplante Verschlüsselungsverfahren ist vorrangig zu klären, ob die Patientenidentifikationsmerkmale getrennt von den medizinischen Daten gespeichert werden. Nur bei einer getrennten Speicherung halten wir das vorgeschlagene Verschlüsselungssystem für ausreichend.

Bevor mit der Speicherung personenbezogener Daten von HIV-Patienten im Rahmen des Dokumentationsprogramms begonnen werden kann, besteht noch ein umfangreicher Abstimmungsbedarf mit den Benutzern über die Umsetzung der Datenschutzanforderungen.

21.4 Schulärztliche Dokumentation

Nach Pilotversuchen in den Bezirken Hamburg-Nord und Harburg ist zum 1. November 1990 in allen hamburgischen Bezirken ein neues schulärztliches Dokumentationsverfahren eingeführt worden. Mit Hilfe der automatisierten Datenverarbeitung ermöglicht es Auswertungen über gesundheitliche Probleme von Kindern und Jugendlichen in den einzelnen Bezirken und in Ham-

burg, die zu einer Verbesserung der gesundheitlichen Vorsorge beitragen sollen.

An der Vorbereitung der fachlichen Weisung als Grundlage des Dokumentationsverfahrens einschließlich des Erhebungsbogens und der Elterninformationsbriefe waren wir rechtzeitig beteiligt worden und haben Verbesserungsvorschläge eingebracht. Die Endfassung der fachlichen Weisung ist allerdings erst auf ausdrückliche Mahnung nach Inkrafttreten übersandt worden.

Dabei stellte sich heraus, daß entgegen mündlichen Zusagen die datenschutzrechtlichen Änderungsvorschläge nur unzureichend umgesetzt und der Erhebungsbogen ohne nochmalige Schlußabstimmung in einigen Punkten verändert worden war. Insbesondere die Information der Eltern über die Rechtsgrundlage der Datenerhebung und die vorgesehene Einwilligungserklärung entsprachen nicht den datenschutzrechtlichen Anforderungen und mußten nachgebessert werden.

Eine Information der Erziehungsberechtigten über Art und Umfang der geplanten Datenerhebung und -verarbeitung im Rahmen der schulärztlichen Dokumentation und über ihre Einwilligung ist erforderlich, da das Schulgesetz nur unzureichende Rechtsgrundlagen für die schulärztliche Untersuchung bietet: Es fehlen Regelungen, in welchem Umfang Informationen über die Schüler erhoben und zu welchen Zwecken sie genutzt werden dürfen. Zulässig nach dem geltenden Schulgesetz ist z.B. die Feststellung der Informationen, die zur Beurteilung der Schulreife erforderlich sind. Weitergehende Angaben, z.B. zur Entwicklung des Kindes, zu Vorerkrankungen, zum Impfstatus und zu sportlichen Betätigungen dürfen – obwohl sie für die Beurteilung des Gesundheitszustands hilfreich und für übergreifende Auswertungen sinnvoll sein können – nur mit ausdrücklicher Einwilligung der Erziehungsberechtigten erhoben und genutzt werden.

Diese Einwilligung soll nach dem neuen Dokumentationsverfahren bei der Erstuntersuchung nach vorheriger schriftlicher Information von dem Erziehungsberechtigten mündlich eingeholt und vom Schulärztlichen Dienst dokumentiert werden. Bei den Folgeuntersuchungen, zu denen die Schüler klassenweise gehen, sind schriftliche Elternfragebögen und Einwilligungserklärungen vorgesehen. Die Elterninformationen und die erforderlichen Einwilligungserklärungen sind inzwischen den datenschutzrechtlichen Anforderungen entsprechend geändert worden.

Beim Ausbau der Gesundheitsberichterstattung ist gerade im schulischen Bereich zu beachten, daß sich die Eltern faktisch kaum der Einwilligung entziehen können. Deshalb sind die Anforderungen an eine klare Information der Eltern hoch anzusetzen. In den geänderten Formularen ist dies nunmehr berücksichtigt worden.

Außerdem werden wir auch künftig darauf hinwirken, daß nur erforderliche Daten erhoben werden. Die ursprünglich z.B. beabsichtigten näheren Fragen

zur Staatsangehörigkeit konnten nur mühsam reduziert werden. Aus einer Eingabe wurde deutlich, daß in Einzelfällen offenbar weit mehr Fragen gestellt werden, als vorgesehen und zulässig sind.

22. Umweltschutz

22.1 Projekt Beschleunigung von Genehmigungsverfahren

Im Jahre 1990 wurde bei der Umweltbehörde eine Projektgruppe installiert, um die Genehmigungsverfahren mit den Bedingungen und Auflagen für die Errichtung technischer Anlagen, von deren Betrieb eine Gefährdung der Umwelt ausgehen könnte, durch den Einsatz von IuK-Technik zu beschleunigen. Da auf Veranlassung des Senatsamtes für den Verwaltungsdienst die Umweltbehörde den Nachweis zu erbringen hatte, daß die geplante ADV-Ausstattung in ein allgemeines ADV-Konzept für die gesamte Umweltbehörde paßt, hat die Umweltbehörde im Rahmen dieser Projektgruppe ein externes Gutachten über die Erstellung eines Netzwerkkonzeptes eingeholt. Hierüber wurde der Hamburgische Datenschutzbeauftragte von der Umweltbehörde erst unterrichtet, als er von anderer Seite einen Hinweis auf die Einrichtung der Projektgruppe erhalten hatte.

Die Umweltbehörde hat mit unterschiedlichen Systemkomponenten bereits eine ganze Reihe von Datenbanken sowohl auf dem System der Datenverarbeitungszentrale als auch auf örtlichen PC eingerichtet, auf denen auch personenbezogene Daten verarbeitet werden. Da die bisher langen Laufzeiten der Genehmigungsverfahren oftmals zu Beschwerden der Antragsteller und auch zum Investitionsstau oder gar zu Abwanderungen der Industriebetriebe führten, soll nunmehr durch ein transparentes Zusammenlegen der Tätigkeiten in den verschiedenen Fachämtern der Umweltbehörde eine wesentliche Beschleunigung der Genehmigungsverfahren erreicht werden. Hierfür soll im wesentlichen ein ständiger Informationsaustausch zu gleichen oder ähnlichen Sachverhalten unter Verwendung gleicher Stammdaten zwischen den einzelnen Datenbanken erfolgen. Als mittelfristige Lösung strebt die Umweltbehörde zu diesem Zweck die Errichtung eines Netzwerkes an.

Wir hatten erstmalig Mitte des Jahres 1991 die Möglichkeit, an einer Projektgruppensitzung teilzunehmen und uns zu den geplanten Datensicherungsmaßnahmen zu äußern. Dabei wurde auf eine Reihe von Schwachpunkten im Detail hingewiesen. Die Umweltbehörde hat zugesagt, beim weiteren Fortgang des Projektes diese Hinweise zu beachten sowie uns rechtzeitig in geeigneter Weise an der Projektarbeit zu beteiligen.

22.2 Dienstanweisung der Umweltbehörde für Datensammlungen in ADV-gestützter Form

Der Rechnungshof hatte in seinem Bericht für die Haushaltsrechnung 1988 das Ergebnis seiner Prüfung über die Sammlung und Erfassung umweltbezogener Daten bei der Umweltbehörde dargestellt. Darin wurde der Umweltbehörde u.a. vorgeschlagen, fachliche Regeln und Standards aufzustellen, denen die Datenverarbeitung in der Umweltbehörde zu folgen habe.

Dieser Vorschlag wurde von der Umweltbehörde im Berichtszeitraum aufgegriffen und der Entwurf einer „Dienstanweisung für den Aufbau und Betrieb von Datensammlungen (Dateien) in ADV-gestützter Form" in das externe Abstimmungsverfahren gegeben.

Der Hamburgische Datenschutzbeauftragte hat die Vorlage dieser Dienstanweisung ausdrücklich begrüßt, zumal leider zahlreiche andere Behörden und Ämter noch immer nicht die Notwendigkeit solcher Regelungen erkannt haben. Die von uns vorgetragenen Änderungs- und Ergänzungswünsche hat die Umweltbehörde ausnahmslos in eine Neufassung des Entwurfs übernommen. Hierzu gab es aus unserer Sicht keine weiteren inhaltlichen Korrekturwünsche.

Das Schutzstufenkonzept zu PC-Sicherungsmaßnahmen, das wir in unserem 9. TB (3.2) veröffentlicht haben, war als Anlage zur Dienstanweisung ebenso vorgesehen wie das Formblatt zur Dateiregistermeldung. Aus dem Formblatt lassen sich die nach dem HmbDSG geforderten Angaben und Maßnahmen entnehmen. Der Entwurf enthielt darüber hinaus eine Auflistung einschlägiger Rechtsvorschriften für den Aufbau und Betrieb von Dateien.

Allerdings äußerte inzwischen das Senatsamt für den Verwaltungsdienst – leider erst nach 3 Monaten – Kritik an der zuletzt vorgelegten Fassung des Entwurfs, die sich zum großen Teil auf den Empfehlungscharakter der Datenschutzhinweise bezog. Daraufhin hat die Umweltbehörde die Bestandteile der Dienstanweisung, die zur Einhaltung datenschutzrechtlicher Bestimmungen und technischer Standards sinnvoll sind, aus dem Entwurf genommen und die Dienstanweisung verabschiedet, ohne uns Gelegenheit zur Stellungnahme zu geben.

Wir haben der Umweltbehörde empfohlen, diese Hinweise zum Datenschutz mit einem von uns vorbereiteten Schreiben den Mitarbeitern und Mitarbeiterinnen nachträglich zur Kenntnis zu geben. Zugleich haben wir betont, daß wir bei Einwendungen gegen unsere Vorschläge zu behördlichen Dienstanweisungen eine abschließende Abstimmung vor deren Erlaß erwarten.

22.3 Novellierung des Hamburgischen Wassergesetzes

Im Berichtszeitraum wurde das Sechste Gesetz zur Änderung des Hamburgischen Wassergesetzes (HWaG) verabschiedet; das novellierte HWaG ist am 1. Februar 1991 in Kraft getreten. Die Umweltbehörde hat den Hamburgischen Datenschutzbeauftragten rechtzeitig und umfassend an dem Novellierungsvorhaben beteiligt.

Aus datenschutzrechtlicher Sicht ist im wesentlichen die Einfügung eines § 101 HWaG von Bedeutung. Nach dieser neuen Bestimmung sind nunmehr die im

Wasserbuch eingetragenen Daten jedermann zugänglich, d.h. die zuständige Wasserbehörde kann zu den bei ihr vorhandenen Daten über Abwassereinleitungen Auskünfte erteilen.

Zu der Rechtsänderung und der damit verbundenen Einführung eines „Gläsernen Abflußrohres" hatte sich der Hamburgische Datenschutzbeauftragte bereits in seinem 8. TB (3.5) grundsätzlich positiv geäußert. Maßgeblich hierfür war die Überlegung, daß die umfassende Information der Allgemeinheit über die Nutzung der Umwelt im Rahmen von industriellen Produktionsprozessen geeignet ist, dem Schutz und dem Erhalt der natürlichen Lebensgrundlagen zu dienen.

Darüber hinaus hat sich der Hamburgische Datenschutzbeauftragte zu dieser Problematik gutachterlich gegenüber dem bürgerschaftlichen Rechtsausschuß geäußert und im Ergebnis erreicht, daß im § 101 HWaG deutlich gemacht wird, welche Daten im einzelnen offengelegt werden dürfen, da in diesen Fällen das Informationsinteresse der Allgemeinheit dem Geheimhaltungsinteresse des Gewässerbenutzers vorgeht.

Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

23. Werbewirtschaft

Die Novellierung des Bundesdatenschutzgesetzes hat im Ergebnis nicht zu nennenswerten Einschränkungen der Werbewirtschaft im Umgang mit personenbezogenen Daten geführt. Die für die Werbewirtschaft wesentlichen Vorschriften sind die §§ 28 und 29 BDSG. Neben Speicherung, Übermittlung und Veränderung personenbezogener Daten sind nunmehr auch ihre Nutzung (insbesondere Adreßabgleich und Wiederverwendung erhobener Daten) und Erhebung (nach Treu und Glauben und auf rechtmäßige Weise) geregelt.

§ 28 Abs. 2 BDSG enthält die Voraussetzungen, unter denen die Übermittlung und Nutzung über die Beschränkungen des Abs. 1 (im Rahmen der Erfüllung eigener Geschäftszwecke) hinaus zulässig ist. Für die Direktwerbung bedeutet dies, daß Übermittlung und Nutzung grundsätzlich zulässig sind, weil ein „berechtigtes" Interesse auch in wirtschaftlichen Erwägungen bestehen kann. § 28 Abs. 2 Nr. 1 b BDSG läßt Übermittlung und Nutzung bestimmter zusammengefaßter Daten über Angehörige einer Personengruppe grundsätzlich zu; dabei darf entgegen der früheren gesetzlichen Regelung die Rufnummer gar nicht und statt des genauen Geburtsdatums lediglich das Jahr der Geburt noch übermittelt werden.

Die Zulässigkeitsvoraussetzungen stehen unter der Bedingung, daß kein Grund zu der Annahme besteht, der Betroffene habe ein schutzwürdiges Interesse am Ausschluß der Übermittlung. Zusätzlich besteht für die Daten nach Nr. 1 b die (widerlegbare) gesetzliche Vermutung, daß der Betroffene ein schutzwürdiges Interesse gegen die Übermittlung der dort genannten besonders sensiblen Daten hat, z.B. hinsichtlich der gesundheitlichen Verhältnisse.

Aus Sicht der Aufsichtsbehörde Hamburg ist es unbefriedigend, daß insbesondere die nur scheinbar engere Regelung des Abs. 2 Nr. 1 a BDSG im Ergebnis auch die zusammengefaßte Übermittlung der besonders sensiblen Daten ermöglichen wird. Dies liegt an den geringen Anforderungen, die an die Annahme eines „berechtigten Interesses" eines Dritten zu stellen sind. Andererseits sind im Bereich der Direktwerbung an das Vorliegen eines schutzwürdigen Interesses des Betroffenen in Literatur und Rechtsprechung bislang sehr hohe Anforderungen gestellt worden.

Die Aufsichtsbehörde bezweifelt außerdem, ob die Aufzählung der besonders sensiblen Daten als abschließend anzusehen ist. Dazu gehören vielmehr auch Daten über die rassische Herkunft und das Sexualleben. Deshalb ist davon auszugehen, daß auch die Übermittlung solcher Daten schutzwürdige Interessen der Betroffenen beeinträchtigt.

Neu und grundsätzlich zu begrüßen ist die Regelung des § 28 Abs. 3 BDSG, die dem Betroffenen gegenüber der speichernden Stelle und gegenüber dem

Datenempfänger Widerspruchsrechte gegen die Nutzung und Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- und Meinungsforschung einräumt. Im Falle eines Widerspruchs ist die Verwendung der Daten für diese Zwecke nicht mehr zulässig und außerdem strafbar (§ 43 Abs. 1 BDSG).

Allerdings beinhaltet das Widerspruchsrecht kein unmittelbares Recht auf Auskunft gegenüber der speichernden Stelle über den Kreis der Empfänger der Daten. Es enthält auch insbesondere gegenüber dem Empfänger nicht das Recht auf Nennung der speichernden Stelle. Im Streitfall müßte daher der Betroffene sein Auskunftsrecht darüber, aus welcher Quelle die Daten stammen oder an wen sie bereits übermittelt wurden, zunächst auf dem Zivilrechtsweg durchzusetzen versuchen, um dann von seinem Widerspruchsrecht wirksam Gebrauch machen zu können. In dem häufigen Fall, in dem der Werbende selbst gar nicht über die Daten verfügt, sondern die Anschriften der Betroffenen von einem Dritten dem Werbematerial hinzugefügt werden, kann der Betroffene sogar weder den Empfänger noch die speichernde Stelle erkennen. Hinsichtlich der Auskunft über die Quelle der Daten wurde daher eine wesentliche Forderung der Aufsichtsbehörde Hamburg (vgl. z.B. 4. TB, 6.2.2.9) nicht erfüllt.

Aus der Sicht der Aufsichtsbehörde wäre im Hinblick auf die neuen Widerspruchsrechte die Aufnahme einer umfassenderen Benachrichtigungspflicht erforderlich gewesen. Eine Benachrichtigungspflicht entfällt z.B. in dem häufigen Fall, in dem Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert sind und es sich um listenmäßig oder sonst zusammengefaßte Daten handelt (§§ 33 Abs. 2 Nr. 7 b, 29 Abs. 2 Nr. 1 b, 28 Abs. 2 Nr. 1 b BDSG). Diese unter anderem für Adressenverlage geltenden Ausnahmetatbestände führen dazu, daß die Möglichkeit des Widerspruchs des Betroffenen sowie die durch einen Widerspruch ausgelöste Strafbewehrung des § 43 Abs. 1 BDSG gegenstandslos werden.

Neu ist die grundsätzliche Bindung des Empfängers von Daten gemäß §§ 28 und 29 BDSG an die Verarbeitung und Nutzung für den Zweck der Übermittlung sowie die Pflicht der speichernden Stelle, den Empfänger auf die Zweckbindung hinzuweisen. Allerdings dürfen die Daten hiervon abweichend für alle nach den Absätzen 1 und 2 zugelassenen Zwecke verwendet werden.

Der bereits in früheren Tätigkeitsberichten (z.B. 5. TB, 6.3.6) erwähnte Verband, der die „Robinson-Liste" (Verzeichnis privater Verbraucher, die keine adressierte Werbung wünschen) führt, hat mit Vertretern der Direktmarketing-Verbände aus Frankreich, den Niederlanden, Großbritannien und Belgien eine „Pariser Konvention über Robinson-Listen" verabschiedet. Im Hinblick auf den europäischen Binnenmarkt soll damit dem Verbraucherinteresse auch bei grenzüberschreitender Direktwerbung Rechnung getragen werden. In Deutschland strebt der Verband an, den Abgleich mit der Robinson-Liste für die Werbewirtschaft verbindlicher zu regeln und die Abgleichquote auf über 90 % (bisher: fast 80 %) zu steigern (Anschrift: Deutscher Direktmarketing Verband e.V. – Robinson-Liste – Schiersteiner Straße 29, 6200 Wiesbaden).

24. SCHUFA

Im Jahr 1991 sind bei der Aufsichtsbehörde vier Eingaben eingegangen, in denen sich die Petenten darüber beschwerten, daß mißbräuchliche Auskunftsersuchen von der SCHUFA beantwortet worden seien. Nach Angaben der Petenten waren sie mit dem SCHUFA-Vertragspartner, der ein bestimmtes berechtigtes Interesse an der Auskunft angegeben hatte, überhaupt nicht in Kontakt getreten. Die Auskünfte waren in den Beschwerdefällen überwiegend telefonisch erteilt worden. Bei telefonischer Auskunfterteilung meldet die anfragende Stelle sich als Vertragspartner und gibt ihre SCHUFA-Kennummer sowie seit mehreren Jahren auch ein Paßwort an. Einige langjährige SCHUFA-Vertragspartner verfügen noch nicht über ein Paßwort.

Zusammen mit der SCHUFA sind wir bemüht, derartige Fälle aufzuklären und gegebenenfalls die Möglichkeit mißbräuchlicher Angaben eines berechtigten Auskunftsinteresses auszuschließen. In zwei der genannten Eingabefälle, in denen über Mitarbeiter der SCHUFA-Vertragspartner unberechtigt „Gefälligkeitsauskünfte" eingeholt wurden, sind die jeweiligen Vertragspartner von der SCHUFA abgemahnt worden. Die anderen Fälle sind noch nicht vollständig abgeschlossen. In Mißbrauchsfällen, die nach dem Inkrafttreten der erweiterten Strafvorschriften des neuen Bundesdatenschutzgesetzes eingetreten sind, haben die Betroffenen binnen einer dreimonatigen Frist die Möglichkeit, Strafantrag zu stellen.

Wie groß die Anzahl der tatsächlich von dieser Art Mißbrauch Betroffenen ist, läßt sich anhand der Zahl der Eingaben nicht abschätzen. Angesichts von über drei Millionen Auskünften, die die SCHUFA Hamburg nach ihren Angaben im Jahr 1991 erteilt hat, und der begrenzten Zahl von Eingaben kann vermutet werden, daß die Vorkehrungen, die die SCHUFA trifft, weitgehend wirksam sind.

Dennoch wollen wir mit der SCHUFA erörtern, wie bei telefonischen Anfragen die Anfrageberechtigung noch besser sichergestellt werden kann. Die Aufsichtsbehörden wollen versuchen, eine quantitative Verbesserung der Stichprobenverfahren, die die SCHUFA zur Prüfung des berechtigten Interesses selbst durchführt, zu erreichen. (Zum berechtigten Interesse siehe auch 26.1.) Die Praxis der SCHUFA, monatlich in fünfzehn Fällen das berechtigte Interesse zu überprüfen, ist aus unserer Sicht nicht ausreichend, zumal bei diesen wenigen Kontrollen keine Mißbrauchsfälle festgestellt wurden. Die beabsichtigte Abschreckung vor mißbräuchlicher Inanspruchnahme der SCHUFA ist mit dieser geringen Anzahl von Kontrollen nicht erreichbar. Die SCHUFA Hamburg beabsichtigt im übrigen, durch verstärkte Aufklärung und Schulung ihrer Vertragspartner mißbräuchlichen Auskunftsersuchen vorzubeugen.

25. Versicherungswirtschaft

Auch im Berichtsjahr wurde die Weiterentwicklung der zentralen Warn- und Hinweissysteme in der Versicherungswirtschaft verfolgt und datenschutzrecht-

lich überprüft (vgl. zuletzt 9. TB, 5.3.1). Ein weiterer Schwerpunkt in der Arbeit der Aufsichtsbehörde lag im Voranbringen der datenschutzrechtlich unbedenklichen Schweigepflicht-Entbindungserklärungen im Schadensfall (vgl. zuletzt 9. TB, 5.3.3).

25.1 Automationsvorhaben

Die Versicherungswirtschaft plant eine Umstellung aller zentralen Warn- und Hinweissysteme auf das phonetische Strukturcode-Verfahren im Laufe des Jahres 1992 (vgl. dazu auch 8. TB, 4.2.1.1). Dabei sollen die Volltexte von den Versicherungsunternehmen an den jeweiligen Verband gemeldet werden. Dort wird der Datensatz codiert und in die Datei, die auf Datenträgern an die Mitgliedsunternehmen versandt wird, eingegeben. Anschließend werden die Volltexte vernichtet. Daraus ergibt sich, daß nach der Erstellung der Datei nur noch die jeweiligen Versicherungsgesellschaften in der Lage sein werden, personenbezogene Daten über Versicherungsantragsteller, Anspruchsteller o.ä. mit der Datei abzugleichen.

25.2 Rechtliche Einordnung der Verbände

Mit dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) wurde Einigkeit darüber erzielt, daß die Verbände unter diesen Umständen Auftragsdatenverarbeiter im Sinne von § 11 Abs. 3 und 4 BDSG sind. Die Versicherungsunternehmen sind speichernde Stellen nach § 28 BDSG, die Datenverarbeitung für eigene Zwecke und in eigener Verantwortung betreiben und § 11 Abs. 1 und 2 BDSG zu beachten haben.

Diese – von den Aufsichtsbehörden lange angestrebte – Einordnung ist angesichts der Einführung des phonetischen Strukturcode-Verfahrens auch praktisch zwingend geworden. Ausschlaggebend dafür ist, daß die Vernichtung der Volltexte und das Fehlen der Abgleichfunktion bei den Verbänden es diesen unmöglich macht, den sonst bestehenden Verpflichtungen zur Benachrichtigung des Betroffenen nach § 33 Abs. 1 BDSG und der Auskunft nach § 34 Abs. 1 BDSG nachzukommen, falls ihre Tätigkeit als geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung gem. § 29 BDSG eingeordnet würde. Diese Pflichten sind nunmehr von den jeweiligen Versicherungsunternehmen wahrzunehmen.

Mit der Umstellung auf das phonetische Strukturcode-Verfahren wird den datenschutzrechtlichen Anforderungen deutlich besser Rechnung getragen. Einerseits ist es den Verbänden infolge der fehlenden Abgleichfunktion unmöglich geworden, bestimmte Personen zu reidentifizieren. Andererseits werden in den Versicherungsunternehmen mit größerer Sicherheit nur noch diejenigen Daten verwendet, die zur Beurteilung des Risikos bei Antragstellung oder der Leistungspflicht im Schadensfall erforderlich sind.

Für das neue Verfahren wird es notwendig sein, zwischen den Verbänden und den beteiligten Unternehmen Verträge abzuschließen, die den Anforderungen

des § 11 BDSG entsprechen. Die Aufsichtsbehörden werden hierbei unterstützend tätig sein und insbesondere darauf hinwirken, daß die Verbände sich in Anlehnung an § 6 Abs. 2 BDSG verpflichten, Betroffene, die sich irrtümlich an sie wenden, über den richtigen Adressaten ihres Rechts aufzuklären. Darüber hinaus wird zu beobachten sein, ob die zeitlichen und inhaltlichen Vorstellungen des GDV den bisherigen Vereinbarungen entsprechend eingehalten werden.

25.3 Meldeverfahren der Kfz-Versicherer

Die Gespräche mit dem HUK-Verband über die Neukonzeption des Meldeverfahrens der Kfz-Versicherer, über die im letzten Tätigkeitsbericht ausführlich berichtet wurde (vgl. 9. TB, 5.3.1.3), sind nunmehr fortgesetzt worden.

Grundlage dieser Neukonzeption ist – wie auch bei den übrigen zentralen Dateien – die Einführung eines einheitlichen Strukturcode-Verfahrens für alle Verbände. Im Berichtsjahr wurde ein entsprechender Softwaretest durchgeführt, dem sich eine Testphase mit einigen ausgewählten Versicherungsunternehmen anschloß, die voraussichtlich Anfang 1992 beendet sein wird.

Die vom HUK-Verband entwickelten Kriterien, die zur Grundlage dafür gemacht werden sollen, ob eine Meldung an das Kraftfahrt Hinweis System erfolgt, waren erneut Gegenstand eingehender Diskussion.

Dabei fiel insbesondere auf, daß nach der Neukonzeption nur noch eine statt der bisherigen fünf Dateien aufgebaut und gepflegt werden soll. Im Rahmen des Systems wird die Speicherung teilweise auf Fahrzeugdaten beschränkt.

Bei Vorliegen konkreter Schadens- oder Abrechnungsmodalitäten sollen folgende Fahrzeugdaten aufgenommen werden:

— Fahrzeug-Identifizierungsnummer (17-stellig),

— amtliches Kennzeichen,

— Verkaufsbezeichnung (Fahrzeugtyp),

— Schadennummer des meldenden Versicherungsunternehmens,

— Telefonnummer des meldenden Versicherungsunternehmens,

— Schadenart,

— Postleitzahl des Schadenortes,

— Land des Unfalls.

Der HUK-Verband begründet die Notwendigkeit der Speicherung dieser Daten, die nur in näher bezeichneten Fällen stattfinden soll, zum einen mit der häufig erforderlichen nachträglichen Zuordnung des Eigentums bei z.B. gestohlenen und wiederaufgefundenen Fahrzeugen. Zum anderen gebe es bestimmte Fahrzeugschäden, die entweder mehrfach bei Versicherungen abgerechnet oder gutgläubigen Erwerbern verschwiegen würden.

Aus datenschutzrechtlicher Sicht ist anzumerken, daß die vorgesehene teilweise Beschränkung der Meldung auf Fahrzeugdaten nicht die Schlußfolgerung zuläßt, es handele sich hierbei um keine personenbezogenen Daten, denn die Angabe der Schadennummer und der Telefonnummer des meldenden Versicherungsunternehmens läßt die Identifizierung des betroffenen Versicherungsnehmers zu.

Gleichwohl ist zu begrüßen, daß es in den genannten Fällen nicht zur Einmeldung der Versicherungsnehmer kommt, sondern diese erst dann identifiziert werden können, wenn entweder ein gestohlenes Fahrzeug wieder aufgetaucht ist oder sich der Verdacht auf betrügerischen Umgang mit einem Fahrzeug konkretisiert hat.

Hinsichtlich der Meldung von Personen, die an einem Schadenfall beteiligt sind, wurde folgendes klargestellt:

Das Konzept sieht vor, daß bestimmte objektivierte Daten von den Kfz-Versicherern an den HUK-Verband in Vollschrift gemeldet, dort mit Hilfe des neuen phonetischen Strukturcode-Verfahrens im Auftrag der Unternehmen verschlüsselt und ihnen als eine Datei in regelmäßigen Abständen auf Magnetbändern übermittelt werden.

Wichtig ist, daß Personendaten nur dann gemeldet werden dürfen, wenn im Schadenfall mittels der nach Punkten gewichteten Kriterien mindestens 60 Punkte erreicht werden.

Die Meldung von sonstigen am Schadenfall beteiligten Personen ist auf Zeugen zu beschränken. Zeugen sind dann zu melden, wenn nach dem Kriterienkatalog im Schadenfall 60 Punkte erreicht werden und der Zeuge in einem der beiden Fahrzeuge saß oder mit einem der Beteiligten verwandt oder bekannt ist und seine Aussage als Beweismittel zur Erlangung der Versicherungsleistung dient.

25.4 Zentrale Registrierstelle Rechtsschutz

In die Datei der Zentralen Registrierstelle Rechtsschutz wurden Personen aufgenommen, deren Rechtsschutz-Versicherungsvertrag vom Versicherungsunternehmen gemäß § 19 Abs. 2 der Allgemeinen Bedingungen für die Rechtsschutzversicherung (ARB 75) gekündigt wurde, weil in 12 Monaten mindestens zwei Versicherungsfälle aufgetreten sind (vgl. 8. TB, 4.2.1.3).

Der Bundesgerichtshof hält § 19 Abs.2 ARB 75 – ebenso wie § 19 Abs.1 – wegen ungleicher Behandlung der Versicherungsnehmer bei den Kündigungsmöglichkeiten, die in dieser Weise nicht in Allgemeinen Geschäftsbedingungen eingeschränkt werden dürfen, für unvereinbar mit § 9 Abs. 2 Nr. 1 AGBG. Das Gericht hat die beklagte Versicherungsgeselischaft verurteilt, es zu unterlassen, eine derartige Bestimmung in künftig abzuschließende Rechtsschutzversicherungsverträge durch Allgemeine Geschäftsbedingungen einzubeziehen sowie sich auf diese Bestimmung bei der Abwicklung derartiger, nach dem

1. April 1977 abgeschlossener Verträge zu berufen (Urteil vom 27. März 1991, Az. IV ZR 130/90). § 19 Abs. 2 ARB 75, auf den sich die Versicherungsunternehmen bei der Meldung von Personen an die Zentrale Registrierstelle Rechtsschutz berufen, ist daher nach unserer Auffassung gemäß § 9 Abs. 1 AGBG unwirksam.

Nach übereinstimmender Meinung der Versicherungswirtschaft und der Aufsichtsbehörden können aufgrund dieser Unwirksamkeit keine weiteren Meldungen an den HUK-Verband erfolgen, die sich auf diese Vorschrift stützen. Der HUK-Verband hat inzwischen im Zusammenwirken mit dem Bundesaufsichtsamt für das Versicherungswesen eine neue Kündigungsregelung vorbereitet, wonach künftig die Leistungspflicht für mindestens drei Versicherungsfälle in 12 Monaten vorliegen muß und dann erst sowohl der Versicherungsnehmer als auch der Versicherer kündigen kann.

Über den Umgang mit dem bereits vorhandenen Bestand der Zentralen Registrierstelle Rechtsschutz konnte bisher keine Einigung erzielt werden. Aus der von Anfang an bestehenden Unwirksamkeit des § 19 Abs. 2 ARB 75 ergibt sich nach Meinung der Aufsichtsbehörden, daß auch die im Bestand vorhandenen Meldungen nicht auf § 19 Abs. 2 ARB 75 gestützt werden dürfen.

Daraus läßt sich jedoch nicht folgern – wie es auch vertreten wird –, daß auf eine vollständige Streichung der in der Datei erfaßten personenbezogenen Daten hinzuwirken ist, was im Ergebnis einer Löschung der gesamten Datei gleichzusetzen wäre. Zweck der Datei ist es, anderen Rechtsschutzversicherern bei der Bearbeitung eines Versicherungsantrages einen Hinweis darauf zu geben, daß die antragstellende Person möglicherweise ein besonderes Risiko darstellt. § 19 Abs. 2 ARB 75 wurde nur deshalb zur Beurteilung herangezogen, weil die betroffene Versicherungsgesellschaft Konsequenzen aus einem Verhalten des Versicherungsnehmers ziehen konnte, das als risikobehaftet angesehen wird. Über diesen Umstand und dessen datenschutzrechtliche Bewertung trifft das angesprochene Urteil des Bundesgerichtshofs jedoch keine Aussage.

Mit der Versicherungswirtschaft werden derzeit Gespräche mit dem Ziel geführt, die bestehende Datei auf eine rechtlich einwandfreie Grundlage zu stellen. Die Vorstellungen gehen dahin, daß nicht mehr auf die in der Vergangenheit erfolgte Kündigung nach § 19 Abs. 2 ARB 75 abgestellt werden darf. Vielmehr soll maßgeblich sein, daß der Versicherer seine Leistungspflicht für mindestens zwei, künftig drei in 12 Monaten eingetretene Versicherungsfälle bejaht hat und das Vertragsverhältnis mit dem Versicherten beendet wurde. Zumindest wird eine Anpassung im Merkblatt, das die Versicherungskunden erhalten, für erforderlich gehalten.

Diese Grundsätze gelten ebenso für die ausgesprochenen ordentlichen Ablaufkündigungen nach § 8 ARB 75, die in Abstimmung mit der Aufsichtsbehörde dann an die Zentrale Registrierstelle Rechtsschutz gemeldet werden konnten, wenn die materiellen Voraussetzungen des § 19 Abs. 2 ARB 75 vorlagen.

Das Merkblatt zur Datenverarbeitung, das auf Verlangen der Aufsichtsbehörden bereits um den Hinweis einer möglichen Meldung an das zentrale Hinweissystem erweitert wurde, soll auch in diesem Punkt angepaßt werden.

Die Versicherungswirtschaft vertritt bisher den Standpunkt, daß hinsichtlich der Altbestände keinerlei Veränderungen vorzunehmen sind. Die Erörterung – auch mit dem Bundesaufsichtsamt für das Versicherungswesen und dem Bundesbeauftragten für den Datenschutz – ist noch nicht abgeschlossen.

25.5 Benachrichtigung der Dritten

Aus dem letzten Tätigkeitsbericht ist ersichtlich, daß die vorgeschlagene Formulierung über die Benachrichtigung Dritter von der Versicherungswirtschaft nicht akzeptiert worden war (vgl. 9. TB, 5.3.1.2).

Auch unter Berücksichtigung des neuen Bundesdatenschutzgesetzes ergibt sich jedoch für die Aufsichtsbehörden kein Anlaß, von der Forderung nach einer qualifizierten Benachrichtigung derjenigen Personen abzusehen, die nicht auf andere Weise von der Aufnahme ihrer Daten in eine Warndatei Kenntnis erlangen konnten (sog. Dritte). Nachdem grundsätzlich Einigkeit darüber erzielt werden konnte, daß die Versicherungsunternehmen bei Anwendung des phonetischen Strukturcodeverfahrens als speichernde Stellen im Sinne des § 28 BDSG und die Verbände als Auftragsdatenverarbeiter im Sinne des § 11 Abs. 3 und 4 BDSG anzusehen sind (vgl. 25.2), beurteilen sich die Übermittlungen personenbezogener Daten von den Versicherungsunternehmen über die Verbände an alle Versicherungsgesellschaften desselben Versicherungszweiges nach § 28 Abs. 2 BDSG.

Ebenso wie nach der alten Rechtslage sind hierbei die schutzwürdigen Interessen des jeweils Betroffenen an dem Ausschluß der Übermittlung und die berechtigten Interessen der Versicherungswirtschaft an der Verhinderung und Aufklärung von Fällen des Versicherungsbetruges gegeneinander abzuwägen. Ein Betroffener, der keine Kenntnis von einer derartigen Übermittlung haben kann, hat jedoch nicht die Möglichkeit, seine schutzwürdigen Interessen bekanntzugeben und zu vertreten.

Der GDV begründete nunmehr seine Ablehnung des bisher von uns vorgelegten Formulierungsvorschlags damit, daß der Dritte umfassender informiert würde als der Versicherungskunde selbst, der nur aus seinem Vertrag in Verbindung mit einem entsprechenden Merkblatt Rückschlüsse auf eine eventuelle Meldung ziehen könne. Daraufhin wurde seitens der Aufsichtsbehörden ein Vorschlag unterbreitet, wonach dem Betroffenen ein Schreiben in Verbindung mit dem auch dem Versicherungskunden zur Verfügung gestellten Merkblatt übersandt werden könnte. Nach weiterer Diskussion über den Inhalt des Schreibens konnte Einigkeit über folgenden Text erzielt werden:

„... unser Versicherungsnehmer meldete uns den obigen Schaden. Im Rahmen der Bearbeitung dieses Schadens wurden die Daten der beteiligten

Personen (konkrete Angabe der gespeicherten Daten z.B. Name, Anschrift, Geschlecht und Geburtstag) in unserem Hause gespeichert. Wir geben Ihnen von der Speicherung nach den Vorschriften des Bundesdatenschutzgesetzes Kenntnis. Im übrigen wird auf Nr. 4 des beigefügten Merkblattes verwiesen."

Dieser Text stellt einerseits eine Benachrichtigung des Betroffenen über die Tatsache der Speicherung und die Art der über ihn bei der Versicherungsgesellschaft gespeicherten Daten gemäß § 33 Abs. 1 BDSG dar. Andererseits erhält der Betroffene – zusammen mit dem Merkblatt – einen Hinweis auf die mögliche Speicherung in einem Warn- und Hinweissystem und hat damit Gelegenheit, ggf. seine schutzwürdigen Interessen im Rahmen der Übermittlung nach § 28 Abs. 2 BDSG geltend zu machen.

25.6 Transfer von Daten in Mitgliedsländer der EG

Die Probleme, die mit der Einführung des europäischen Binnenmarktes hinsichtlich der Übermittlung von personenbezogenen Daten aus den zentralen Dateien in andere EG-Länder entstehen, wurden bereits im 9. TB (5.3.1.4) behandelt. Es besteht Grund zu der Annahme, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß einer derartigen Übermittlung gemäß § 28 Abs. 2 BDSG hat. Dies gilt insbesondere dann, wenn in dem entsprechenden Land keine oder unzureichende Datenschutzgesetze existieren, weil dann die in der Bundesrepublik geltenden Rechte aus dem BDSG nicht wahrgenommen werden können.

Von der Versicherungswirtschaft wurde eine Lösung dieses Problems bisher nicht für erforderlich gehalten, weil der Transfer von Daten aus den Warn- und Hinweissystemen ins Ausland nicht geplant sei. Daher sei weder von den Versicherungsunternehmen noch von den Verbänden ein Konzept für den Umgang mit den personenbezogenen Daten entwickelt worden, die nach Öffnung des EG-Binnenmarktes ins Ausland übermittelt werden. Es wurde zugesagt, die Datenschutz-Aufsichtsbehörden im Falle der Entwicklung eines entsprechenden Konzepts zeitgerecht zu beteiligen.

In Zukunft ist besonderes Augenmerk darauf zu richten, welche Verfahrensweisen die Versicherungswirtschaft im Auslandsgeschäft verfolgt. Sollten z.B. ausländischen Versicherungsunternehmen, abgesehen von deren deutschen Niederfassungen, Datenbestände aus den zentralen Warn- und Hinweissystemen zur Verfügung gestellt werden, muß der Schutz und insbesondere auch die Information der Betroffenen sichergestellt werden.

Im Rahmen eines multilateralen Garantie-Abkommens zwischen den nationalen Versicherungsbüros vom 15. März 1991, das auf seiten Deutschlands vom HUK-Verband unterzeichnet wurde (grüne Versicherungskarte), haben sich 17 europäische Länder darüber geeinigt, in einem Kfz-Schadensfall Daten ins Ausland weiterzugeben. Ziel dieses Verfahrens ist es, die Durchsetzung von

Schadensersatzansprüchen auch im europäischen Ausland zu gewährleisten.

Dieses Ziel ist grundsätzlich zu begrüßen. Dennoch sind mit der Versicherungswirtschaft Gespräche darüber aufzunehmen, wie der nach dem BDSG datenschutzrechtlich unbedenkliche Umgang mit den Daten der Versicherten im Ausland gewährleistet werden kann.

25.7 Schweigepflicht-Entbindungsklauseln in Schadensfällen

Im Berichtszeitraum haben sich die Datenschutz-Aufsichtsbehörden und das Bundesaufsichtsamt für das Versicherungswesen weiterhin bemüht, die Schweigepflicht-Entbindungsklauseln mit den Verbänden abzustimmen. Dabei geht es um die Klauseln, die in Schadensfällen bei der Haftpflicht-, der Reiserücktrittskosten-, der Berufsunfähigkeits- und Pflegeversicherung von den Versicherten selbst oder von sonstigen Anspruchstellern zu unterzeichnen sind.

Ein erfolgreicher Abschluß ist nur dann zu erzielen, wenn die Schweigepflicht-Entbindung nicht weiter gefaßt wird, als es für die Aufgaben der Versicherungsgesellschaften unbedingt erforderlich ist. Ein Versicherungsunternehmen muß im Schadensfall überprüfen können, ob die geltend gemachten Beträge tatsächlich auf dem Schadensfall beruhen. Das Abfordern von darüber hinausgehenden Informationen kann für den übermittelnden Arzt eine strafbare Verletzung der Schweigepflicht (§ 203 StGB) bedeuten.

25.7.1 Haftpflicht-Versicherung

Der GDV legte den Datenschutz-Aufsichtsbehörden einen eigenen Textentwurf vor, der in dieser Form nicht übernommen werden konnte. Der Grund lag darin, daß zum einen die Freiwilligkeit der Abgabe dieser Erklärung nicht deutlich wurde und zum anderen die Zweckbindung der Schweigepflicht-Entbindungserklärung nicht zum Ausdruck kam. Statt dessen wurde folgender Textvorschlag gemacht:

> „Der Versicherer hat mir mitgeteilt, daß er zur Beurteilung des von mir geltend gemachten Schadensersatzanspruchs die Überprüfung von Angaben für erforderlich hält, die ich zur Begründung meines Anspruchs gemacht habe. Zu diesem Zweck befreie ich freiwillig Ärzte, Zahnärzte und Angehörige anderer Heilberufe sowie Bedienstete von Krankenanstalten und Behörden, die an der Heilbehandlung beteiligt waren, von ihrer Schweigepflicht, und zwar auch über meinen Tod hinaus."

Der GDV hat sich mit dieser Formulierung einverstanden erklärt.

25.7.2 Reise-Rücktrittskosten-Versicherung

Die Verhandlungen über eine einheitliche Schweigepflicht-Entbindungsklausel im Schadensfall bei der Reise-Rücktrittskosten-Versicherung wurden fortgesetzt.

Der bereits mit dem Bundesaufsichtsamt abgestimmte Vorschlag der Aufsichtsbehörden stieß insbesondere deshalb auf Kritik des Deutschen Transportversicherer-Verbandes (DTV), weil ihm die darin genannte Frist für die Überprüfung von Vorerkrankungen von einem Jahr für bestimmte Krankheitsarten zu kurz erschien. Die Aufsichtsbehörden hatten daraufhin vorgeschlagen, daß es grundsätzlich bei der einjährigen Überprüfungsfrist bleiben soll, während die Frist für langwierige oder wiederkehrende Krankheiten zwei Jahre betragen kann.

Der DTV hat einen überarbeiteten Entwurf vorgelegt, der auf Anregung der Aufsichtsbehörde noch konkretisiert werden soll.

25.7.3 Berufsunfähigkeits- und Pflegerentenversicherung

Die Texte zur Schweigepflicht-Entbindungserklärung in der Berufsunfähigkeits- und Pflegerentenversicherung, auf die sich die Aufsichtsbehörden und das Bundesaufsichtsamt für das Versicherungswesen (BAV) geeinigt hatten, sind mittlerweile nach Anhörung des Verbandes der Lebensversicherungs-Unternehmen vom vorgenannten Aufsichtsamt genehmigt, als geschäftsplanmäßige Erklärungen im Veröffentlichungsblatt des BAV bekannt gemacht worden und werden von den Versicherern bereits genutzt.

26. Handels- und Wirtschaftsauskunfteien

26.1 Aufzeichnung und Kontrolle des berechtigten Interesses an einer Auskunft

Auch nach Novellierung das Bundesdatenschutzgesetzes sind gemäß § 29 Abs. 2 Satz 3 BDSG Auskunfteien weiterhin verpflichtet, bei jeder erteilten Auskunft die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung aufzuzeichnen.

Im 9. TB (5.4.1) wurde dargestellt, welche Probleme bei der Kontrolle des berechtigten Interesses bestehen. Die Aufsichtsbehörden und die Vertreter der Handels- und Wirtschaftsauskunfteien haben sich seitdem zu einem weiteren Gespräch getroffen, in dem die Auskunfteien sich bereit erklärten, eine qualitative und quantitative Veränderung des Kontrollverfahrens zu überprüfen.

Zur qualitativen Verbesserung wird durch die Handels- und Wirtschaftsauskunfteien die Einführung eines von den Aufsichtsbehörden beispielhaft vorgeschlagenen neuen Formulars für Anfragen erörtert, in dem entweder eine kurze, präzise Umschreibung des der Auskunft zugrunde liegenden Vorganges oder die Vorlage eines entsprechenden zentralen Dokumentes als Nachweis für das Vorhandensein eines berechtigten Interesses verlangt werden soll.

Als quantitative Verbesserung prüfen die Handels- und Wirtschaftsauskunfteien, den bisherigen Satz auf 2 Promille für die Kontrollen zu verdoppeln und unabhängig davon die Stichproben auf die absolute Mindestzahl von 12 im Jahr

festzulegen. Darüber hinaus sollen die Kontrollen nicht am Ende eines Quartals oder Jahres stattfinden, sondern im Sinne einer ständigen Kontrolle auf die Zeiträume gleichmäßiger verteilt werden.

26.2 Grenzüberschreitender Datenverkehr

Das Problem der Datenübermittlung ins Ausland kann zur Zeit nur dadurch gelöst werden, daß die übermittelnde Stelle den Datenempfänger im Wege zivilrechtlicher Vereinbarungen dazu verpflichtet, den Standard des Datenschutzes im Sinne der übermittelnden Stelle zu gestalten. Die Vertreter der Handels- und Wirtschaftsauskunfteien wollen trotz ihrer früher geäußerten Bedenken das Vertragsmodell erneut rechtlich prüfen.

Die Aufsichtsbehörden schlugen vor, folgende Elemente in das Vertragsmodell einzubeziehen:

— keine Weitergabe an Dritte,

— Zweckbindung,

— Datensicherung,

— Kontrolle durch die jeweilige Auskunftei beim auswärtigen Vertragspartner,

— Löschung, Sperrung, Berichtigung entweder über die datenexportierende Stelle oder durch den Datenimporteur im Ausland selbst,

— Schadensersatz zugunsten des Betroffenen oder Vertragsstrafe.

Die Aufsichtsbehörden begrüßen, daß die Auskunfteien Überlegungen in dieser Richtung anstellen, und bieten ihre Unterstützung an. Die Auskunfteien wollen sich untereinander abstimmen und voraussichtlich bis Ende 1991 eine Stellungnahme, gegebenenfalls mit Vorschlägen für ein Vertragsmodell, vorlegen.

27. Private bundesweite Schuldnerverzeichnisse

Der im 9. TB (4.14.1.4 und 5.6) kritisierte Gesetzentwurf der Bundesregierung zur Regelung der Auskünfte aus dem Schuldnerverzeichnis – §§ 915 bis 915 i ZPO – wurde in der vergangenen Legislaturperiode nicht mehr verabschiedet. Der Gesetzentwurf war vor allem kritisiert worden, weil eine ausdrückliche Regelung fehlte, ob und ggf. unter welchen restriktiven Bedingungen bundesweite zentrale Schuldnerverzeichnisse durch Private erstellt werden dürfen. Ferner war die eindeutige Identifizierbarkeit der Person, über die Daten gespeichert werden, nicht hinreichend sichergestellt. Ein weiterer Mangel des Gesetzentwurfes bestand darin, daß die Aufsichtsbehörde keine besonderen Kontrollbefugnisse erhalten soll, die Verwendung der Informationen aus dem Schuldnerverzeichnis zu überprüfen.

Auch der Bundesrat in seiner Stellungnahme zu dem Gesetzentwurf und der Bundesbeauftragte für den Datenschutz waren der Auffassung, daß diese Mängel unbedingt behoben werden müßten. Dennoch hat die Bundesregierung den Gesetzentwurf in unveränderter Fassung neu eingebracht. Die Frage nach der Zulässigkeit privater bundesweiter Schuldnerverzeichnisse ist daher weiterhin ungeklärt (siehe auch unter 19.1.2).

Trotz des fortgeschrittenen Standes des Gesetzgebungsverfahrens streben wir an, noch Einfluß auf die weitere Beratung des Gesetzes zu nehmen, um die datenschutzrechtlich gebotenen Regelungen zu erreichen. Hinsichtlich der – insbesondere von uns angeregten – anlaßfreien Kontrollbefugnis der Aufsichtsbehörde hat der Bundesminister der Justiz inzwischen keine Einwände mehr geäußert, so daß hier auf eine Änderung zu hoffen ist.

In unserem Zuständigkeitsbereich gibt es bislang noch kein privates Unternehmen, das über ein funktionierendes bundesweites privates Schuldnerverzeichnis verfügt und hieraus Auskünfte erteilt. Das im 9. TB (5.6) erwähnte Unternehmen, das an der Errichtung eines solchen Verzeichnisses festhalten wollte, hat uns anläßlich einer Eingabe im August mitgeteilt, daß es derzeit noch keinerlei Anfragen zu Eintragungen aus dem Schuldnerverzeichnis beantwortet. Die Existenz einer Auskunftei in einem anderen Bundesland, die bereits Auskünfte aus einem bundesweiten Register erteilt, ist den Aufsichtsbehörden allerdings bekannt; es liegen Hinweise dafür vor, daß weitere Unternehmen Interesse am Aufbau eines privaten zentralen Schuldnerregisters haben.

Der Präsident des Amtsgerichts Hamburg lehnt zur Zeit neu eingehende Anträge auf Erteilung von Abschriften des Schuldnerregisters in Einklang mit der von uns vertretenen Rechtsauffassung ab. Die endgültige Verfahrensweise kann erst nach der gesetzlichen Neuregelung festgelegt werden.

28. Arbeitnehmerdatenschutz

28.1 Medizinische Eignungsuntersuchungen

Eine Zuschrift des Bremer Datenschutzbeauftragten machte uns auf datenschutzrechtliche Probleme bei den Eignungsuntersuchungen von Bewerbern durch niedergelassene Ärzte aufmerksam. Hierbei ging es insbesondere um den Umfang der Untersuchung und die Übermittlung an den zukünftigen Arbeitgeber.

Eine entsprechende Anfrage bei der Landesvereinigung der Arbeitgeberverbände und bei der Ärztekammer Hamburg ergab ein uneinheitliches Bild: Während die Arbeitgebervereinigung über keine brauchbaren Informationen verfügt, führte die Ärztekammer eine Umfrage beim Hartmann-Bund, dem Berufsverband der praktischen Ärzte und Ärzte für Allgemein-Medizin und beim Verband Deutscher Betriebs- und Werksärzte e.V. durch.

Während die ersten beiden Verbände mit einer derartigen Fragestellung bisher nicht konfrontiert worden waren, stellte der Verband der Betriebsärzte fest, daß alle Eignungsuntersuchungen der Schweigepflicht unterliegen und dem

zukünftigen Arbeitgeber nur die Ergebnisse der Untersuchung mitgeteilt werden. In keinem Falle würden Anamnesedaten und/oder Untersuchungsbefunde einer Firma mitgeteilt, wenn nicht eine Entbindung von der ärztlichen Schweigepflicht vorliegt.

In einem Schreiben an die Ärztekammer und die Ärzteverbände in Hamburg wurden daraufhin folgende datenschutzrechtliche Leitlinien für medizinische Eignungsuntersuchungen formuliert:

— Arbeitsplatz-Bewerber sollten nur so viel über ihren Gesundheitsstatus offenbaren müssen, wie es das legitime Interesse des Arbeitgebers an einer vertrags- und ordnungsgemäßen Erfüllung der jeweiligen Arbeitsplatzanforderungen verlangt.

— Die medizinische Untersuchung sollte deswegen auf diesen Zweck beschränkt bleiben, was eine Information des Arztes über den Anlaß der Untersuchung und die Art des Arbeitsplatzes voraussetzt.

— Da in Bewerbungssituationen kaum von einer wirklich freiwilligen Einwilligung in die Preisgabe persönlicher Daten ausgegangen werden kann, sollten allgemeine Schweigepflicht-Entbindungserklärungen prinzipiell nicht verlangt werden. Sie kommen allenfalls bezüglich spezifischer arbeitsplatzrelevanter Krankheiten in Betracht, müssen auf den konkreten Zweck beschränkt sein und den jeweiligen von der Schweigepflicht zu entbindenden Arzt benennen.

— Stellt sich bei der ärztlichen Untersuchung heraus, daß der Bewerber für den in Aussicht genommenen Arbeitsplatz gesundheitlich ungeeignet oder nur beschränkt geeignet ist, verlangt das Grundrecht auf informationelle Selbstbestimmung, daß dies zunächst dem Bewerber selbst mitgeteilt wird und er die Möglichkeit erhält, eine Datenübermittlung an den Arbeitgeber durch eine Rücknahme seiner Bewerbung zu vermeiden.

— Alle in der ärztlichen Untersuchung erhobenen Befunde und Daten unterliegen der ärztlichen Schweigepflicht. Eine Übermittlung dieser sensiblen Daten an den zukünftigen Arbeitgeber ist nicht erforderlich. Ausreichend – und damit allein zulässig – ist nur die Mitteilung des Endergebnisses der Untersuchung („geeignet", „nicht geeignet"). Bei „bedingter Eignung" können entscheidende Einschränkungen (z.B.: nicht schwer heben, Schutzbrille tragen) bzw. Empfehlungen für den Arbeitsplatz und die Arbeitsgestaltung übermittelt werden. Dazu ist die Angabe der Diagnose in aller Regel ebensowenig erforderlich wie die Mitteilung von Randbemerkungen über Übergewichtigkeit, Rauchgewohnheiten oder ähnliches. Da solche weitergehenden Datenübermittlungen an den Arbeitgeber nicht nötig sind, kommt auch eine darüber hinausgehende – ohnehin kaum freiwillige – Schweigepflicht-Entbindung durch den Bewerber nicht in Betracht.

— Die ärztlichen Unterlagen der Bewerberuntersuchung dürfen nicht für andere Zwecke verwendet und nicht mit anderen Unterlagen vermischt werden. Sie müssen dem Untersuchten zur Einsicht zur Verfügung stehen und grundsätzlich innerhalb eines überschaubaren Zeitraumes vernichtet bzw. dem Betroffenen ausgehändigt werden, wenn ihre Aufbewahrung nicht mehr erforderlich ist.

Die Ärztekammer kündigte an, dem Anliegen des Hamburgischen Datenschutzbeauftragten durch eine Veröffentlichung im Hamburger Ärzteblatt Rechnung zu tragen. Die Forderung nach einer Löschung innerhalb eines überschaubaren Zeitraums widerspreche jedoch der 10-jährigen Dokumentationspflicht eines jeden Arztes.

Hierzu vertreten wir die Auffassung, daß sich die Dokumentationspflicht nur auf Behandlungsunterlagen bezieht, nicht aber auf Eignungsuntersuchungen, die keine Krankheitssymptome zum Anlaß haben. So heißt es im § 28 Abs. 5 HmbDSG für den öffentlichen Bereich ganz allgemein: „Personenbezogene Daten" – also auch medizinische Daten –, „die vor der Eingehung eines Beschäftigungsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, daß ein Beschäftigungsverhältnis nicht zustande kommt". Da die Untersuchungsunterlagen den für die Bewerberauswahl notwendigen Unterlagen zuzuordnen sind, müssen sie nach unserer Auffassung jedenfalls bei einer Einstellungs-Ablehnung unverzüglich gelöscht bzw. an den Bewerber ausgehändigt werden.

Die vorstehende Rechtsauffassung wurde auch den anderen Datenschutzbeauftragten des Bundes und der Länder sowie den Aufsichtsbehörden für den nicht-öffentlichen Bereich zur Kenntnis gegeben. Hinsichtlich der Bewerber für den öffentlichen Dienst haben die Datenschutzbeauftragten inzwischen in einer Entschließung vom September 1991 entsprechende Anforderungen an die ärztliche Untersuchung formuliert.

28.2 Psycho-Tests bei der Bewerberauswahl

Im Rahmen der Auseinandersetzung um die Scientology-Church erhielten wir Unterlagen einer Personalberatungsfirma, die Anlaß boten für weitere Nachforschungen. Ein Hamburger Unternehmen bediente sich des folgenden Auswahlverfahrens dieser Personalberatungsfirma: Der Arbeitgeber prüft die fachliche Qualifikation eines Bewerbers und legt ihm dann Persönlichkeits-Fragebogen der Beratungsfirma vor. Diese bestehen aus 200 zum Teil sehr persönlichen Fragen wie z. B.: „Wird Ihr Urteil durch Ihre Gefühle stark beeinflußt?", „Sind Sie für Rassentrennung und Klassenunterschiede?", „Grübeln Sie oft über Tod, Krankheit, Schmerz und Kummer nach?".

Der gesamte Fragenkatalog entspricht dem Persönlichkeitstest, den die Scientology-Church für ihre Mitglieder verwendet. Der Bewerber hat bei jeder Frage zwischen ja/unsicher/nein zu entscheiden und ein entsprechendes Kästchen anzukreuzen. Auf einem gesonderten Bogen vermerkt der Arbeitgeber den Namen der Firma, das Datum, die Stellenbezeichnung sowie das Geschlecht

und das Alter über oder unter 18 Jahre des Bewerbers, nicht aber seinen Namen. Alle Antworten sowie die letztgenannten Angaben werden vom Arbeitgeber kopiert und an die Personalberatungsfirma übersandt. Diese wertet die Daten elektronisch aus, teilt das Ergebnis dem Arbeitgeber mit und berät ihn ggf. in einem persönlichen Gespräch.

Datenschutzrechtlich sind insbesondere zwei Bereiche bedenklich:

— Zum einen erhält der Arbeitgeber, bei dem die ausgefüllten Fragebogen verbleiben, die Antworten auf Fragen, die über das von der Rechtsprechung umrissene „Fragerecht des Arbeitgebers" weit hinausgehen. Zusätzlich zu den Antworten auf zum Teil intime Einzelfragen enthält die Auswertung der Personalberatungsfirma ein umfassendes Persönlichkeitsprofil des Bewerbers. Auf einer Liste mit 10 Merkmalen („stabil/labil", „glücklich/unglücklich" „verständnisvoll", usw.) wird ein Durchschnittswert einer Skala von minus 10 bis plus 10 eingetragen. Ergänzt wird die Tabelle durch eine „detaillierte Beschreibung der Eigenschaften" und eine Empfehlung für die Stellenbesetzung. Der Test wird für alle Bewerber unabhängig vom Fachgebiet, von der Hierarchiestufe und von bestimmten Aufgaben in gleicher Weise verwendet. Er ist ein allgemeiner psychologischer Persönlichkeitstest, der weder auf besondere Anforderungen des zu besetzenden Arbeitsplatzes Rücksicht nimmt, noch wissenschaftlich anerkannt ist. Der Bewerber hat in der Regel keine Vorstellung davon, was bzw. welche Eigenschaften mit dem Fragebogen getestet werden. Damit verstößt der Test gegen das Persönlichkeitsrecht, wie es das Bundesverfassungsgericht etwa im sog. Mikrozensus-Urteil näher konkretisiert hat.

— Zum anderen besteht die Gefahr, daß das Personalberatungsunternehmen auch ohne Angabe des Bewerbernamens eine Reidentifikation vornehmen kann. Durch die Vertragsbeziehung mit dem Arbeitgeber einerseits und die Übermittlung der zu besetzenden Stelle, des Alters (unter/über 18) und des Geschlechts andererseits wird es bei entsprechendem Einsatz leicht möglich sein, durch einen Anruf beim Arbeitgeber oder beim (neuen) Inhaber der zu besetzenden Stelle selbst den Namen des Betroffenen zu ermitteln. Es ist zudem sehr wahrscheinlich, daß die mit dem höchsten Wert empfohlene Person auch tatsächlich vom Arbeitgeber für die Stelle ausgewählt wurde. So können die Testergebnisse und die ausgewählte Person unschwer miteinander verknüpft werden.

28.3 Datenübermittlung bei waffenführenden Arbeitnehmern

Im 9. TB (5.7.3) wurde berichtet, wie Bewerber für ein Wach- und Sicherheitsunternehmen auf ihre Zuverlässigkeit überprüft werden. Dabei wurde vor allem kritisiert, daß Erkenntnisse des Landeskriminalamtes über das Wirtschafts- und Ordnungsamt direkt dem Arbeitgeber zugehen, ohne daß der Bewerber von dem Inhalt der Mitteilung Kenntnis erhält. Gegen eine dem Bewerber abverlangte Einwilligungserklärung wurden Bedenken wegen mangelnder Freiwilligkeit geäußert.

Inzwischen hat die Behörde für Inneres den Wirtschafts- und Ordnungsämtern empfohlen, bei sicherheitsrelevanten Erkenntnissen zuvor den Bewerber selbst anzuhören und ihm Gelegenheit zu geben, die Bewerbung und den Antrag auf Erteilung eines Waffenscheines zurückzunehmen. Einzel-Erkenntnisse sollten dem Arbeitgeber in keinem Falle mitgeteilt werden. Hinsichtlich der Übermittlung von der Polizei an das Wirtschafts- und Ordnungsamt beruft sich die Behörde für Inneres mangels bereichsspezifischer Rechtsgrundlage nach wie vor auf den sog. Übergangsbonus, beschränkt die Mitteilung ggf. jedoch auf die Bemerkung: „Es bestehen Zuverlässigkeitsbedenken".

Diese allgemeine Formulierung hat jedoch den Nachteil, daß der Betroffene dagegen keine substantiellen Einwände geltend machen und fehlerhafte Speicherungen nicht erkennen und ggf. berichtigen lassen kann. In jedem Falle ist eine bereichsspezifische Ermächtigung für eine aussagekräftige Übermittlung von der Polizei an das Wirtschafts- und Ordnungsamt anzustreben, wie sie die Behörde für Inneres nach eigenen Angaben auch betreibt.

In dem konkreten, im 9. TB wiedergegebenen Fall konnte inzwischen eine erhebliche Verbesserung des vom Sicherheitsunternehmen verwendeten Bewerberfragebogens erreicht werden, so daß etwa Fragen nach der Gewerkschaftsmitgliedschaft oder der Religionszugehörigkeit ebenso entfallen sind wie Fragen zum Verkehrsmittel für den Arbeitsweg oder zum Gläubiger eventueller Schulden.

29. Sonstige Probleme aus dem nicht-öffentlichen Bereich

29.1 Rechtsanwaltspraxen, insbesondere Mahnverfahren

Im vergangenen Berichtszeitraum beschäftigten sich einige Eingaben mit dem Umgang mit personenbezogenen Daten bei Rechtsanwälten:

In einem Fall wurden etwa 10 Jahre alte Unterlagen über zivilrechtliche Auseinandersetzungen, Verkehrsordnungswidrigkeiten-, Strafermittlungs- und Mahnverfahren in einem allgemein zugänglichen Müllbehälter gefunden und uns zur Rückgabe ausgehändigt.

In einem weiteren Fall wurde in einem Mahnverfahren dem Gericht zum Beweis einer bestehenden Schuld eine mehrere Seiten umfassende Liste mit offenen Salden eingereicht, die zusätzlich viele andere Schuldner namentlich auswies. Mit der Kopie des Schriftsatzes erhielt der vom Verfahren betroffene Schuldner Kenntnis von Daten, die keineswegs für ihn bestimmt waren. Unsere Intervention wurde von dem betroffenen Anwalt bereitwillig zum Anlaß genommen, die Verfahrensweise zu ändern und dem Datenschutz in der Kanzlei zukünftig besondere Aufmerksamkeit zu widmen.

Als ein mehr generelles Problem wurde die Frage aufgeworfen, ob das Versenden von Mahnungen durch einen Anwalt als nicht verschlossene Briefdrucksa-

che dem heutigen Verständnis von Datenschutz noch entspricht. Hierüber sind wir u.a. auch mit der Hanseatischen Rechtsanwaltskammer im Gespräch.

Kritisiert wurde schließlich ein Fragebogen, den eine von einem Inkasso-Dienst eingeschaltete Kanzlei an den Schuldner versendet und in dem sie ihn auffordert, detaillierte Informationen über seine Einkommens- und Vermögenslage anzugeben. Ähnliche Angaben wurden darin für den „Lebensgefährten" vorgesehen. In der Erörterung mit der Kanzlei und insbesondere mit dem Inkasso-Unternehmen wurde festgestellt, daß von den mit dem Fragebogen erhobenen Daten nur einige bestimmte bei der Inkassostelle gespeichert werden und die übrigen Angaben mit dem Fragebogen in einer Akte abgeheftet werden. Mit dem „Lebensgefährten" sollten nur solche Partner befragt werden, die hinsichtlich der Forderung tatsächlich Mitschuldner waren. Das betroffene Inkasso-Unternehmen zeigte sich in einem konstruktiven Gespräch bereit, den Bedenken durch das Einführen eines neuen Fragebogens Rechnung zu tragen. Es war bereit, durch – mit der beauftragten Kanzlei abgestimmte – Schreiben nach Möglichkeit noch transparenter zu machen, welche Angaben des Schuldners bei welcher Stelle verbleiben. Der inzwischen vorliegende verbesserte Fragebogen macht u. a. die Freiwilligkeit der Angaben deutlich und gibt an, welche Daten gespeichert werden.

Diese Einzelfälle zeigen, daß der Datenschutz – teils aus Versehen im Einzelfall, teils aber auch, weil die notwendige Sensibilität fehlt – auch bei Rechtsanwälten hin und wieder Lücken aufweist. Sie zeigen aber auch eine zunehmende Kooperationsbereitschaft bei der Beseitigung der Beanstandungen.

29.2 Taxi-Auftrags-Verfahren

Nachdem die Aufsichtsbehörde durch eine Beschwerde von einem neuen Verfahren einer Taxen-Zentrale zur Auftragsvermittlung erfuhr, wurden genauere Informationen eingeholt.

Eine Petentin hatte beobachtet, daß ihr Name, die Abfahrt-Adresse und ihr Zusatzwunsch nach besonderen Ortskenntnissen auf einer Anzeige im Taxi sichtbar war. Sie vermutete eine dauerhafte und unzulässige Speicherung und eine später mögliche Auswertung dieser Angaben.

Der Besuch der Taxen-Zentrale führte zu folgendem Ergebnis:

Bei einem Anruf werden durch eine Telefonistin der Name des Kunden und seine Abholadresse in den Zentralrechner aufgenommen. In Einzelfällen kommen Sonderwünsche des Kunden oder die Zieladresse hinzu. Die Taxis dieser Zentrale sind mit einem besonderen Ortungsgerät ausgestattet, so daß der Rechner die Auftragsdaten an dasjenige Fahrzeug sendet, das sich in der Nähe des Anforderungsortes aufhält. Über eine Anzeige am Armaturenbrett erhält nur dieser eine Fahrer Kenntnis von dem Auftrag und den hierfür notwendigen Daten. Der Datensatz bleibt nur so lange auf der Anzeige lesbar, bis ein

Folgeauftrag eingeht und den alten überschreibt. Im Zentralrechner bleiben die jeweiligen Auftragsdaten nur etwa eine Woche lang gespeichert, um eventuelle Kundenanfragen bezüglich verlorengeganger Gegenstände, nachträgliche Bitten um Belege oder Reklamationen bearbeiten zu können.

Der festgestellte Umgang mit den Kundendaten begegnet keinen rechtlichen Bedenken.

§ 28 Abs.1 Nr.1 BDSG gestattet eine Verarbeitung im Rahmen der Zweckbestimmung eines mit dem Betroffenen geschlossenen Vertrages. Die Speicherung und Weitergabe der Auftragsdaten an den ausführenden Fahrer dient gerade dem Zweck der Abwicklung des Beförderungsvertrages.

Auch die Bearbeitung von späteren Anfragen der Kunden ist noch als im Rahmen des Vertragsverhältnisses erfolgend anzusehen, da es sich um einen Service im Interesse des Kunden handelt. Die Speicherung in der Zentrale nach der direkten Abwicklung des Fahrauftrages kann zusätzlich damit begründet werden, daß sie auch der Freihaltung gegenüber möglichen Schadensersatzansprüchen dienen kann. Aus diesem Grund ist die kurzfristige Speicherung von einer Woche durchaus noch erforderlich und deshalb auch zulässig.

Darüber hinaus wird das System auch eingesetzt, um Stammkunden mit einer festen Kundennummer auszustatten und bedienen zu können.

Unter dieser Nummer werden Name und eine feste Abholadresse des Kunden (üblicherweise seine Wohn- oder Geschäftsanschrift) gespeichert. Hierüber erhält er eine schriftliche Mitteilung von der Taxenzentrale. Bei der Anforderung eines Wagens gibt der Kunde in diesem Falle nur noch seine Kundennummer durch. Die den Auftrag entgegennehmende Telefonistin bestätigt die Richtigkeit der Kundennummer durch Nennung des Namens, der unter der jeweiligen Nummer gespeichert ist, und fragt evtl. auch nach, wohin das Taxi kommen soll. Die weitere Auftragsabwicklung unterscheidet sich nicht von der bei Einzelkunden.

Für dieses Verfahren gelten dieselben Erwägungen wie bei der Beurteilung der einwöchigen Speicherung der Auftragsdaten von Einzelkunden. Es ist rechtlich insbesondere deshalb unbedenklich, weil die längerfristige Speicherung gerade dem Zweck des zwischen der Taxen-Zentrale und dem Kunden bestehenden Vertrages entspricht.

Abschließend bleibt festzustellen, daß dieses Verfahren der Auftragsvermittlung auch aus datenschutzrechtlicher Sicht eine Reihe von Vorteilen bietet. Die Kundendaten sind beim Fahrer und bei der Zentrale nur für eine begrenzte Zeit verfügbar und unterliegen einer sehr eingeschränkten Zugriffsmöglichkeit. Darüber hinaus wird der einzelne Auftrag nicht mehr im Sprechfunk allen Fahrern dieser Zentrale zum Anhören angeboten, sondern wird nur einem einzigen – der dem Abholort am nächsten ist – zugewiesen. Ein zufälliges Mithören durch Kunden in anderen Fahrzeugen ist damit ausgeschlossen. Das neue Verfahren, das zunächst Anlaß zu näherer Prüfung gab, hat sich demnach als durchaus datenschutzfreundlich erwiesen.

Geschäftsverteilung (Stand: 1. Dezember 1991)

Der Hamburgische Datenschutzbeauftragte
Baumwall 7, 2000 Hamburg 11

Tel.: 040/3504–2045
BN: 9.41–2045
Fax: 040/3504–2372

		Durchwahl
Dienststellenleiter:	Dr. Hans-Hermann Schrader	D –2044–
Stellvertreter:	Dr. Hans-Albert Lennartz	D 2 –2046–
Stellvertreter IuK- und Datenschutztechnik:	Peter Schaar	–2231–
Vorzimmer:	Eva-Maria Reupke	–3045–

D 1 – Geschäftsstelle

		Durchwahl
Leiter:	Detlef Malessa	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
Bibliothek
Register nach § 24 HmbDSG
Bearbeitung von Eingaben
Senats-/Bürgerschaftsdrucksachen

D 11: Vorzimmerdienst
Textverarbeitung
Eingabenverwaltung

D 12: PC-Textverarbeitung
Registratur
Postverteilung

D 2 – Referat

		Durchwahl
Leiter:	Dr. Hans-Albert Lennartz	D 2 –2046–
Referent:	Ulrich Werner	D 20 –2581–
Sachbearbeiter:	Detlef Malessa	D 21 –2223–

D 2: Grundsatzfragen des Datenschutzes
Novellierung der Datenschutzgesetze
Verfassungsschutz
Justizverwaltung
Staatsanwaltschaft
Strafvollzug
Ausbildungsleiter für die Juristenausbildung

D 20: 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–
Referentin:	Veronica Matusall	D 31 –2564–
Sachbearbeiter:	Dietmar Nadler	D 32 –2236–

D 3: Telekommunikation
Online-Datenbanken
IuK-Gesamtplan
technische Assistenz für die Bereiche
— Polizei/Meldewesen
— Verfassungsschutz
— Justiz
— Wissenschaft und Forschung
— Kultur
datenschutzrechtliche Betreuung der Bereiche
— Statistik
— Wahlen
— Medien

D 30: LAN
MS-DOS
Host-PC-Kopplung
Ec-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
— Wirtschaft
datenschutzrechtliche Betreuung des Bereichs Umweltschutz

D 32: Richtlinien zur Datensicherung und Datenverarbeitung
Speichertechnik
BS 2000/MVS
IBM 138/AS 400
technische Assistenz für die Bereiche
— Bauwesen
— Personalwesen
datenschutzrechtliche Betreuung der Bereiche
— Finanzen
— Organisation
— Bürgerschaft

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–
	Dr. Ulrike-Paffrath-Pfeuffer	D 6-2	–2541–
Sachbearbeiter:	Bernhard-Schmidtke	D 61	–2468–

Aufsichtsbehörde nach § 38 Bundesdatenschutzgesetz

D 6-1: Versicherungswirtschaft einschließlich Wahrnehmung des Vorsitzes im Arbeitskreis Versicherungswirtschaft
Bauen und Wohnen, insbesondere Mietangelegenheiten
Transport und Verkehr einschließlich HVV
Handel, Industrie, gewerbliche Dienstleistungen und freie Berufe

D 6-2: Auskunfteien, Wirtschafts- und Handelsauskunfteien
SCHUFA
Markt- und Meinungsforschung
Kreditwirtschaft
Versandhandel
Werbung
Adreßhandel
Datenbankbetreiber, Mailboxen und Netzanbieter
Grenzüberschreitender Datenverkehr im öffentlichen und nicht-öffentlichen Bereich, insbesondere Datenschutz der Europäischen Gemeinschaften

D 61: Beratung und Betreuung von Unternehmen, Vereinen, Verbänden usw. insbesondere bei Auftragsdatenverarbeitung, dem Bildschirmtext und der sonstigen Datenverarbeitung
Beratung von Bürgern und Bearbeitung von Eingaben insbesondere bei sonstigen Datenschutzangelegenheiten im nicht-öffentlichen Bereich

Stichwortverzeichnis