BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG

15. Wahlperiode

Drucksache **15/2691**

25.01.95

Der Hamburgische Datenschutzbeauftragte

An die
Frau Präsidentin der Bürgerschaft

Betr.: 13. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

Gemäß § 23 Hamburgisches Datenschutzgesetz übersende ich der Bürgerschaft den 13. Tätigkeitsbericht*.
Dem Senat teile ich den Tätigkeitsbericht gleichzeitig zu.

Dr. Schrader

* Verteilt nur an die Abgeordneten der Bürgerschaft

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

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

vorgelegt im Januar 1995
(Redaktionsschluß: 2. Dezember 1994)

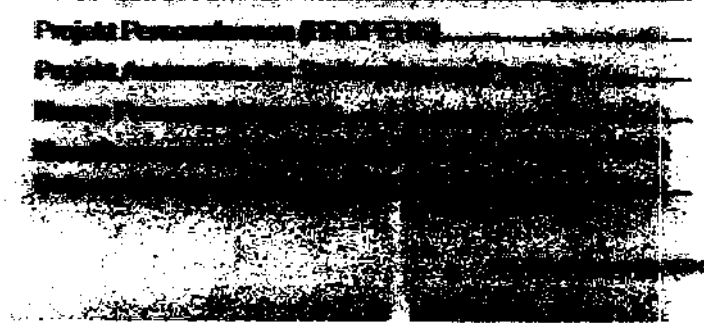
Dr. Hans-Hermann Schrader

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Baumwall 7 – 20459 Hamburg – Tel. 36 04 21
Auflage 1 000 Exemplare

Druck: Lütcke & Wulff, 20097 Hamburg

INHALTSVERZEICHNIS

Einzelne Probleme des Datenschutzes im öffentlichen Bereich



13. Tätigkeitsbericht 1994 HmbDSB

Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

Zusammenfassung wichtiger Punkte

Grundrecht auf Datenschutz Bei der Verfassungsreform ist die Chance nicht genutzt worden, das Grundrecht auf Datenschutz in das Grundgesetz aufzunehmen. Auch ohne eine Grundgesetzänderung könnten und sollten die jeweiligen Grundrechtseinschränkungen künftig in den Gesetzen ausdrücklich gekennzeichnet werden (1.1).

Hamburgübergreifende Datenverarbeitung Die Vernetzung in Verwaltung und Wirtschaft über Hamburg hinaus erhöht die Schwierigkeiten erheblich, für einen wirksamen Datenschutz zu sorgen. Es muß – auch bei der EG-Datenschutzrichtlinie – erreicht werden, daß regelmäßig das Recht am Ort desjenigen maßgeblich ist, der für die Datenverarbeitung verantwortlich ist; dort muß auch die Datenschutzkontrolle verbleiben (1.3).

Grundschutzkonzept Die hamburgische Verwaltung hat sich auf ein Grundschutzkonzept für die automatisierte Verarbeitung von Daten verständigt. Damit wurde eine wichtige Arbeitshilfe geschaffen (3.1).

X.25-Dienst und elektronische Post Bei der Nutzung der elektronischen Datenübertragung und der elektronischen Post in der hamburgischen Verwaltung müssen die Anwender selbst dafür sorgen, daß besonders sensible Daten verschlüsselt übertragen werden.Darüber hinaus ist sicherzustellen, daß Unberechtigte nicht über Netze auf gespeicherte vertrauliche Informationen zugreifen können (3.3 und 3.4).

Personalberichtswesen Beschäftigtendaten dürfen nur anonymisiert zu statistischen Auswertungen herangezogen werden.Die Anonymität ist in jedem Zeitpunkt des Verfahrens zu gewährleisten, insbesondere bei Langzeitstudien mit einer Fülle verschiedener Erhebungsmerkmale (7.6.2).

Ausländerzentralregister Angesichts der weitreichenden gesetzlichen Eingriffe, die das Gesetz über das Ausländerzentralregister enthält, sind künftig die verbleibenden Handlungsmöglichkeiten zum Schutz der Betroffenen voll wahrzunehmen (15.2).

Europol Das geplante Europol-Übereinkommen darf sich nicht über die datenschutzrechtliche Verantwortlichkeit der Länderpolizeien hinwegsetzen, die Daten im Europol-Informationssystem speichern (17.2).

Parlamentarischer Untersuchungsausschuß „Hamburger Polizei" Die personenbezogene Untersuchung muß sich auf solche Fälle beschränken, in denen hinreichende Anhaltspunkte dafür vorliegen, daß Polizeibeamte rechtswidrige Übergriffe zu verantworten haben (17.8).

Verfassungsschutzgesetz Im Vergleich zum Senatsentwurf darf die Novellierung des Gesetzes nicht zu einer Aufweichung der Trennung zwischen Poli-

[redacted] Verfassungsschutz und zu anderen Abschwächungen des Daten[redacted] (18.1).

[redacted]schutzprüfung Bei einer Querschnittsprüfung des Landesamtes für Verfassungsschutz, das seine Arbeitsweise auf automatisierte Verfah[redacted] wurden vielfach Verarbeitungen festgestellt, die mit dem Entwurf des neuen Hamburgischen Verfassungsschutzgesetzes unvereinbar sind (18.3).

Strafverfahrensänderungsgesetz Der Entwurf des Bundesrates für gesetzliche Regelungen zur Datenverarbeitung im Strafverfahren ist völlig unzulänglich. Er ist mit den Anforderungen des Bundesverfassungsgerichts an Datenschutzregelungen unvereinbar (19.1.2).

Zentralkartei der Staatsanwaltschaft Der Rückstand von etwa 40.000 Vorgängen über den Ausgang des jeweiligen Verfahrens gefährdet die Rechte einer großen Zahl von betroffenen Bürgern. Daraufhin ist eine förmliche Beanstandung nach § 25 HmbDSG wegen der datenschutzrechtlichen Mängel angekündigt worden, falls nicht unverzüglich für Abhilfe gesorgt wird (19.2.2).

AK St.Georg Eine Prüfung ergab Defizite bei der Patientenaufnahme und bei der Datensicherung in verschiedenen Bereichen. Es konnten entsprechende Verbesserungen erreicht werden (21.4).

Fernwartung UKE Bei der Fernwartung der Patientendaten der Intensivstation hat der Hersteller in San Diego/USA den unbeschränkten Zugriff auf diese sensiblen Daten; die Überwachung der Fernwartung durch das UKE ist unzureichend. Diese Mängel in der Datensicherheit werden nach § 25 HmbDSG förmlich beanstandet (21.7).

Neue Einwilligungsklausel bei Versicherungen Mit der Versicherungwirtschaft wurde eine neue Einwilligungsklausel nach dem Bundesdatenschutzgesetz erarbeitet. Diese „Allfinanzklausel" läßt dem Versicherungsnehmer die Wahlfreiheit hinsichtlich der Nutzung seiner Daten auch für Finanzdienstleistungen (23.4). Sie verpflichtet die Versicherungen zur Aushändigung des Merkblatts über die Datenverarbeitung (23.5).

Bargeldloser Fahrkartenverkauf Die Einführung des bargeldlosen Zahlungsverfahrens beim Hamburgischen Verkehrsverbund (HVV) darf nicht den „gläsernen Fahrgast" zur Folge haben. Deshalb soll der HVV Vorkehrungen treffen, um Bewegungsprofile auszuschließen (26.2.2).

1. Zur Lage des Datenschutzes

1.1 Grundrecht auf Datenschutz

Bei der Verfassungsreform ist die Chance nicht genutzt worden, das Grundrecht auf Datenschutz in das Grundgesetz aufzunehmen. Nach intensiven Beratungen hat es der Bundestag am 30. Juni 1994 in namentlicher Abstimmung mit Mehrheit abgelehnt, das Grundgesetz um einen Art. 2a über den Datenschutz zu ergänzen. Bei den abschließenden Entscheidungen von Bundestag und Bundesrat im September 1994 hat sich daran nichts geändert.

Nachdem ursprünglich durchaus bei allen Fraktionen Bereitschaft zu einer Grundgesetzergänzung bestand, sind die Gründe für die Ablehnung durch die Bundestagsmehrheit inzwischen deutlich geworden. Die beiden Vorsitzenden der Gemeinsamen Verfassungskommission, Prof. Dr. Scholz und Bürgermeister Dr. Voscherau, haben sich dazu geäußert.

Professor Scholz hat erklärt, daß der Datenschutz als ein „bloßer Ausschnitt" aus dem Persönlichkeitsrecht nicht mit einem eigenen Grundgesetzartikel verselbständigt werden sollte, weil sonst „zugunsten des Datenschutzes ein massives Ungleichgewicht" hätte entstehen können. Demnach sollte dieses Grundrecht nicht noch zusätzlich im Grundgesetz verstärkt werden, auch wenn das Bundesverfassungsgericht ausdrücklich ein eigenständiges Grundrecht auf Datenschutz annimmt.

Bürgermeister Dr. Voscherau hat dies in der Bürgerschaft mit den Worten bestätigt: Das Grundrecht auf „Datenschutz in der Verfassung ... war für die konservative Seite nicht hinnehmbar. Warum nicht? Es läßt sich nur eine Antwort denken: Ist es erst drin, kann man es schwerer eine Nummer kleiner machen."

Ob diese Ablehnung auf Dauer bestehen bleiben wird, ist abzuwarten. Angesichts der Gefährdungen für den Datenschutz (siehe auch 1.2 und 12. TB, 1.1 und 1.2) wäre es eigentlich umgekehrt konsequent, wenn sich gerade diejenigen, die den Werteverlust beklagen, für eine Stärkung der informationellen Selbstbestimmung einsetzen würden.

Schon vor einer Grundgesetzergänzung könnten die Einschränkungen des Datenschutzes in Gesetzentwürfen künftig dadurch gekennzeichnet werden, daß eine Zitierklausel in den Gesetzestext aufgenommen wird. Sie könnte lauten: „Einschränkung von Grundrechten Durch dieses Gesetz wird das Grundrecht auf Datenschutz (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes) eingeschränkt."

Durch eine derartige Zitierklausel würden – zusammen mit der Begründung zu dieser Bestimmung – jeweils die Datenschutzeinschränkungen von Anfang an im Gesetzgebungsverfahren verdeutlicht werden. Dies entspricht gemäß den Aussagen des Bundesverfassungsgerichts dem eigentlichen Sinn des Zitier-

gebots nach Art. 19 GG, daß der Gesetzgeber die Grundrechtseinschränkung ausdrücklich offenlegt.

In diesem Sinne habe ich der Bürgerschaft ein Ersuchen an den Senat zum Grundrecht auf Datenschutz vorgeschlagen. Der Senat könnte dann ein solches Verfahren für die hamburgischen Gesetze einführen. Für die Bundesgesetze könnte er ein entsprechendes Verfahren durch eine Entschliessung des Bundesrates anstreben. Auch dies ist in meinem Vorschlag für ein Ersuchen an den Senat vorgesehen.

Derartige Vorkehrungen für die Gesetzgebung sind dringend geboten, um die zunehmenden gesetzlichen Einschränkungen des Datenschutzes für alle am Gesetzgebungsverfahren Beteiligten überprüfbar darzustellen. Sie können dann jeweils die Erforderlichkeit und Verhältnismäßigkeit der vorgesehenen Einschränkungen gezielt feststellen. Damit werden zwar – wie auch sonst durch das Zitiergebot – weitere Einschränkungen nicht von vornherein verhindert. Sie werden aber dadurch in geeigneter Weise zum Gegenstand der öffentlichen Auseinandersetzung.

Das Bundesverfassungsgericht hat dazu im sog. Fangschaltungsbeschluß vom 25. März 1992 ausgeführt: „Wenn das Grundgesetz die Einschränkung von grundrechtlichen Freiheiten und den Ausgleich zwischen kollidierenden Grundrechten dem Parlament vorbehält, so will es damit sichern, daß Entscheidungen von solcher Tragweite aus einem Verfahren hervorgehen, das der Öffentlichkeit Gelegenheit bietet, ihre Auffassungen auszubilden und zu vertreten, und die Volksvertretung anhält, Notwendigkeit und Ausmaß von Grundrechtseingriffen in öffentlicher Debatte zu klären."

In dieselbe Richtung geht der kürzliche Vorschlag für einen zusätzlichen Art. 19a der EG-Datenschutzrichtlinie. Danach haben die Mitgliedstaaten sicherzustellen, daß Datenverarbeitungen mit spezifischen Risiken für die Rechte und Freiheiten des einzelnen vor Beginn der Verarbeitung geprüft werden. Die Mitgliedstaaten können gemäß diesem Vorschlag „eine solche Prüfung auch im Zuge der Vorbereitung einer gesetzgeberischen Maßnahme des Parlaments durchführen, die die Verarbeitung erlaubt und geeignete Garantien festlegt."

Derartige verfahrensmäßige Verstärkungen des Grundrechtsschutzes sind gerade in der jetzigen Lage des Datenschutzes notwendig. Ich stimme dazu mit der Problemdarstellung überein, die Bundesverfassungsrichter Prof. Dr. Grimm nach der Datenschutzveranstaltung in Hamburg (12. TB, 1.8.2) auf dem Hessischen Forum Datenschutz gegeben hat.

Er hat einerseits hervorgehoben, daß das „Datenschutzgrundrecht" an der Spitze des Grundrechtskatalogs steht. Andererseits hat er darauf verwiesen, daß die grundrechtlichen Schutzpflichten insbesondere bei der Staatsaufgabe der inneren Sicherheit zunehmend zu Einschränkungen der Freiheitsrechte in der Gesetzgebung führen.

In diesem Zusammenhang hat er die besonderen Gefahren durch die Wende der Staatstätigkeit zur Prävention verdeutlicht. Im Präventionsstaat geht es darum, schon bloße Risiken nach Möglichkeit zu vermeiden; infolgedessen wächst der Informationsbedarf des Staates über persönliche Daten der Bürger gewaltig an. Dabei sei für den Staat im Interesse der Risikovermeidung „potentiell jedermann Störer".

Zugleich können die gesetzlichen Regelungen für breit angelegte Präventionsmaßnahmen kaum konkret gefaßt werden. Daher bleibt die Gesetzesausführung der Verwaltung ohne gesetzgeberische Steuerung und ohne wirksame gerichtliche Kontrolle.

Nach den Worten von Professor Grimm werden dadurch die Demokratie und auch der Rechtsstaat entwertet. Außerdem drohe der Verhältnismäßigkeitsgrundsatz zu sterben, wenn die Sicherheitsbedürfnisse als immens wichtig angesehen würden und dadurch bei der Abwägung der Freiheitsschutz auch für die informationelle Selbstbestimmung nicht mehr gewährt würde.

Diese durchaus dramatische Darstellung ist mit der zwischenzeitlichen Entwicklung in der Gesetzgebung bestätigt worden. Ein aktuelles Beispiel ist dafür das Verbrechensbekämpfungsgesetz, gegen das ich mich zusammen mit den anderen Datenschutzbeauftragten gewandt habe (siehe 1.2 und 18.4).

Umso mehr kommt es darauf an, gleichwohl die noch mögliche Freiheitssicherung in der Gesetzgebung zu erreichen. Als wichtigsten Punkt nennt Professor Grimm zu Recht das Bestimmtheitserfordernis, wonach die Grundrechtseinschränkungen im jeweiligen Gesetz „jeweils so bestimmt gehalten werden müssen, wie es der Gegenstand nur irgend zuläßt." Dagegen wird neuerdings zum Teil massiv verstoßen, wie die Kritik der Datenschutzbeauftragten insbesondere zum Länderentwurf für ein Strafverfahrensänderungsgesetz 1994 zeigt (siehe 19.1.2).

Wenn der Gesetzgeber im Bund und auch in Hamburg die vermeintlich notwendigen Einschränkungen der Freiheit weiter intensivieren sollte, verbleibt schließlich die Überprüfung der Verfassungsmäßigkeit durch das Bundesverfassungsgericht. Es wird anhand der anhängigen Verfahren – aus Hamburg zum Gesetz über die Datenverarbeitung der Polizei – ohnehin in absehbarer Zeit zu entscheiden haben, ob seine verfassungsrechtlichen Anforderungen gemäß dem Volkszählungsurteil noch beachtet werden.

1.2 Datenschutzentwicklung 10 Jahre nach dem Volkszählungsurteil

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer Sitzung im März 1994 in Potsdam eine „Bestandsaufnahme über die Situation des Datenschutzes – 10 Jahre nach dem Volkszählungsurteil" vorgelegt, die am Ende dieses Tätigkeitsberichts (TB) wiedergegeben ist. Die Datenschutzbeauftragten haben darin dargestellt, wie in der Informationsgesellschaft immer

weniger die Grundsätze des Volkszählungsurteils eingehalten werden. Insbesondere gerät zunehmend in Vergessenheit, daß die Einschränkung durch staatliche Regelungen nicht weiter gehen darf, als es zum Schutz öffentlicher Interessen unerläßlich ist.

Dabei sind diese Grundsätze des Datenschutzes keine Erfindung des Bundesverfassungsgerichts. Kürzlich ist vielmehr zu Recht darauf hingewiesen worden, daß 125 Jahre vor dem Volkszählungsurteil bereits Lorenz von Stein – als einer der großen Rechtsgelehrten des Konstitutionalismus – diese Grundsätze vertreten hat: „Der Staat hat nur das Recht, über diejenigen Lebensverhältnisse des Einzelnen Angaben zu fordern, deren allgemeine Kenntniß als eine Bedingung für die Entwicklung des Gesammtlebens angesehen werden müssen."

Die Datenschutzbeauftragten sind jedenfalls in ihrer Bestandsaufnahme zu dem Ergebnis gekommen, daß Individualrechte vielfach ohne zwingende Gründe zugunsten staatlicher Eingriffsrechte zurückgedrängt werden. Sie haben festgestellt: „Mehr und mehr begegnet der Staat dem einzelnen Bürger mit Mißtrauen und schafft ein immer dichteres Kontrollnetz. Es ist fraglich, ob dieses Menschenbild dem des Grundgesetzes entspricht."

Es ist in der Tat unübersehbar, daß sich der Datenschutz in einer wechselseitigen Vertrauenskrise von Staat und Bürgern befindet. Das Schutzgut der informationellen Selbstbestimmung ist das Vertrauen des Bürgers, daß sein Persönlichkeitsrecht bei der Verwendung seiner Daten durch Staat und Wirtschaft gewahrt wird (vgl. § 1 Abs. 1 BDSG). Zu diesem Vertrauensschutz gehört die Erwartung des Bürgers, daß Staat und Wirtschaft seine Daten nur im unerläßlichen Umfang verwenden. Voraussetzung für diese Zurückhaltung von Staat und Wirtschaft ist andererseits deren Vertrauen in die Rechtstreue des Bürgers.

Dieses sich ergänzende Vertrauen sinkt offenbar auf beiden Seiten. Wie neuere Umfragen gezeigt haben, nimmt das Vertrauen des Bürgers in die staatliche Grundordnung insbesondere gegenüber dem Staat als Gesetzgeber ab (so die Feststellungen von Professor Scholz). Ebenso sinkt offenbar das Vertrauen des Staates gegenüber den Bürgern mit der Folge ständig neuer gesetzlicher Freiheitseinschränkungen.

Das von Bundestag und Bundesrat im September 1994 mit großer Mehrheit angenommene Verbrechensbekämpfungsgesetz ist dafür ein deutliches Zeichen. Trotz der öffentlichen Kritik – auch durch die Datenschutzbeauftragten (18.4) – soll künftig der Bundesnachrichtendienst seine Erkenntnisse aus dem internationalen Fernmeldeverkehr auswerten und an die Strafverfolgungsbehörden weitergeben dürfen; bei diesen Abhörmaßnahmen wird unvermeidlich auch eine große Zahl Unbeteiligter einbezogen werden. Damit nimmt das heimliche Abhören inflationär zu, wobei als Voraussetzung für das Abhören

kein konkreter strafrechtlich relevanter Verdacht gegen die betroffenen Bürger bestehen muß.

Die institutionelle Kontrolle weitet sich durch die technische Entwicklung auch sonst in Staat und Wirtschaft erheblich aus, wie die Datenschutzbeauftragten in ihrer Bestandsaufnahme wiedergegeben haben. Mit vermehrtem Datenabgleich aus automatisierten und vernetzten Dateien können schließlich alle Bürger und fast alle Lebensbereiche erfaßt werden.

In der Titelgeschichte des SPIEGEL von Ende November 1994 „Der Chip-Bürger Alles auf eine Karte" wird zutreffend an einer Vielzahl von Fällen dargestellt, daß Plastik-Karten mit Mikrochips „unsere Lebensgewohnheiten total verändern" werden. Die Überwachung im Straßenverkehr bei Autobahngebühren, im Nahverkehr durch bargeldlose Zahlung mit Chipkarten, im Gesundheitsbereich durch geplante Patientenkarten sind dafür einige von vielen Beispielen.

In der Telekommunikation bis hin zum interaktiven Fernsehen ist schon jetzt die Tendenz erkennbar, daß immer mehr eigene Gestaltungsmöglichkeiten durch größeren Komfort mit immer mehr Datenverarbeitung erkauft werden. Nicht nur das Telefonverhalten, sondern künftig auch das Fernsehverhalten wird individuell überprüfbar. Mit den möglichen Zugriffen auf die persönlichen Daten steigen die Risiken für die Bürger, und zwar nicht nur bei Mißbrauch, sondern durchaus auch bei legalem Vorgehen der jeweiligen Stellen.

Die Datenschutzbeauftragten haben in ihrer Bestandsaufnahme erklärt, daß die Umsetzung des Vorkszählungsurteils nicht nur durch geeignete Rechtsgrundlagen, sondern verstärkt durch die Entwicklung geeigneter technisch-organisatorischer Maßnahmen abgesichert werden muß.

Der Datenschutz muß deshalb neue Wege gehen. Dazu gehört ein Ausbau des vorgezogenen Datenschutzes einschließlich einer Risikoanalyse der jeweils vorgesehenen Informationstechnik. Ebenso wird dazu die Unterstützung datenschutzfreundlicher Technologien gehören. Neben der Kontrolle werden demnach Beratung und Empfehlung zunehmende Bedeutung haben.

Im Ergebnis kann die Antwort auf die aktuellen Gefährdungen des Datenschutzes nur darin bestehen, mit einer Palette von rechtlichen, technischen und organisatorischen Vorkehrungen den Grundsätzen des Volkszählungsurteils Rechnung zu tragen. Es hilft nicht weiter, die neueren gesellschaftlichen und technischen Entwicklungen abzulehnen; vielmehr geht es darum, an der Gestaltung technischer und gesellschaftlicher Entwicklungen mitzuwirken.

1.3 Schwerpunkt hamburgübergreifende Datenverarbeitung

Die Ausweitung der Vernetzung personenbezogener Daten in der hamburgischen Verwaltung ist bereits in unserem IuK-Datenschutzbericht eingehend behandelt worden (12. TB, 3.1). In den letzten Jahren ist die Vernetzung durch

große Projekte wie PROSA (6.1) und PROPERS (7.1) vorangebracht worden. Die Vernetzung in Verwaltung und Wirtschaft reicht aber längst über Hamburg hinaus. Sie erfaßt mehrere benachbarte Bundesländer, z.B. bei der SCHUFA-Nord (22.3), alle Bundesländer, wie bei der Steuerverwaltung (1.5.1), oder ist sogar für eine Reihe von europäischen Staaten geplant, wie bei Europol (17.2).

Die Schwierigkeiten, einen wirksamen Datenschutz zu erreichen, werden durch diese überregionale Datenverarbeitung erhöht, bei der häufig verschiedene Stellen beteiligt sind. Für die Gewährleistung des Datenschutzes stellt sich zunächst die Frage, welche Rechtsgrundlagen jeweils für den Datenschutz maßgeblich sind.

Dabei kommen das Sitzland- oder das Territorialitätsprinzip in Betracht, indem für das anzuwendende Recht entweder auf den Sitz der datenverarbeitenden Stelle abgestellt wird oder auf den Ort, an dem die jeweilige Stelle die Datenverarbeitung durchführt. Verbunden ist damit die Frage, wer für die Datenschutzkontrolle zuständig ist.

Bei den Beratungen der EG-Datenschutzrichtlinie (1.8) ist diese Frage bis zuletzt streitig erörtert worden. Während ursprünglich der Ort der Datenverarbeitung maßgeblich sein sollte, ist in der Fassung des Richtlinienentwurfs von Mitte Oktober 1994 – entgegen der Position der deutschen Seite – das Sitzlandprinzip zugrunde gelegt worden. Daran knüpft die Zuständigkeit der Datenschutzkontrolle mit der Folge an, daß die hamburgische Aufsichtsbehörde künftig bei Firmen mit Sitz in Hamburg auch für deren Datenverarbeitungen in anderen Bundesländern und im Ausland zuständig würde.

Als Kompromiß wurde vom deutschen Vorsitz bei den Beratungen der EG-Richtlinie vorgeschlagen, daß das Sitzlandprinzip grundsätzlich gelten soll, aber für alle Niederlassungen das Recht am Ort ihrer Datenverarbeitung angewendet wird. Das Sitzlandprinzip würde dann nur noch die Fälle umfassen, in denen die Datenverarbeitung eines Unternehmens in einem anderen Mitgliedstaat erfolgt, in dem es keine Niederlassung hat.

Die deutsche Delegation hat – auch nach unserer Auffassung zu Recht – die Tendenz unterstützt, daß regelmäßig das Recht am Ort der Datenverarbeitung maßgeblich sein soll. Anderenfalls könnten datenverarbeitende Unternehmen durch die Verlagerung ihres Sitzes wie bei der Ausflaggung von Schiffen die Rechtsgrundlage fast beliebig wählen.

Nicht allein die überörtliche Ausdehnung vernetzter Systeme führt zu datenschutzrechtlichen Problemen, sondern auch die Zugriffsmöglichkeit von Stellen mit unterschiedlichen Aufgaben. Ein anschauliches Beispiel hierfür ist das Ausländerzentralregister, das bundesweit die Daten von Millionen Menschen für den Zugriff der öffentlichen Verwaltung in insgesamt 12 verschiedenen Bereichen unabhängig von deren regionaler Zuständigkeit zur Verfügung stellt (15.2).

Wenn mehrere Stellen beteiligt sind, ist das Prinzip der datenschutzrechtlichen Verantwortung für die Betroffenen und für die Kontrolle besonders wichtig. Für die öffentlichen Stellen folgt dieses Prinzip aus dem Grundsatz, daß personenbezogene Daten jeweils nur zur Erfüllung der gesetzlichen Aufgaben verarbeitet werden dürfen (§§ 12 ff. HmbDSG), für die nicht-öffentlichen Stellen aus der Befugnis zur Datenverarbeitung für „eigene Geschäftszwecke" (§§ 28 bis 30 BDSG).

Wenn eine Stelle zur Verfolgung dieser Zwecke Daten verarbeitet, ist sie für die Zulässigkeit und Richtigkeit verantwortlich. Eine hamburgische Behörde oder ein hamburgisches Unternehmen verlieren ihre Verantwortung nicht, wenn sie die Daten in einem bundesweiten oder sogar internationalen Informationssystem speichern. Sie behalten die Verantwortung insbesondere gegenüber dem Betroffenen, wenn er seine Datenschutzrechte geltend macht. Auch die Datenschutzkontrolle muß sich nach dem Recht der Stelle richten, die für die Datenverarbeitung verantwortlich ist. Dabei kommt es nicht darauf an, ob noch andere Stellen ihren „Besitz" an den Daten erklären.

Diese Probleme haben uns veranlaßt, die hamburgübergreifende Datenverarbeitung als Querschnitt-Thema zu behandeln. In den verschiedenen Abschnitten des Tätigkeitsberichts wird auf die damit zusammenhängenden Fragen eingegangen, z.B. bei der Steuerverwaltung (1.5.1), beim Ausländerzentralregister (15.2), bei der Polizei (insbesondere 17.1 und 17.2), bei überregionalen Forschungsprojekten (21.3), bei der Fernwartung für das UKE (21.7) und bei der grenzüberschreitenden Datenverarbeitung in der Versicherungswirtschaft (23.3 und 23.9).

1.4 Weiterer Schwerpunkt Zweigstellen

In der Verwaltung und Wirtschaft ist außerdem die problematische Entwicklung verstärkt festzustellen, daß bei großen Einrichtungen wie den Krankenkassen oder Kreditinstituten sämtliche Zweigstellen einen umfassenden Zugriff auf die personenbezogenen Daten ihrer Kunden haben. Damit hat eine Vielzahl von Mitarbeitern die Möglichkeit, diese sensiblen Daten wahrzunehmen, obwohl die Daten regelmäßig nur bei einer Zweigstelle benötigt werden. Teilweise ist dies auf die unzulängliche EDV-Technik zurückzuführen (siehe 6.4). Beispielsweise das Projekt Sozialhilfe-Automation (PROSA) zeigt aber, daß sich eine rechtlich gebotene Beschränkung des Zugriffs grundsätzlich technisch realisieren läßt.

Wir haben deshalb dieses Thema als weiteren Schwerpunkt gewählt. Im Sinne eines datenschutzgemäßen Verfahrens haben wir uns dafür ausgesprochen, daß der Bürger die Wahlmöglichkeit haben soll, ob er einen Zugriff auf seine Daten nur bei einer von ihm bestimmten Zweigstelle oder bei mehreren Zweigstellen zulassen will. Dies ist auch mit dem Wunsch der Unternehmen nach

Kundenfreundlichkeit vereinbar, indem der Bürger entscheidet und ihm nicht ein Service-Angebot mit Zugriff aller Zweigstellen aufgedrängt wird.

Um die Strukturen dieser Zweigstellenproblematik zu verdeutlichen, wird das Thema in diesem TB an verschiedenen Beispielen dargestellt. Meist geht es dabei um Zweigstellen innerhalb Hamburgs, wie bei dem Zugriff von Krankenkassen auf Beitrags- und Leistungsdaten (6.4) und dem Zugriff von Kreditinstituten auf Kontoinformationen ihrer Kunden (26.1). Zu verweisen ist auch auf die frühere Behandlung des Themas im Meldewesen (9. TB, 4.9.3, und 10. TB, 13.11). Zum Teil geht es aber auch um Zugriffsmöglichkeiten über Hamburg hinaus, z.B. bei den Zweigstellen der SCHUFA-Nord (22.3). Insoweit wird das Querschnitt-Thema einer hamburgübergreifenden Datenverarbeitung um diesen Aspekt ergänzt.

Außerdem wird als informationstechnische Grundlage für die Entscheidung des Bürgers, welche Zweigstelle zugriffsberechtigt sein soll, die sog. Mandantenfähigkeit von Datenverarbeitungssystemen behandelt (3.9). Hier bietet die technische Ausgestaltung den Ansatzpunkt für eine datenschutzfreundliche Lösung.

1.5 Hamburgische Datenschutzvorschriften

Die Novellierung des Hamburgischen Datenschutzgesetzes ist im Jahre 1994 weiter vorbereitet worden. Einige bereichsspezifische Datenschutzregelungen sind in hamburgischen Gesetzen hinzugekommen. Es fehlt aber noch eine Reihe von Datenschutzregelungen in wichtigen Bereichen.

1.5.1 Hamburgisches Datenschutzgesetz

Im Februar 1994 hatte die Justizbehörde den Referentenentwurf eines Gesetzes zur Änderung des Hamburgischen Datenschutzgesetzes an die Behörden zur Stellungnahme übermittelt. In dem Entwurf wird zur Fortentwicklung des Hamburgischen Datenschutzgesetzes insbesondere vorgesehen, den Anwendungsbereich zu präzisieren (§ 2), die Dateibeschreibungen und die Registerführung zu vereinfachen (§§ 9 und 24), eine gesetzliche Pflicht zur Risikoanalyse einzuführen (§ 10) und die Stellung des Hamburgischen Datenschutzbeauftragten zu verbessern (§ 22 und 23).

Zugleich werden in dem Gesetzentwurf verschiedene Regelungen aus neueren Landesdatenschutzgesetzen übernommen. Dazu bestand Veranlassung, nachdem seit Inkrafttreten des Hamburgischen Datenschutzgesetzes am 1. August 1990 zwölf neue Landesdatenschutzgesetze erlassen worden sind, die teilweise bessere Lösungen für datenschutzrechtliche Fragen aufzeigen als das geltende hamburgische Gesetz. Außerdem waren einige Vorschriften des Hamburgischen Datenschutzgesetzes an das neue Bundesdatenschutzgesetz anzupassen, das überwiegend am 1. Juni 1991 in Kraft getreten ist.

Der Gesetzentwurf stimmt weitgehend mit den Vorschlägen überein, die ich im Laufe der Abstimmung mit der Justizbehörde gemacht habe.

Bedenken sind von den Behörden vor allem dagegen erhoben worden, daß die privatrechtlich organisierten öffentlichen Unternehmen in den Anwendungsbereich des Hamburgischen Datenschutzgesetzes einbezogen und dabei als öffentliche Stellen behandelt werden sollen, soweit sie Aufgaben der öffentlichen Verwaltung wahrnehmen. Mit der vorgesehenen Präzisierung des Anwendungsbereichs wird jedoch nur die Regelung in § 2 Abs. 2 BDSG nachvollzogen, daß die sog. Vereinigungen öffentlicher Stellen der Länder unabhängig von ihrer Rechtsform zu den öffentlichen Stellen gehören. Demgemäß enthalten inzwischen alle Landesdatenschutzgesetze ähnliche Regelungen über die Einbeziehung dieser Stellen, die dann – soweit sie im Wettbewerb stehen – wiederum weitgehend nur das Datenschutzrecht für nicht-öffentliche Stellen zu beachten haben.

Außerdem haben sich viele Behörden gegen eine Pflicht zur Risikoanalyse gewandt. Dies ist schon deshalb nicht akzeptabel, weil nach den geltenden Verwaltungsvorschriften ohnehin „eine Schwachstellen-Analyse mit anschließender Risikobewertung" vorzunehmen ist. Hier geht es um den gesetzlich zu regelnden Grundrechtsschutz durch Verfahren, ohne den die Risiken nicht transparent werden und ohne den ein vorgezogener und damit rechtzeitig wirksamer Datenschutz nicht zu erreichen ist (11. TB, 1.1). Die gesetzliche Regelung kann und soll sich dabei auf wenige grundsätzliche Aussagen beschränken.

Gegen eine Pflicht zur Risikoanalyse wurde auch geltend gemacht, daß bei einer hamburgübergreifenden Datenverarbeitung – z.B. in der Steuerverwaltung – die Datenschutzvorkehrungen arbeitsteilig von verschiedenen Bundesländern entwickelt würden und deshalb eine eigene hamburgische Risikoanalyse entfallen müsse. Gerade in solchen Bereichen, die wie die Steuerverwaltung mit besonders sensiblen personenbezogenen Daten umgehen, ist jedoch eine Risikoanalyse unverzichtbar, weil die Datenschutz-Verantwortung nach §§ 8 und 10 HmbDSG auch dann bei der anwendenden hamburgischen Stelle bleibt.

Die Arbeitsteilung hinsichtlich der Datenschutzvorkehrungen muß daher zwischen den Ländern abgestimmt werden mit der Maßgabe, daß alle Länder unterrichtet werden und Gelegenheit zur Stellungnahme und Änderung der Vorschläge haben. Die behaupteten Erschwernisse bei arbeitsteilig entwickelten und betreuten Programmen dürften schon deshalb nicht bestehen, weil alle Beteiligten vergleichbaren Datenschutzanforderungen Rechnung zu tragen haben.

Im Oktober 1994 hat die Justizbehörde den fortgeschriebenen Entwurf eines Gesetzes zur Änderung des Hamburgischen Datenschutzgesetzes vorgelegt. Der Entwurf enthält nun auch die wichtige Regelung der Wartung einschließ-

lich Fernwartung in § 3 HmbDSG sowie Datenschutzregelungen für gemeinsame oder verbundene Dateien in § 11a HmbDSG (vgl. 12. TB, 1.4). Die bürgerschaftliche Beratung und Verabschiedung der Novellierung des Hamburgischen Datenschutzgesetzes im Laufe des Jahres 1995 bleibt abzuwarten.

1.5.2 Bereichsspezifische Datenschutzvorschriften

Wichtige Fortschreibungen des Datenschutzes sind im Hamburgischen Mediengesetz vom 20. April 1994 enthalten (4.2). Damit sind in Hamburg die Rechtsgrundlagen nicht nur für den herkömmlichen Rundfunkbereich, sondern auch für rundfunkähnliche Dienste und damit auch für interaktive Programme rechtzeitig geschaffen worden. Die Datenschutzbestimmungen entsprechen in vollem Umfang unseren Vorschlägen.

Mit der Ergänzung des Rundfunkstaatsvertrages, die am 1. August 1994 in Kraft getreten ist, wurden die Reality TV-Sendungen mit Verstößen gegen die Menschenwürde verboten. Unseren Bedenken (12. TB, 4.3.1) wurde damit umgehend Rechnung getragen. Bemerkenswert ist dabei die zusätzliche Regelung, wonach „eine Einwilligung unbeachtlich (ist)". In der amtlichen Begründung heißt es dazu treffend: „Insoweit ist der Kernbereich der Menschenwürde ein objektiver, unverfügbarer und unverzichtbarer Wert, den der Staat nicht nur gegen Dritte, sondern sogar gegen den Betroffenen selbst schützen muß."

In der bürgerschaftlichen Beratung befindet sich die Novellierung des Hamburgischen Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (21.1). Die Datenschutzvorschriften in diesem sensiblen Bereich wurden aktualisiert.

Im Hamburgischen Beamtengesetz wurden eingehende Vorschriften über den Datenschutz im Personalaktenbereich eingefügt (7.3). Das Beamtenrechtsrahmengesetz des Bundes mit seinen datenschutzfreundlichen Neuerungen wurde dabei in das hamburgische Landesrecht übernommen. Ergänzend ist die Regelung über den Datenschutz bei Beschäftigungsverhältnissen in § 28 HmbDSG bei der Novellierung des Hamburgischen Datenschutzgesetzes anzupassen (7.4.).

Der Entwurf des neuen Hamburgischen Verfassungsschutzgesetzes wurde in der Bürgerschaft beraten (18.1). Nach einer ausführlichen Anhörung wurden Ende 1994 von den Fraktionen Änderungsvorschläge eingebracht, die in wichtigen Punkten den Datenschutz verringern würden.

1.5.3 Fehlende Datenschutzvorschriften

In den bürgerschaftlichen Ausschußberatungen zum 12. TB sind die dort genannten Lücken im hamburgischen Datenschutzrecht (12. TB, 1.5) zusammenfassend behandelt worden. Es fehlen demnach immer noch wichtige gesetzliche Datenschutzvorschriften in Hamburg. Dazu gehören insbesondere

ein hamburgisches Gesetz über das öffentliche Gesundheitswesen (21.1), ein hamburgisches Sicherheitsüberprüfungsgesetz (18.2), gesetzliche Vorschriften zur Umweltdatenverarbeitung (12. TB, 5.1) und die Schulgesetznovellierung mit Rechtsverordnung (9.1).

Für diese nicht vollständige Aufzählung ist erneut daran zu erinnern (12. TB, 1.5.1), daß der sog. Übergangsbonus mit dem Ende der Legislaturperiode dieser Bürgerschaft endgültig abgelaufen sein wird. Die Äußerung in der Stellungnahme des Senats zum 12. TB, diese Ausführungen zum Übergangsbonus seien Spekulation, trifft nicht zu. Der Bundesrat hat schon im Jahre 1992 aus Anlaß der Beratungen des Schengener Übereinkommens erklärt: „Es wird zwar nicht verkannt, daß dem Gesetzgeber eine ausreichende Zeit für die Beratung und den Erlaß der erforderlichen Vorschriften zu lassen ist; jedoch gibt es bereits in der Rechtsprechung die Auffassung, daß die Übergangsfrist abgelaufen sei."

1.5.4 Richtlinien

Zur Verbesserung des Datenschutzes in Hamburg tragen zusätzlich die Richtlinien bei, die bisher vom Senatsamt für den Verwaltungsdienst und nach dem zwischenzeitlichen Aufgabenwechsel von der Finanzbehörde – Amt für Informations- und Kommunikationstechnik – erarbeitet wurden (3.2).

Von praktischer Bedeutung ist insbesondere die Richtlinie zum Verfahren der Datensicherung im IuK-Bereich (DS-Richtlinie) vom 4. Oktober 1994 (3.2.1) und die zuvor mit Wirkung vom 1. Mai 1994 in Kraft getretene Richtlinie über die Sicherheit der Datenverarbeitung auf Arbeitsplatzrechnern in der hamburgischen Verwaltung (PC-Richtlinie) vom 15. April 1994 (3.2.3).

1.6 Auftragsverwaltung nach Art. 84 ff. Grundgesetz

Im Rahmen der Diskussion um einen Vordruck zur Überprüfung des Kindergeldanspruchs (6.7) ist die grundsätzliche Frage aufgetreten, welche datenschutzrechtlichen Handlungsmöglichkeiten der Länder bei Auftragsverwaltung nach Art. 84 ff. Grundgesetz (GG) bestehen.

Wir sind für derartige Fälle zu dem Ergebnis gekommen, daß Weisungen im Rahmen der Bundesauftragsverwaltung (Art. 85 Abs.3 GG) die Länder auch dann verpflichten, wenn sie rechtswidrig sind. Das angewiesene Land kann gegenüber dem Bund aber in einem Remonstrationsverfahren die Rechtswidrigkeit der Weisung darstellen und sich für eine Abhilfe einsetzen.

Für uns bedeutet dies, daß wir gegenüber den zuständigen Landesbehörden erforderlichenfalls auf ein derartiges Remonstrationsverfahren hinwirken werden. Wenn die Behörden die Rechtswidrigkeit gegenüber dem Bund nicht geltend machen wollen, könnte ich diese Untätigkeit förmlich beanstanden. Die Ausführung der zwar rechtswidrigen, aber bindenden Weisung durch die Lan-

desbehörden kann ich jedoch nicht nach § 25 HmbDSG beanstanden. Sofern diese eingeschränkten Handlungsmöglichkeiten nicht zum Erfolg führen, ist die Beteiligung des Bundesbeauftragten für den Datenschutz erforderlich. Er kann sich bei den zuständigen Bundesministerien für die abschließende Korrektur rechtswidriger Weisungen an Landesbehörden einsetzen.

1.7 Bundesdatenschutzgesetz

Mit einer Änderung des Bundesdatenschutzgesetzes ist erst zu rechnen, wenn nach Verabschiedung der EG-Datenschutzrichtlinie die notwendigen Anpassungen innerhalb der Übergangsfrist von voraussichtlich 3 Jahren vorzunehmen sind.

Für Hamburg ist nach langer zeitlicher Verzögerung inzwischen mit der Anordnung über Zuständigkeiten auf dem Gebiet des Datenschutzes vom 23. September 1994 bestimmt worden, daß der Hamburgische Datenschutzbeauftragte die Aufsichtsbehörde nach § 38 BDSG ist.

Die Prüfungen der Unternehmen, die nach dem Bundesdatenschutzgesetz einer ständigen Aufsicht unterliegen, sind im Jahr 1994 weiter intensiviert worden (29.2). Der gesetzlichen Aufgabe zu ständiger Kontrolle in diesem Bereich der Wirtschaft ist damit zunehmend entsprochen worden.

1.8 Entwicklung der EG-Datenschutzrichtlinie

Die Beratungen in der Gruppe „Wirtschaftsfragen" des Ministerrates wurden im zweiten Halbjahr 1994 unter deutschem Vorsitz fortgeführt. Im Oktober 1994 wurde eine aktuelle konsolidierte Fassung des Richtlinienentwurfs erstellt. Die Beschlußfassung des Binnenmarktrats über den gemeinsamen Standpunkt war nach Redaktionsschluß dieses TB vorgesehen. Da es sich um eine gemeinsame Richtlinie des Europäischen Parlaments und des Rates handelt, ist nach Feststellung des gemeinsamen Standpunkts erneut das Europäische Parlament zu beteiligen.

Eine Hauptfrage bei den Beratungen ist das Problem, ob für die Geltung des Datenschutzrechts der Mitgliedstaaten das Sitzlandprinzip (Sitz des Unternehmens) oder das Territorialitätsprinzip gelten soll (siehe oben 1.3).

Ein wichtiges Problem war und ist die Frage, ob das Datenschutzrecht der Mitgliedstaaten weitergehende und damit strengere Datenschutzanforderungen als die Richtlinie enthalten darf. Der Wortlaut der konsolidierten Fassung läßt nur zu, daß die Mitgliedstaaten die Voraussetzungen für eine rechtmäßige Datenverarbeitung „näher bestimmen". Übereinstimmend wurde aber angenommen, daß die Richtlinie den Mitgliedstaaten die Möglichkeit bietet, über allgemeine Datenschutzgesetze hinaus für bestimmte Sektoren spezielle Verarbeitungsbedingungen vorzusehen.

Übereinstimmung bestand ferner darin, daß ein Mitgliedstaat mit strengeren Regelungen innerhalb des Rahmens der Richtlinie einen Datentransfer in Mitgliedstaaten mit weniger strengen Regelungen unterbinden kann.

Auch über die Bestimmungen, die die Meldepflicht betreffen, wurde kontrovers diskutiert. Aufgenommen in den Text wurde nun auf Forderung der deutschen Seite die Möglichkeit zur Selbstkontrolle der Unternehmen durch einen betrieblichen Datenschutzbeauftragten. Dadurch kann die Meldepflicht der Verarbeitungen entfallen oder vereinfacht werden.

Es ist vorgesehen, daß die Mitgliedstaaten nach Annahme der Richtlinie die erforderlichen Rechts- und Verwaltungsvorschriften binnen 3 Jahren erlassen. Dabei wird darauf zu achten sein, daß der deutsche Datenschutzstandard möglichst nicht für eine europäische Vereinheitlichung verringert wird.

Getrennt von der EG-Datenschutzrichtlinie wird die sog. ISDN-Richtlinie des europäischen Parlaments und des Rates weiterberaten. Hierzu liegt ein geänderter Vorschlag der EG-Kommission vom 14. Juni 1994 vor. Das Ergebnis der EG-Datenschutzrichtlinie als Grundlage auch für die ISDN-Richtlinie soll abgewartet werden.

1.9 Verhältnis zum Bürger

Wir haben uns weiterhin bemüht, die vielfältigen Anliegen aufzugreifen, die die Bürger an uns herantragen. Eine wichtige Aufgabe war gleichzeitig die Öffentlichkeitsarbeit, um über die Medien den Bürgern die Themen zu vermitteln, die für sie datenschutzrechtlich von besonderer Bedeutung sind.

1.9.1 Eingaben

Es erreichten uns erneut zahlreiche Eingaben. Bis Ende November 1994 gingen 332 schriftliche Eingaben zu folgenden Themen ein:

Öffentlicher Bereich	164
davon Inneres und Justiz	72
Gesundheit und Soziales	32
Sonstiges	60
Nicht-öffentlicher Bereich	68
davon Versandhandel	5
Versicherungswirtschaft	23
Kreditwirtschaft	14
Werbung	20
Arbeitnehmer-Datenschutz	13
Schufa und Auskunfteien	19
Gesundheitswesen	18
Wohnungswirtschaft	5

Im zweimonatigen Abstand werden nach wie vor Bürgersprechstunden zu Datenschutzfragen in der Dienststelle angeboten. Die Termine werden über die Hamburger Zeitungen und Rundfunkveranstalter vorher bekanntgegeben. Auf diese Weise konnten auch Bürger informiert werden, die sich sonst möglicherweise nicht an uns gewandt hätten.

1.9.2 Öffentlichkeitsarbeit

Zusammen mit dem Kommunikationsverein Hamburger Juristen haben wir am 28. Juni 1994 ein Kolloquium mit Herrn Dethloff, dem Erfinder der Chipkarte, über „Die Zukunft der Chipkarte – Patientenkarte, Nahverkehrskarte, Mehrzweckkarte –" veranstaltet. Bei der wiederum gut besuchten Podiumsdiskussion wurden die Entwicklungsmöglichkeiten und Risiken für den Datenschutz an aktuellen Beispielen aufgezeigt. Dazu gehören die Einführung der Krankenversichertenkarte in Hamburg sowie der Nahverkehrskarte als Vorhaben des Hamburger Verkehrsverbundes. Als Ausblick auf die Zukunft wurde außerdem die Mehrzweckkarte als mögliche künftige Kombination für Telefonieren, Parken usw. behandelt.

Diese Fragen waren auch Thema der vierteljährlichen Pressekonferenzen in der Dienststelle mit Vertretern der Hamburger Zeitungen und des Rundfunks. Weitere Themen auf den Pressekonferenzen waren u.a. das Grundrecht auf Datenschutz im Grundgesetz, der Datenzugriff aller Geschäftsstellen von Krankenkassen und die Fernwartung von Patientendaten im Ausland.

In der Reihe der „Hamburger Datenschutzhefte" haben wir im April 1994 die Broschüre „Datenschutz in der Arztpraxis" veröffentlicht. Das Interesse ist sehr groß. Im Oktober 1994 erschien die 2. Auflage. Ein Nachdruck wurde in einem anderen Bundesland auf dortige Kosten an die Ärzte verteilt.

Im Oktober 1994 wurde eine Broschüre über den „Datenschutz in Netzen" als Beratung und Empfehlung zur Verbesserung des Datenschutzes bei den neuen Informations- und Kommunikationstechniken herausgegeben. Die Broschüre soll dazu beitragen, für die rechtzeitige Vorbereitung von Sicherheitskonzepten über die Mechanismen und Defizite einzelner Standard-Produkte zu informieren. Damit haben wir im technischen Bereich drei Broschüren, die bundesweit Interesse gefunden haben, über den Datenschutz für PC, für UNIX-Mehrplatzanlagen und nunmehr für Netze veröffentlicht.

1.10 Zusammenarbeit mit Verwaltung und Justiz

Das insgesamt positive Zusammenwirken mit den hamburgischen Behörden und Kammern sowie der Justiz wurde fortgesetzt. Das Datenschutz-Jahrestreffen, das bereits zum dritten Mal jeweils Mitte Februar durchgeführt wurde, gab

erneut Gelegenheit zum Meinungsaustausch mit Vertretern der Bürgerschaft, Justiz, Verwaltung, Kammern, Gewerkschaften und Bürgervereinen.

Von den langfristig vorbereiteten großen Automationsprojekten befindet sich das Projekt Sozialhilfe-Automation (PROSA) inzwischen weitgehend in der Anwendung (6.1), während das Projekt Personalwesen (PROPERS) teilweise die Pilotphase erreicht hat (7.1). Die Eignung der Datenschutzvorkehrungen kann damit bei einer zunehmend großen Zahl von Beteiligten in der Praxis geprüft werden. Weitere Vorhaben wie das Projekt Automation der Stellenplanung (ProStep) sind neu hinzugekommen (7.2).

Als Arbeitshilfe haben wir eine aktualisierte Liste der hamburgischen Gesetze und Verordnungen mit Datenschutzbestimmungen (Stand Ende September 1994) zusammengestellt. Es liegt im gegenseitigen Interesse, daß diese Rechtsvorschriften mit vielfältigen bereichsspezifischen Regelungen ebenso wie die Verwaltungsvorschriften, insbesondere die inzwischen vorliegenden Richtlinien (1.5.4), für die Verwaltung und Justiz jederzeit zur Verfügung stehen. Deshalb prüfen wir zur Zeit gemeinsam mit der Finanzbehörde – Amt für Informations- und Kommunikationstechnik – die Möglichkeiten für eine technikunterstützte Datenschutz-Informationssammlung, mit der diese Datenschutzgrundlagen auf Datenträgern als Textdatenbank mit Suchfähigkeit bereitgestellt werden.

2. Entwicklung der Dienststelle

Im Jahr 1994 gab es nur wenige personelle Veränderungen. Für eine Referatsleiterstelle konnte erreicht werden, daß die Wiederbesetzung schließlich zugelassen wurde. Bei dem knappen Personalbestand der Dienststelle mit insgesamt 15 Stellen für den öffentlichen und nicht-öffentlichen Bereich gerät unsere Handlungsfähigkeit schnell an ihre Grenzen. Dennoch bin ich weiter bereit, daß Mitarbeiter/innen auch kurzfristig in andere Bereiche der hamburgischen Verwaltung wechseln, wenn dafür eine baldige Nachfolgemöglichkeit gewährleistet ist.

Die herausgehobene Stellenbewertung für meinen Stellvertreter konnte nun auch dienstrechtlich umgesetzt werden. Zur Mobilität innerhalb der Dienststelle wurde dadurch beigetragen, daß Aufgabenbereiche untereinander ausgetauscht werden. Der Anteil der Teilzeitbeschäftigten und der Frauenanteil sind weiterhin hoch (12. TB, 2.).

3. Informations- und Kommunikationstechnik

3.1 Grundschutzkonzept

Im letzten Tätigkeitsbericht (vgl. 12. TB, 3.2) haben wir ausführlich über die Anforderungen an ein Grundschutzkonzept als Voraussetzung für die Einführung neuer Automationsverfahren berichtet. Eine behördenübergreifende Arbeits-

gruppe, an der auch wir beteiligt waren, hat inzwischen ein Grundschutzkonzept für die Informationstechnik in der hamburgischen Verwaltung erarbeitet. Anregungen und Ergänzungen aufgrund der Stellungnahmen der Behörden und Fachämter wurden dabei berücksichtigt.

Das Grundschutzkonzept soll als Arbeitshilfe bei der Erstellung von Sicherheitskonzepten für den Einsatz von IuK-Systemen dienen. Es enthält in Form einer Checkliste eine Zusammenstellung von Regeln, deren Beachtung und Umsetzung in konkrete organisatorische, personelle und technische Maßnahmen einen Grad der Verfügbarkeit, Integrität und Vertraulichkeit der automatisiert verarbeiteten Daten gewährleisten kann, der einem mittleren Schutzbedarf angemessen ist. Für die Einstufung des Schutzbedarfs können die Kriterien aus dem IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik herangezogen werden.

Das Grundschutzkonzept ersetzt nicht die Erstellung von Risikoanalysen. Es bleibt weiterhin erforderlich, jedes in Planung befindliche IuK-System zunächst hinsichtlich seines Schutzbedarfs zu bewerten und einzustufen. Ergibt sich ein geringer bis mittlerer Schutzbedarf, kann unter der Voraussetzung, daß Sicherheitsmaßnahmen nach den Grundschutzregeln getroffen werden, auf eine individuelle Schwachstellenanalyse verzichtet werden. Nur dann, wenn die Daten einem höheren Schutzbedarf unterliegen, sind im Einzelfall zusätzliche oder wirksamere Schutzmaßnahmen einzuführen.

Die umfangreiche Checkliste zeigt Beispiele für einzelne Schutzmaßnahmen auf und enthält jeweils Verweise auf bestehende, für die hamburgische Verwaltung verbindliche Richtlinien. An mehreren Stellen werden zudem über den Grundschutz hinausgehende Sicherheitsmaßnahmen empfohlen, die geeignet sind, auch einen höheren Schutzbedarf abzudecken (z.B. Verschlüsselung von Daten im Netz).

Das Grundschutzkonzept bietet auch aus unserer Sicht eine umfassende Unterstützung für die Planung des IuK-Einsatzes. Die Anwendung der darin enthaltenen Regeln kann entscheidend dazu beitragen, den erforderlichen Untersuchungs- und Planungsaufwand im Einzelfall zu verringern.

3.2 Stand der Richtlinien zur Datensicherung

Auf Beschluß des Senats vom 18. Januar 1994 ist die bisherige Abteilung 3 des Senatsamts für den Verwaltungsdienst – Organisationsamt – zur Finanzbehörde verlagert worden. Seit dem 1. April 1994 werden die ministeriellen und steuernden Aufgaben für Grundsatzangelegenheiten der IuK-Technik in der hamburgischen Verwaltung damit nunmehr von dem dort neu eingerichteten Amt für Informations- und Kommunikationstechnik wahrgenommen. Hierzu zählt u.a. auch die Erarbeitung von Rahmenvorgaben und Standards für den Einsatz

von IuK-Technik sowie von Vorgaben zur verwaltungsmäßigen Umsetzung des Datenschutzes und der Datenschutzrevision.

Im Berichtsjahr sind hierzu folgende, für die hamburgische Verwaltung verbindliche neue Richtlinien in Kraft getreten:

— Richtlinie über die Entsorgung von Datenträgern (Entsorgungsrichtlinie, MittVw 1994, S. 165),

— Richtlinie zum Verfahren der Datensicherung im IuK-Bereich (DS-Richtlinie, MittVw 1994, S. 326),

— Richtlinie zur Gestaltung der IuK-Architektur in der hamburgischen Verwaltung (IuK-Architektur-Richtlinie),

— Richtlinie über die Sicherheit der Datenverarbeitung auf Arbeitsplatzrechnern in der hamburgischen Verwaltung (PC-Richtlinie, MittVw 1994, S. 75).

3.2.1 DS-Richtlinie

Am 1. November 1994 ist eine Neufassung der Richtlinie zum Verfahren der Datensicherung im IuK-Bereich (DS-Richtlinie) in Kraft getreten. Gegenüber der bis dahin immer noch geltenden Fassung vom 6. Juli 1977 berücksichtigen die neuen Regelungen nicht nur die inzwischen fortgeschrittene Entwicklung im IuK-Bereich der hamburgischen Verwaltung. Sie enthalten nunmehr auch erstmals Verweise auf das Hamburgische Datenschutzgesetz.

In der neuen DS-Richtlinie wurde auch die Zuständigkeit für die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme festgelegt, die auf Datenverarbeitungsanlagen des Landesamts für Informationstechnik als zentraler Rechenstelle eingesetzt werden. Dies erfolgte bislang in der Anordnung über Zuständigkeiten auf dem Gebiet des Datenschutzes vom 25. Mai 1982, die in der vom Senat am 23. September 1994 beschlossenen Neufassung keine Regelung mehr enthält. Die zentrale DV-Revision obliegt jetzt der Finanzbehörde gemäß Abschnitt 3 Abs. 2 der DS-Richtlinie.

Die DS-Richtlinie sieht u.a. vor, daß die Finanzbehörde zu unterrichten ist, wenn fachbezogene Regelungen für die Datensicherung in den einzelnen Behörden und Ämtern erlassen werden und wenn bei der Durchführung der Datensicherung wesentliche Mängel auftreten. Aus systematischen Gründen verweist nur die zugrundeliegende Senatsdrucksache im einleitenden Teil darauf, daß die Überwachung und Beratung in Fragen der Datensicherung selbstverständlich auch zu den Aufgaben des Hamburgischen Datenschutzbeauftragten zählt (§ 23 in Verbindung mit § 8 HmbDSG) und daß unsere Beteiligung weiterhin gesondert in der Richtlinie zur Beteiligung des Hamburgischen Datenschutzbeauftragten vom 12. November 1992 (Beteiligungsrichtlinie, MittVw 1992, S. 271 und MittVw 1994, S. 75) geregelt ist. Auch ohne eine entsprechende Bestimmung in der neuen DS-Richtlinie besteht deshalb für alle Stel-

len der hamburgischen Verwaltung die Verpflichtung, den Hamburgischen Datenschutzbeauftragten über wesentliche Mängel zu informieren, die in ihrem Zuständigkeitsbereich bei der Datensicherung auftreten. Dies ergibt sich nicht nur aus Nr. 3.3 Absatz 1 der Beteiligungsrichtlinie („Sonstige Vorgänge"), sondern vor allem aus dem HmbDSG selbst. § 23 Abs. 5 Satz 1 HmbDSG enthält die Verpflichtung, daß die Behörden den Hamburgischen Datenschutzbeauftragten von sich aus über alle für den Datenschutz wichtigen Angelegenheiten ihres Geschäftsbereichs so frühzeitig unterrichten, daß er seine Beratungsaufgaben erfüllen kann. In diesem Sinne wird auch die entsprechende Bestimmung in § 24 Abs. 4 Satz 1 BDSG für die öffentlichen Stellen des Bundes ausgelegt.

3.2.2 Richtlinie zur IuK-Architektur

Ziel der Richtlinie vom 15. November 1994 ist es, durch verbindliche Rahmenvorgaben für den IuK-Einsatz eine einheitliche informationstechnische Infrastruktur in der hamburgischen Verwaltung zu schaffen. Die in der Richtlinie festgelegten Standards werden bei Bedarf an die technischen Entwicklungen angepaßt und fortgeschrieben.

Der Hamburgische Datenschutzbeauftragte begrüßt eine solche Standardisierung. Zum einen kann damit der Einsatz von häufig nicht aufeinander abgestimmten Insellösungen mit oftmals erheblichen Sicherheitsrisiken reduziert werden. Zum anderen besteht die Möglichkeit, wichtige Datensicherungsstandards verbindlich vorzugeben, die bislang jeweils anwendungsbezogen mit den Fachbehörden diskutiert werden mußten.

Erfreulicherweise werden in der Richtlinie nicht nur Netzwerk- und Transportprotokolle, sondern auch Netz-Betriebssysteme standardisiert. Obwohl zunächst vorgesehen war, die hamburgische Verwaltung hinsichtlich der Einbindung von Arbeitsplatzrechnern in Netzwerke ausschließlich auf den LAN-Manager festzulegen, können die Behörden jetzt auch Novell Netware einsetzen. Diese Wahlmöglichkeit ist aus datenschutzrechtlicher Sicht zu begrüßen. Durch einen Verzicht auf Novell Netware hätte sich die hamburgische Verwaltung unnötig selbst von datensicherungstechnischen Neuentwicklungen wie beispielsweise der Verschlüsselung von Inhaltsdaten abgekoppelt, die von Novell als bislang dominierendem Marktführer angekündigt worden sind. TCP/IP-Dienste wie TELNET oder NFS, deren datensicherungstechnische Defizite wir in Kap. 6.7 unserer Broschüre zu UNIX-Mehrplatzanlagen näher dargestellt haben, müssen im Einzelfall auf mögliche Sicherheitsrisiken untersucht werden.

Datensicherungstechnisch bedenklich ist die Aufnahme von „Windows for Workgroups" als Peer-to-Peer-Lösung für kleinere Netze. Die Bedenken richten sich nicht generell gegen den Einsatz von Peer-to-Peer-Systemen, auch wenn diese nicht den Sicherheitsstandard von Client-Server-Systemen bieten. Problematisch ist vielmehr, daß die lokalen Sicherheitsmechanismen von „Windows for Workgroups" ohne großen Aufwand umgangen werden können. Da Außenstehende jederzeit auf netzweit freigegebene Netzdaten zugreifen können, sollte bei der Verarbeitung personenbezogener Daten besser auf sichere Peer-to-Peer-Produkte zurückgegriffen werden.

3.2.3 PC-Richtlinie

Mit dieser Richtlinie, die ab 1. Mai 1994 gilt, hat die Finanzbehörde die seit Jahren existierende und vom Hamburgischen Datenschutzbeauftragten schon früher kritisierte Regelungslücke im PC-Bereich (vgl. 9. TB, 3.1.2) endlich geschlossen. Zum einen setzt sich die Richtlinie inhaltlich sehr weitgehend mit der Virenproblematik und entsprechenden Maßnahmen zur Virenerkennung auseinander. Zum anderen kommen auch Sicherungsmaßnahmen nicht zu kurz, die eine unbefugte Nutzung von personenbezogenen Daten verhindern sollen.

Erfreulicherweise werden in der Anlage zur Richtlinie zahlreiche Grundfunktionen aufgelistet (u.a. Bootschutz, differenzierte Rechteverwaltung sowie Protokollierung von Systemverwaltertätigkeiten und Sicherheitsverstößen), die beim PC-Betrieb umzusetzen und ggf. von PC-Sicherheitsprodukten zur Verfügung zu stellen sind. Bei der Verarbeitung sensibler personenbezogener Daten werden zusätzliche Funktionen wie beispielsweise die Verschlüsselung von Datenträgern und eine von der Systemverwaltung getrennte Auswertung der Protokolldateien gefordert.

Mit der Unterscheidung zwischen Mindest- und Zusatzfunktionen stellt die Richtlinie auf ähnlich abgestufte Sicherheitsmaßnahmen ab, wie wir sie in unserer PC-Broschüre formuliert haben. Die PC-Richtlinie kann in der vorliegenden Form entscheidend dazu beitragen, die Sicherheit auf Arbeitsplatzrechnern in der hamburgischen Verwaltung zu verbessern.

3.2.4 UNIX-Richtlinie

Der Hamburgische Datenschutzbeauftragte hat sich in der Vergangenheit intensiv mit dem Datenschutz beim Betriebssystem UNIX auseinandergesetzt (siehe 12. TB, 3.4 sowie unsere Broschüre „Datenschutzkonzept für UNIX-Mehrplatzanlagen"). Vordringliches Ziel unserer Kritik und der darauf basierenden Forderungen ist die Gewährleistung eines angemessenen Sicherheitsstandards bestehender UNIX-Anlagen.

Damit haben wir eine der wesentlichen Techniklinien der hamburgischen Verwaltung hinsichtlich der Datensicherheit aufgearbeitet. Die bestehenden Regelungen sind jedoch weiterhin insgesamt unbefriedigend. Wir haben dem jetzigen Amt für Informations- und Kommunikationstechnik in der Finanzbehörde zu Beginn des Berichtsjahres die Entwicklung einer UNIX-Richtlinie nahegelegt, um auch in diesem Bereich einen Verbindlichkeitsgrad herzustellen, der

denen anderer IuK-Techniken (z.B. PCs, siehe 3.2.3) entspricht. Dies wurde erfreulicherweise positiv aufgenommen. In der Stellungnahme des Senats zum 12. TB wurde die Erarbeitung einer solchen Richtlinie angekündigt.

3.3 X.25-Datenübertragungsdienst in der hamburgischen Verwaltung

Das Landesamt für Informationstechnik (LIT) hat inzwischen einen paketvermittelten Datenübertragungsdienst auf Basis des technischen Standards CCITT X.25 für die hamburgische Verwaltung in Betrieb genommen, über dessen Planung wir bereits im 11. TB berichtet hatten (11. TB, 4.4). Es ist davon auszugehen, daß dieser Dienst auf längere Sicht die bisher für die Anbindung von Endgeräten an das LIT-Rechenzentrum genutzten Standleitungen ablösen wird. Ferner soll hiermit die Datenübertragung zwischen Rechnern, die an unterschiedlichen Standorten aufgestellt sind, und zwischen lokalen Netzen abgewickelt werden. Ein weiteres Einsatzgebiet für den X.25-Dienst wird der Übergang zu öffentlichen Netzen – insbesondere Datex-P – sein.

Als Trägernetz für den Datenübermittlungsdienst wird das Telekommunikationsnetz der hamburgischen Verwaltung genutzt. In Zukunft sollen jedoch auch Übertragungsdienstleistungen anderer Netzbetreiber in Anspruch genommen werden.

Die Verbindungen zwischen den Netzknoten (Trunks) sind zur Zeit als Standleitungen realisiert. Zukünftig werden auch Kanäle in Backbone-Netzen (z.B. ATM) für Trunks genutzt werden. Die Anwenderanschlüsse sind vorerst ausschließlich über festgeschaltete Übertragungswege mit den Netzknoten verbunden, wobei zur Zeit noch zwei getrennte Teilnetze – eines für die interne Kommunikation, eines für externe Verbindungen – betrieben werden. In Zukunft sollen diese beiden Teilnetze zusammengefaßt und auch Anschlußmöglichkeiten über Wählnetze eingerichtet werden.

Mit dem Übergang von Standleitungen zu vermittelten Systemen unter Nutzung von Zugängen aus öffentlichen Wählnetzen entstehen neuartige Datenschutzrisiken (vgl. zu den spezifischen Risiken bei X.25-basierten Diensten auch die ausführlichere Darstellung in unserer Broschüre über „Datenschutz in Netzen", 5.4):

— Externe Teilnehmer können unbefugt Zugriff auf Rechner erhalten.

— Teilnehmer können ihre wahre Identität dem Netz gegenüber verschleiern oder unter falscher Identität Ressourcen des Netzes in Anspruch nehmen (Maskerade).

— Abgehörte Kennungen und Paßwörter können den unbefugten Zugang zu Anwendungen sowie den unbefugten Zugriff auf Daten ermöglichen.

— Unter Nutzung von Administrationskennungen kann die Netzkonfiguration unbefugt verändert werden.

Dem X.25-Dienst der hamburgischen Verwaltung liegt ein Sicherheitskonzept zugrunde, das mit uns abgestimmt wurde. In diesem Sicherheitskonzept werden die vom LIT realisierten Maßnahmen beschrieben, mit denen den Risiken begegnet werden soll. Hinzuweisen ist insbesondere auf folgendes:

— Beim Verbindungsaufbau wird geprüft, ob es sich um einen berechtigten Teilnehmer bzw. Teilnehmeranschluß handelt (Authentifikation).

— Es besteht die Möglichkeit, geschlossene Benutzergruppen (GBG) einzurichten. In diesem Fall ist die Kommunikation auf andere Mitglieder der GBG beschränkt; Verbindungen zu Externen können nicht aufgebaut werden.

— Durch die Einrichtung fester virtueller Verbindungen (Permanent Virtual Circuit – PVC) baut der X.25-Dienst automatisch eine Verbindung zwischen zwei Teilnehmern auf, ohne daß eine X.25-Adresse angegeben wird. Der PVC-Modus ist vergleichbar mit dem Betrieb von Standleitungen. Im Unterschied zu einer physikalischen Standleitung wird die Verbindung beim PVC erst bei Verbindungsanforderung durch den Vermittlungsrechner geschaltet.

— Anschlüsse können so konfiguriert werden, daß sie wahlweise nur für ankommende oder nur für abgehende Verbindungen freigeschaltet sind.

Damit wird zumindest ein Standard erreicht, der auch bei anderen paketvermittelten Diensten gewährleistet wird (z.B. Datex-P).

Leider wird – entgegen unseren Anregungen – vom LIT bislang noch kein Dienst zur Datenverschlüsselung angeboten, der allein dem Abhörrisiko wirksam begegnen könnte. Das LIT hat jedoch zugesagt zu prüfen, ob ein Verschlüsselungsdienst zu einem späteren Zeitpunkt als Leistungsmerkmal angeboten werden kann. Es bleibt also zumindest vorerst Sache des Anwenders, bei Übertragung sensibler Daten für eine sichere Verschlüsselung zu sorgen.

Da sich die Verantwortung des LIT als Betreiber des X.25-Dienstes nicht auf die lokalen Komponenten (z.B. lokale Netze und dezentrale Rechner) erstreckt, müssen die Anwender zusätzlich zu den vom LIT angebotenen Sicherheitsdiensten eigene Maßnahmen ergreifen, um eine unberechtigte Nutzung des Dienstes oder einen unberechtigten Zugriff auf lokale Daten aus dem Netz (insb. Hacking) zu verhindern.

Zu den Obliegenheiten des Anwenders gehört insbesondere die konsequente Verwaltung von X.25-Nutzerkennungen und eine restriktive, aufgabenbezogene Vergabe von Zugriffsrechten. Desweiteren kann sich – insbesondere bei der Verarbeitung sehr sensibler personenbezogener Daten – die Notwendigkeit ergeben, Zugriffe aus und auf den X.25-Dienst besonders zu protokollieren, um einen möglichen Mißbrauch aufdecken zu können.

3.4 X.400-Dienst – elektronische Post in der hamburgischen Verwaltung

Bereits seit 1990 beschäftigt sich die hamburgische Verwaltung mit der Einführung eines einheitlichen Systems für den behördenübergreifenden elektronischen Versand von Dokumenten. In einem 1991 begonnenen Pilotprojekt sollten die technischen, organisatorischen und fachlichen Anforderungen für ein flächendeckendes „Electronic Mail" (EM) ermittelt werden. Obwohl seinerzeit die entsprechende Technik installiert worden war, verlief das Pilotprojekt im Sande; ein Zwischenbericht kam 1992 über das Entwurfsstadium nicht hinaus, und ein Abschlußbericht wurde gar nicht erst begonnen. Da wir uns von dem Pilotprojekt auch Erkenntnisse darüber erhofft hatten, wie der Dienst datenschutzgerecht gestaltet werden könnte, war der formlose „Abschluß" des Projekts recht enttäuschend.

Durch Unterabschnitt 2.5.2 der Telekommunikationsrichtlinie vom 26. Januar 1993 (TK-RL – vgl. 12.TB, 3.5) wurde der Versand von Dokumenten mittels EM in der hamburgischen Verwaltung grundsätzlich zugelassen. Die TK-RL enthält die Vorgabe, daß gegen die unbefugte Einsichtnahme und die irrtümliche Zustellung der Dokumente geeignete technische und organisatorische Maßnahmen zu treffen sind. Insbesondere dürfen die Endeinrichtungen nicht unkontrolliert zugänglich sein, und gespeicherte Dokumente sind durch Sicherungsmaßnahmen zu schützen.

Die Arbeiten an der Realisierung von EM wurden erst im Jahr 1994 wieder aufgenommen. Im Mai 1994 erfuhren wir von der Finanzbehörde – Amt für Informations- und Kommunikationstechnik –, daß das Landesamt für Informationstechnik (LIT) plane, den Behörden bis Ende 1994 einen X.400-basierten elektronischen Postdienst zur Verfügung zu stellen. In den daraufhin mit der Finanzbehörde und dem LIT geführten Gesprächen haben wir darauf hingewiesen, daß mit einem flächendeckenden X.400-Angebot erhebliche datenschutzrechtliche Probleme verbunden sind, die gelöst werden müssen, ehe ein entsprechendes System eingeführt werden kann:

— Die Sicherheit der Übertragung ist auf dem gesamten Weg (auf Übertragungsleitungen und auf Rechnern, die als elektronische „Postämter" für die Zustellung zu sorgen haben und Nachrichten zwischenspeichern) zu gewährleisten. Dazu ist es erforderlich, sowohl Mechanismen gegen die unbefugte Kenntnisnahme (insb. Verschlüsselung) als auch gegen Verfälschung, Wiedereinspielung und Fehlleitung zu treffen.

— Sofern EM auf Systemen abgewickelt werden soll, die auch für andere Verfahren – z.T. auch mit sensiblen personenbezogenen Daten – eingesetzt werden, besteht die Gefahr, daß Daten aus den automatisierten Verfahren übernommen und mittels EM an Dritte versandt werden. Aus diesem Grund sollten gesonderte Mailserver als „Postamtsrechner" eingesetzt werden; im übrigen müssen die Anwendungen konsequent von den Mailfunktionen getrennt werden.

— Schließlich ist danach zu fragen, ob ein EM-System für die Aufgabenerfüllung jeweils erforderlich und angesichts der verbleibenden Restrisiken für den Datenschutz vertretbar ist.

Das LIT hat einen Zwischenbericht über sein EM-Projekt vorgelegt. Dieser Zwischenbericht besteht bezüglich der Verfahrenssicherheit lediglich aus einem Abdruck der entsprechenden Ausführungen aus dem Entwurf des Projektberichts aus dem Jahr 1992. Dieser Bericht enthält keine Erkenntnisse über X.400-Software, die dem Standard von 1988 entspricht, da derartige Software seinerzeit nicht getestet wurde. Der 88er Standard beinhaltet jedoch einige für die Gewährleistung des Datenschutzes erhebliche Neuerungen. Das LIT hat zugesagt, das Sicherheitskonzept bis Ende 1994/Anfang 1995 entsprechend zu ergänzen.

Wir erwarten von der Fortschreibung des Sicherheitskonzepts ferner, daß auf die datensicherungstechnischen Wechselwirkungen zwischen den Komponenten eingegangen wird, die an dem EM-System beteiligt sind (Rechnerbetriebssysteme, lokale Netze, Telekommunikationsnetz der FHH, X.25-Datenübermittlungsdienst – vgl. 3.3 – und spezielle EM-Software).

Die in dem Zwischenbericht des LIT enthaltene Aussage, daß Arbeitsplatzrechner und die als „Behördenpostamt" genutzten UNIX-Systeme auch für weitere Mehrwertdienste eingesetzt werden können, ist problematisch. Gegen eine derartige Mehrfachnutzung hätten wir nur dann keine Bedenken, wenn die grundlegenden Sicherheitsprobleme gelöst sind. Dabei ist insbesondere darauf hinzuweisen, daß bei UNIX-Rechnern der Systemverwalter auf die mit der Mail-Funktion übertragenen Daten grundsätzlich lesend, ändernd oder löschend zugreifen kann, sofern keine wirksamen Gegenmaßnahmen ergriffen werden (vgl. hierzu unsere Broschüre „Datenschutzkonzept für UNIX-Mehrplatzanlagen", 5.1).

Eine von der Finanzbehörde im Juni 1994 zugesagte Risikoanalyse fehlt noch gänzlich. In dieser Risikoanalyse sollen die Sicherheitsmaßnahmen dargestellt werden, die – auch bezogen auf die Sensibilität der jeweils verarbeiteten Daten – aus Sicht der anwendenden Behörden erforderlich sind.

Parallel zu diesen Vorhaben hat sich auch das Projekt Personalwesen (PROPERS, vgl. 7.1) mit der Einführung von EM befaßt. Im Hinblick darauf, daß in der Personalverwaltung zum großen Teil hochsensible Personaldaten verarbeitet werden, erscheint uns dieser Bereich als weniger geeignet, hier erste Erfahrungen mit dem Einsatz von EM zu sammeln. Zudem würde es schwerwiegenden datenschutzrechtlichen Bedenken begegnen, wenn die PROPERS-Rechner als zentrale Behördenpostämter auch für die übrigen Bereiche der Behörden dienen sollen.

Wir gehen davon aus, daß angesichts der grundlegenden datenschutzrechtlichen Bedeutung, die der elektronischen Post zukommt, vor der Inbetriebnahme des übergreifenden EM-Systems die noch zu erarbeitenden bzw. zu aktualisierenden Sicherheitskonzepte der Finanzbehörde und des LIT mit uns abgestimmt werden.

3.5 Absicherung von Telekommunikations-Anlagen

Im landeseigenen Telekommunikationsnetz der hamburgischen Verwaltung werden derzeit mehr als sechzig große Fernsprechnebenstellenanlagen betrieben. Dabei handelt es sich überwiegend um elektronische Telekommunikationsanlagen (TK-Anlagen). Noch im Einsatz befindliche mechanische Systeme werden Zug um Zug gegen moderne und mehrdienstefähige TK-Anlagen ersetzt.

Die TK-Anlagen sind an ihren jeweiligen Standorten in eigens dafür hergerichteten Räumen untergebracht. Diese Räume sind mit Sicherheitsschlössern versehen. Die Schlüssel werden bei Pförtnern, Polizeirevierwachen oder dem für die Aufrechterhaltung des Betriebs zuständigen Personal des Landesamtes für Informationstechnik aufbewahrt. Die Schlüssel werden nur an zutrittsbefugte Mitarbeiter ausgehändigt. Die Übergabe wird in Schlüsselbüchern protokolliert.

Hinsichtlich der räumlichen Absicherung und der Erhaltung der Funktionsfähigkeit der TK-Anlagen sind grundsätzlich Schutzmaßnahmen getroffen worden (z.B. einbruchhemmende Türen und Fenster, Brandabschottung der Kabeltrassen, unterbrechungsfreie Stromversorgung). Die Erhöhung des Gefährdungspotentials durch Einbruch und Vandalismus, aber vor allem auch datenschutzrechtliche Problemstellungen erfordern jedoch zusätzliche Sicherheitsmaßnahmen.

Bei dem Einsatz elektronischer TK-Anlagen kommt es zur Verarbeitung von personenbezogenen Teilnehmer- und Verbindungsdaten. Daher ist eine Manipulation der Software für den Verbindungsaufbau und die unzulässige Speicherung und Auswertung der genannten Daten zu verhindern. Besondere Gefahren aus datenschutzrechtlicher Sicht, die sich aus dem Zugang zu den TK-Anlagen ergeben, liegen auch in einem unbefugten Aufschalten zum Mithören der Telefongespräche, die über die jeweilige Nebenstellenanlage geführt werden.

Neben der Sprachkommunikation werden die TK-Anlagen auch zunehmend für die behördenübergreifende Datenkommunikation zwischen Rechnern genutzt. Gemäß § 8 Abs. 1 HmbDSG sind deshalb technische und organisatorische Maßnahmen zu treffen, die geeignet sind, den Schutz der dem Fernmeldegeheimnis unterliegenden Daten zu gewährleisten. Außerdem ist sicherzustellen, daß nicht unbefugt in DV-Systeme eingedrungen werden kann, die an das Netz angeschlossen sind.

Da die Software der derzeit eingesetzten TK-Anlagen die Einrichtung von individuellen Benutzerkennungen und Paßworten für die einzelnen Wartungstechniker nicht vorsieht, können die oben genannten Anforderungen aus unserer Sicht nur durch ein revisionssicheres räumliches Zugangskontrollsystem erfüllt werden. Dieses muß technisch so gestaltet sein, daß der Zutritt zu den Räumen nur nach Prüfung der Zugangsberechtigung gewährt wird. Jedes Betreten und Verlassen der Räume ist chronologisch zu erfassen und zu protokollieren. Die Vergabe, der Entzug und bei Bedarf die Sperrung von Zugangsberechtigungen sind zentral zu dokumentieren.

Eine Arbeitsgruppe der Fernmeldeabteilung der Baubehörde (jetzt Landesamt für Informationstechnik) hatte unter Mitwirkung eines externen Unternehmens bereits im Jahr 1992 konkrete Anforderungen an ein erweitertes Sicherheitssystem definiert. Neben den zuständigen Personalräten und dem Senatsamt für den Verwaltungsdienst – Organisationsamt – (jetzt Finanzbehörde – Amt für Informations- und Kommunikationstechnik –) waren auch wir in dieser Arbeitsgruppe vertreten. Das neue Schutzkonzept sah ein personenbezogenes Zugangskontrollsystem für alle Räume vor, in denen große TK-Anlagen installiert sind.

Mit an den Türen angebrachten Zugangssicherungs-Terminals sollte berechtigten Personen ein ungehinderter Zugang gewährt und unberechtigten Personen der Zutritt verwehrt werden. Alle Ereignisse sollten an einen zentralen Rechner (Leitstand) gemeldet und dort erfaßt werden. Der Zugang sollte nur über eine personenbezogene Chipkarte erfolgen können und zentral auf dem Rechner dokumentiert werden. Vom Leitstand aus sollte auch die Sperrung einzelner Zugangsberechtigungen möglich sein. Unregelmäßigkeiten, z.B. abgewiesene Zugangsversuche oder Meldungen bei Türöffnungsüberschreitungen, sollten an dem zentralen Bedienplatz angezeigt werden.

Mit den für die Umsetzung dieses Konzeptes erforderlichen finanziellen Mitteln sollte Jahr für Jahr eine bestimmte Anzahl von Räumen an das neue Sicherungssystem angeschlossen werden. Begonnen werden sollte mit den mehrdienstefähigen TK-Anlagen. Eine entsprechende Haushaltsunterlage für die ersten zwanzig Anlagen wurde Anfang 1993 erstellt. Wegen der personenbezogenen Identifikation und Dokumentation des örtlichen Zugangs war die förmliche Beteiligung des Personalrats bereits vorbereitet worden. Durch die Einrichtung des Landesamtes für Informationstechnik (LIT) und die damit verbundene Veränderung von Zuständigkeiten mußte das Vorhaben jedoch zunächst zurückgestellt werden.

Im Juli 1993 wurde uns vom LIT auf Nachfrage mitgeteilt, daß man beabsichtige, das bereits erstellte Sicherheitskonzept zu überarbeiten, um eine kosten-

günstigere Lösung zu erreichen. Insbesondere wolle man auf die Speicherung und Kontrolle der Bewegungsdaten auf einem zentralen Rechner verzichten. Wir haben daraufhin deutlich gemacht, daß wir die jetzt beabsichtigte Abkehr von der personenbezogenen Identifikation des räumlichen Zugangs nicht akzeptieren könnten.

Daraufhin hat das LIT im Februar 1994 angekündigt, für die zusätzliche Absicherung der TK-Anlagen eine neue Zieldefinition zu erarbeiten. Diese sollte berücksichtigen, daß die Einrichtung eines zentralen Leitstandes erst nach dem für Mitte 1995 vorgesehenen Umzug des LIT in ein neues Gebäude möglich ist. Dies hätte zur Folge gehabt, daß noch im Jahr 1994 eine Haushaltsunterlage für Baumaßnahmen zu erstellen gewesen wäre, um für 1996 über erste erforderliche Mittel zu verfügen. Daneben wäre ein Mindeststandard für die Übergangszeit zu schaffen gewesen.

Mit Redaktionsschluß dieses Tätigkeitsberichts erhielten wir von der Finanzbehörde – Amt für Informations- und Kommunikationstechnik – Einsicht in Unterlagen des LIT über ein in Teilen verringertes Sicherheitskonzept sowie die dafür erforderlichen Kosten. Dieses Konzept sieht weiterhin die personenbezogene Identifikation und die zentrale Aufschaltung von Ereignismeldungen vor. Allerdings gab die Finanzbehörde zu verstehen, daß sie von dem Sinn der beschriebenen zusätzlichen Maßnahmen noch immer nicht überzeugt sei.

Wir haben in ausführlicher Diskussion deutlich gemacht, daß ein Verzicht auf ein zentrales Zugangskontrollsystem nur dann in Frage kommt, wenn durch die Software der TK-Anlagen selbst die Vergabe von individuellen Zugriffsberechtigungen ermöglicht wird. Wartungsarbeiten auf der TK-Anlage sind revisionssicher zu protokollieren. Ist dies gewährleistet, kann für solche TK-Anlagen auf eine elektronische räumliche Zugangssicherung verzichtet werden, wenn gleichzeitig eine strikte Schlüsselverwaltung erfolgt. Die Finanzbehörde hat zugesagt, gemeinsam mit dem LIT die Ausstattung der derzeit genutzten TK-Anlagen zu prüfen.

3.6 Risiken beim Betrieb von Terminal-Servern

Im Zuge der voranschreitenden Umstellung der IuK-Infrastruktur auf heterogene Netze kommen häufig Terminal-Server zum Einsatz, um Terminals als Teil der bestehenden DV-Ausstattung weiterhin nutzen zu können. Dies führt bei den in der Regel verwendeten broadcastorientierten Netzen auf Ethernet-Basis zu einem – gegenüber der traditionellen, direkten Anbindung von Terminals an den Host-Rechner – erhöhten Sicherheitsrisiko.

Dieses Risiko besteht darin, daß der Datenverkehr zwischen Terminal und Host in dem gesamten Netzsegment verfügbar ist, an das der Terminal-Server angeschlossen ist. Dies schließt nicht nur die volle Länge des verwendeten Kabels, sondern insbesondere alle daran installierten Anschlüsse ein. Die Gefahr

des unberechtigten Abhörens ist damit weit höher als beim direkten Anschluß an den Host. Zudem können dabei die Daten aller an das abgehörte Segment angeschlossenen Terminals ausgewertet werden, wovon u.U. eine Vielzahl von Verfahren betroffen ist.

Die besondere Problematik liegt hierbei darin, daß herkömmliche Technik über eine moderne Infrastruktur betrieben wird. Sicherungsmaßnahmen, die die erhöhten Risiken dieser Infrastruktur kompensieren könnten, sind dabei nicht einsetzbar. Während über heterogene Netze betriebene Client-Server-Verfahren durch den Einsatz geeigneter Netz-Betriebssysteme relativ sicher gestaltet werden können (siehe Kapitel 7 unserer Broschüre „Datenschutz in Netzen"), ist dies beim Anschluß von Terminals nicht möglich. Weder kann eine Differenzierung zwischen Inhalts- und Verbindungsdaten oder zwischen unterschiedlich schützenswerten Daten vorgenommen werden, noch ist ein Schutz der Dateninhalte überhaupt möglich. So werden Kennungen und dazugehörige Paßwörter ebenso in Klarform übertragen wie alle anderen Daten auch.Verschlüsselung oder andere Techniken zur Sicherung der Dateninhalte liegen außerhalb der Möglichkeiten heutiger Terminal-Server.

Als einzig wirksame Maßnahme bleibt daher die möglichst weitgehende Abkehr vom Broadcast-Prinzip, wie bereits im 12. TB (3.3.1) ausgeführt wurde. Durch eine verfahrensorientierte Segmentierung der Netze in Kombination mit filternden Sternkopplern wird eine Streuung der sensiblen Daten über weite Teile des Netzes vermieden und das Abhörrisiko auf wenige Leitungen bzw. solche Anschlüsse begrenzt, die baulich besonders geschützt sind. Diese Anforderung muß frühzeitig bei der Planung eines Vernetzungsvorhabens berücksichtigt werden.

Beim Anschluß aktiver Endgeräte wie PCs sollte jedoch – ggf. zusätzlich – von der Möglichkeit der Verschlüsselung Gebrauch gemacht werden, um Paßwörter oder sensible personenbezogene Daten im Netz zu schützen. Verschlüsselungsdienste werden außer von Netz-Betriebssystemen auch von Netz-Sicherheitssoftware (z.B. Kerberos) angeboten oder können direkt in die Verfahren eingebunden werden.

3.7 Transparenz und Qualität von Verschlüsselungsverfahren

Bei der Verarbeitung besonders sensibler Daten wird von Seiten der Datenschutzbeauftragten häufig die Verschlüsselung dieser Daten gefordert. Keine andere Einzelmaßnahme ermöglicht einen vergleichbar hohen Schutz personenbezogener Daten vor dem Zugriff Unberechtigter. Auch wir haben in unseren bisherigen Broschüren und in unserer beratenden und kontrollierenden Tätigkeit auf diesen Umstand hingewiesen und in entsprechenden Fällen auf eine Umsetzung dieser Maßnahme gedrängt.

Dabei stellt die Beurteilung von konkreten Verschlüsselungsverfahren oder -produkten jedoch ein erhebliches Problem dar, da eine eigenständige Qualitätsprüfung solcher Verfahren durch die Datenschutzbeauftragten in der Regel nicht möglich ist. Wir sind daher auf die wissenschaftliche Fachkenntnis anderer angewiesen, um uns ein Bild über die Güte der verfügbaren kryptografischen Methoden zu verschaffen und ihre Einsatzmöglichkeiten in der Datenschutzpraxis zu bewerten.

Da der formale Beweis der Sicherheit eines Verfahrens im allgemeinen nicht möglich ist, muß auf schwächere Methoden zurückgegriffen werden. Dabei bietet die Diskussion in der Fachöffentlichkeit die besten Beurteilungsmöglichkeiten für Außenstehende. Verfahren, die in diesem Rahmen intensiv und dauerhaft thematisiert werden, sind daher für Datenschutzbeauftragte von besonderer Bedeutung. Da voraussichtlich die Gefahr unerkannter Sicherheitslücken oder anderer Schwächen von Verschlüsselungsverfahren umso kleiner ist, je ausführlicher sie begutachtet wurden, können solche Verfahren als die sichersten unter den bekannten gelten.

Demgegenüber sind Verfahren, die einer solchen öffentlichen kritischen Würdigung entzogen sind, für Außenstehende kaum zu beurteilen. Dies gelingt allenfalls indirekt, indem dem Einzelurteil einer vertrauenswürdigen Instanz, die das Verfahren geprüft hat, mehr oder weniger gefolgt wird. Die zusätzliche Sicherheit, die bei einer Geheimhaltung des Verfahrens gewonnen werden kann, relativiert sich dabei rasch. Zwar ist der Faktor „security by obscurity" (d.h. Sicherheitsgewinn durch Geheimhaltung) nicht zu verleugnen. Je weniger Informationen einem Angreifer zur Verfügung stehen, desto schwieriger wird sein Versuch werden, das Verfahren zu entschlüsseln. Andererseits ist eine ganze Reihe sehr sicherer Verschlüsselungsverfahren verfügbar, deren hohe Qualität nicht in der Geheimhaltung ihrer Funktionsweise begründet liegt. Solchen Verfahren ist aus Sicht des Datenschutzes der Vorzug zu geben.

Dabei zeigt die technische Entwicklung – insbesondere im Hardware-Bereich –, daß auch die bestehenden, bewährten Verfahren kontinuierlich am Stand der Technik gemessen werden müssen. So sind heutzutage durch leistungsfähige PCs Rechenkapazitäten für jedermann verfügbar, die vor zehn Jahren noch den Betrieb eines kleineren Rechenzentrums erfordert hätten. Sogenannte Brute-Force-Methoden zur unberechtigten Entschlüsselung, die sämtliche denkbaren Kombinationen systematisch durchprobieren, rücken in manchen Fällen plötzlich in den Bereich des Möglichen.

Dieser Entwicklung unterliegen sowohl ältere Verfahren wie z.B. DES als auch modernere Entwicklungen wie RSA. Da die Länge der verwendeten Schlüssel (im allgemeinen gemessen in Bits) eine entscheidende Rolle für die Möglichkeit eines solchen Brute-Force-Angriffs spielt, besteht bei Verfahren, die eine freie Wahl der Schlüssellänge erlauben (z.B. RSA), die Möglichkeit, die technische Fortentwicklung durch eine Verlängerung des Schlüssels in fast beliebigem Umfang zu kompensieren. So wurde zwar kürzlich das RSA-Verfahren bei 129-stelligem Schlüssel (entsprechend 429 Bits) in achtmonatiger Arbeit mehrerer hundert Rechner geknackt. Bei Verwendung von Schlüsseln mit doppelter oder vierfacher Länge sind solche Versuche jedoch weit außerhalb des in absehbarer Zeit Möglichen. Der erzielte Verschlüsselungsschutz ist daher für heutige Verhältnisse sehr gut.

Im Gegensatz dazu stoßen Verfahren mit fester Schlüssellänge (z.B. DES mit 56 Bits) bereits heute an ihre Grenzen. So ist etwa die Sicherheit von Paßwörtern unter dem Betriebssystem UNIX, die mit dem DES-Verfahren verschlüsselt gespeichert werden, mittlerweile nur noch bei voller Ausschöpfung der maximalen Paßwortlänge und des gesamten Zeichenvorrats gegeben. Bei geringerer Länge oder eingeschränkter Zeichenmenge können UNIX-Paßwörter mit heutiger Standardtechnik in erträglicher Zeit entschlüsselt werden (z.B. Paßwörter aus maximal sechs Kleinbuchstaben innerhalb von höchstens fünf Tagen). Die Maßnahme, in neueren UNIX-Versionen die verschlüsselten Paßwörter vor den neugierigen Augen sämtlicher Benutzer zu schützen, ist zwar eine richtige Reaktion auf diese Tatsache, kann aber letztlich nicht mehr als ein Notbehelf sein.

Andererseits kann bei Verwendung hochwertiger Verfahren die heute allgemein verfügbare Rechenkapazität für einen Verschlüsselungsschutz eingesetzt werden, der die Vertraulichkeit wichtiger Daten gegenüber sämtlichen denkbaren Interessenten in nahezu perfekter Weise sicherstellt. Betrachtet man die ergänzenden Dienste, die auf Verschlüsselungstechnik basieren (elektronische Unterschrift, Herkunfts- und Empfangsnachweis elektronisch versandter Dokumente usw.), kann die Kryptologie mit Recht als „Schlüsseltechnologie" bezeichnet werden, von der auch der Datenschutz weiterhin profitieren wird.

3.8 Optische Medien/Archivierung

Für die Archivierung umfangreicher Datenbestände wird in Wirtschaft und Verwaltung zunehmend von der Möglichkeit der Speicherung auf optischen Medien Gebrauch gemacht. Datenschutzrechtlich problematisch sind hierbei vor allem das Sperren und Löschen personenbezogener Daten gemäß § 19 HmbDSG bzw. § 35 BDSG. Für die Beurteilung, inwieweit eine effektive Sperrung bzw. Löschung von Daten auf optischen Speichern überhaupt technisch möglich ist, haben wir die verschiedenen Aufzeichnungsverfahren näher betrachtet.

Optische Datenträger wie die CD-ROM und WORM-Platten (write once read multiple) arbeiten ohne aufwendige Magnettechnik. Lesen und Beschreiben erfolgen allein über die jeweils unterschiedliche Intensität, mit der ein Laserstrahl auf die Oberfläche des Datenträgers gerichtet wird. Das reflektierte Licht wird aufgefangen und in lesbare Zeichen umgesetzt. Bei der CD-ROM erfolgt

das Beschreiben bislang noch vorwiegend fabrikmäßig in Presswerken. Allerdings werden zunehmend auch CD-ROM-Laufwerke auf dem Markt angeboten, die das individuelle Beschreiben von CD-ROM erlauben. Bei einer WORM-Platte kann jede unbeschriebene Stelle ein einziges Mal mit Daten beschrieben werden und wie eine CD-ROM beliebig oft gelesen werden. Ein nachträgliches Löschen, Überschreiben oder Ändern von Daten ist weder bei CD-ROM noch bei WORM-Platten technisch möglich.

Magneto-optische Datenträger haben anders als optische Speicher eine magnetisierbare Metalloberfläche, die ein stärkerer Laserstrahl erwärmen und zum Schmelzen bringen kann (beschreiben). Zusätzliche Magnete sorgen dabei dafür, daß sich die punktgenau erhitzte Oberfläche je nach beabsichtigter Bedeutung in eine bestimmte Richtung dreht. Ein schwächerer Laserstrahl wird dagegen entsprechend der magnetischen Polung vom Metall reflektiert und interpretiert (lesen). Datenträger, die nach dem magneto-optischen Aufzeichnungsverfahren arbeiten, werden MOD (modifiable optical disc) genannt. Hierauf ist das Löschen und mehrfache Überschreiben von Daten technisch möglich.

Gemäß § 3 Abs. 5 BDSG bzw. § 4 Abs. 2 HmbDSG ist Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten. Diese Anforderung können WORM-Platten nicht erfüllen. Jeder optische Datenträger enthält ein eigenes Filesystem, in dem die Adressen der auf der Platte gespeicherten Daten verzeichnet sind. Bei WORM-Platten kann aufgrund der oben beschriebenen Aufzeichnungstechnik kein Überschreiben bereits gespeicherter Daten erfolgen.

Um einen Datensatz oder ein bestimmtes Datenfeld zu löschen, wird deshalb an das Inhaltsverzeichnis ein entsprechender Zusatz angehängt (auf einer noch nicht beschriebenen Stelle des Datenträgers). Wird auf die WORM zugegriffen, liest die Archivierungssoftware das gesamte Verzeichnis von der Optical Disc und erzeugt anhand der zusätzlichen „Nachträge" ein aktuelles Inhaltsverzeichnis auf der Festplatte des Rechners, d.h. das Filesystem wird jeweils anhand der Zusatzeinträge aktualisiert.

Auf diese Weise werden tatsächlich auf der WORM noch enthaltene Daten als gelöscht interpretiert. Ein Zugriff ist dann zumindest über die Standardsoftware ausgeschlossen. Allerdings können WORM-Platten mit spezieller Software auch unter Umgehung des aktuellen Inhaltsverzeichnisses gelesen werden, so daß auch die nachträglich als „gelöscht" markierten Daten weiterhin abrufbar sind.

Im Gegensatz zum HmbDSG bietet das BDSG jedoch eine Ausnahmeregelung. Gemäß § 35 Absatz 3 Nr. 3 BDSG kann das eigentlich erforderliche Löschen durch das Sperren ersetzt werden, wenn eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem

Aufwand möglich ist. Sperren ist das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken (§ 3 Abs. 5 Nr. 4 BDSG). Dies schließt demnach nicht zwingend aus, daß auf gesperrte Daten mit Hilfe spezieller Programme im Einzelfall doch zugegriffen werden kann. Insofern wäre rein theoretisch auch bei Verwendung von WORM-Platten eine Erfüllung der Anforderungen an die Löschung nach dem BDSG möglich. Das Inhaltsverzeichnis auf dem Datenträger erhält dann die oben beschriebenen Zusätze, die von der Archivierungssoftware als Sperren (bzw. Löschen) interpretiert werden.

Nach § 4 Abs. 2 Nr. 5 HmbDSG muß dagegen auch schon das Sperren so erfolgen, daß jede weitere Verarbeitung der Daten verhindert wird. Für den Anwendungsbereich des HmbDSG ist daher festzuhalten, daß WORM-Platten nicht geeignet sind, die datenschutzrechtlichen Anforderungen an die Sperrung und Löschung personenbezogener Daten zu erfüllen.

Auch für den Anwendungsbereich des BDSG muß die Frage erlaubt sein, inwieweit die oben beschriebene Problematik nicht im Rahmen einer Risikoanalyse vor der Einführung neuer Speichertechnik zu berücksichtigen ist. MOD bieten gegenüber WORM-Platten eine vergleichbare Speicherdichte und ein ähnliches Zugriffsverfahren. Der Aufwand für den Einsatz dieser Technik steht deshalb durchaus in einem angemessenen Verhältnis zu dem damit erreichbaren Schutzzweck. Um eine datenschutzgerechte Löschung gewährleisten zu können, sollten daher auch im Anwendungsbereich des BDSG bei sensiblen personenbezogenen Daten von vornherein nur MOD verwendet werden.

Ist in einem Automationsverfahren bereits WORM-Speichertechnik im Einsatz, sollten die Datenträger in regelmäßigen, möglichst kurzen Abständen kopiert werden. Dabei werden entsprechende Zusatzeinträge im Inhaltsverzeichnis berücksichtigt und zu löschende Daten nicht mit übertragen. Die bisher genutzten Speichermedien sind anschließend zu vernichten. Nur so können bislang hierauf nur logisch nicht mehr verfügbare Daten auch physikalisch unwiderruflich „gelöscht" werden.

3.9 Mandantenfähige Informationssysteme

Ein wesentliches Kriterium für die Zulässigkeit der Verarbeitung personenbezogener Daten ist das Erforderlichkeitsprinzip: Daten dürfen nur dann verarbeitet werden, wenn dies zur Erfüllung der Aufgabe bzw. zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist. Aus diesem generellen, in den Datenschutzgesetzen festgelegten Prinzip läßt sich auf technisch-organisatorischer Ebene ein Grundsatz ableiten, der unter dem Begriff „need-to-know" bekannt ist. Damit wird ein Konzept bezeichnet, mit dem sichergestellt werden soll, daß jeder genau diejenigen Daten bearbeiten kann, die er oder sie zur Aufgabenerfüllung benötigt – nicht weniger, aber auch nicht mehr.

Die Umsetzung dieses Konzepts durch konkrete technische und organisatorische Maßnahmen ist umso wichtiger, je umfassender die Datenmengen sind, auf die arbeitsteilig zugegriffen wird, und je größer deren Sensibilität ist. Bei Datenbankanwendungen, die auf einer unternehmens- oder behördenweit zentralen Datenhaltung basieren, kommt diesem Konzept besondere Bedeutung zu. Der Zugriff auf die Daten muß entsprechend der arbeitsteiligen Abgrenzung eingeschränkt werden, etwa nach örtlicher Zuständigkeit bestimmter Zweigstellen oder Ämter, nach Zuständigkeit anhand der Namen – z.B. für die Anfangsbuchstaben A bis E der Nachnamen – oder anderer Merkmale der gespeicherten Personen. Systeme, die eine solche Abgrenzung ermöglichen, werden als „mandantenfähig" bezeichnet.

Aus technischer Sicht kommt eine Umsetzung dieser Maßnahme auf zwei Ebenen in Betracht: Zum einen kann die Mandantenfähigkeit auf Ebene der Anwendung durch eine entsprechende Programmierung gewährleistet werden, zum anderen können Mechanismen direkt auf Ebene des Datenbanksystems genutzt werden.

Zwar ist die bloß anwendungsbezogene Umsetzung vom eingesetzten Datenbanksystem unabhängig und daher universell, andererseits ist sie mit einer ganzen Reihe von Nachteilen verbunden. Neben dem hohen Implementationsaufwand und dem damit verbundenen Risiko durch Programmierfehler ist vor allem nachteilig, daß die so festgelegten Beschränkungen nur beim Zugriff auf die Daten mit Hilfe dieser Anwendung gelten, nicht aber generell bei Benutzung der zugrundeliegenden Datenbank. Eine Umgehung dieses Schutzes kann daher nicht ausgeschlossen werden.

Aus diesen Gründen sind für arbeitsteilig genutzte Datenbestände solche Datenbanksysteme vorzuziehen, die die Mandantenfähigkeit durch geeignete Mechanismen selbständig sicherstellen können. Dabei tritt die Schwierigkeit auf, daß die Zugriffsberechtigung für einen Datensatz von seinem Inhalt (z.B. vom Namen der gespeicherten Person) abhängig ist und insofern erst beim Zugriffsversuch bestimmt werden kann. Ein statischer, fest an den Datensatz gebundener Zugriffsschutz, den die meisten Datenbanksysteme bieten, wird dieser Anforderung nicht gerecht. Als geeignete Mechanismen kommen jedoch sogenannte Sichten (views) oder das Verfahren der Abfragemodifikation (query modification) in Betracht.

Das View-Konzept der Datenbanksprache SQL (Structured Query Language) ermöglicht es, die „Sicht" auf eine Datenbank benutzerspezifisch und abhängig von Datensatzinhalten einzuschränken. Ein Benutzer kann so nur denjenigen Ausschnitt aus der Datenbank bearbeiten, der ihm durch die View-Definition zur Verfügung gestellt wird, z.B. von allen gespeicherten Personen nur diejenigen mit einem bestimmten Wohnort. Ändern sich die Wohnorte der Personen (etwa durch Umzug), ändert sich entsprechend auch die Menge der Datensätze, auf die dieser Benutzer zugreifen kann. Der andere Teil der gespeicherten Daten ist für diesen Benutzer dabei gleichsam nicht vorhanden, durchaus aber für andere Benutzer mit anderen Zuständigkeiten und Zugriffsrechten.

Die Abfragemodifikation, über die z.B. die Datenbanksysteme ADABAS oder INGRES verfügen, basiert auf der automatischen Ergänzung des formalen Ausdrucks, mit dem ein Datenbankzugriff durchgeführt wird. Auf diese Weise werden durch das Datenbanksystem umfassende Zugriffsversuche – entsprechend festgelegter Zugriffsregeln – auf das gewünschte Maß eingeschränkt. Auch dies geschieht benutzerbezogen und in Abhängigkeit der Dateninhalte.

Insgesamt sind diese Mechanismen zwar mit gewissen Geschwindigkeitseinbußen verbunden und führen so zu längeren Antwortzeiten. Bei der Mandantenfähigkeit handelt es sich jedoch um ein entscheidendes Prinzip zur Wahrung elementarer Datenschutzbelange. Wir haben diese Sicherung bei zentralen Datenbanksystemen daher stets gefordert und halten dies bei der anhaltenden Tendenz zu übergreifenden Zugriffen auf personenbezogene Daten für immer relevanter.

Einzelne Probleme des Datenschutzes im öffentlichen Bereich

4. Telekommunikation/Neue Medien

4.1 Projekt Interaktives Fernsehen

Die Handelskammer Hamburg hat ein Pilotprojekt Interaktives Fernsehen initiiert. Bei den Vorgesprächen für dieses Projekt, an denen auch der Hamburgische Datenschutzbeauftragte beteiligt war, sollten zunächst die technischen, wirtschaftlichen und rechtlichen Voraussetzungen für interaktive Dienste geklärt werden. Dabei kamen sowohl reine Fernsehanwendungen als auch Anwendungen aus dem Handel und dem Dienstleistungssektor zur Sprache.

Inzwischen ist eine von verschiedenen Firmen getragene Gesellschaft für Digitales und Interaktives Fernsehen (DITV) gegründet worden, die den für Mitte 1995 vorgesehenen Start des Pilotprojekts vorbereiten soll. In das Projekt sollen zunächst 1.000 Hamburger Haushalte einbezogen werden, von denen jedoch nur 100 einen voll interaktiven Breitbandanschluß bekommen sollen und die damit gezielt gespeicherte Filme oder Firmenvideos abrufen können (video on demand). Bei den restlichen Haushalten soll die Rückkopplung über ISDN erfolgen. Sie können zwar keine Filme direkt abrufen; ihnen soll jedoch ein gegenüber normalen „Kabelkunden" erheblich ausgeweitetes Angebot zur Verfügung gestellt werden, indem sie Zugriff auf zusätzliche Übertragungskanäle bekommen (near video on demand).

Die besondere Problematik interaktiver Dienste besteht darin, daß jeweils Verbindungsdaten und Abrechnungsdaten über die Nutzung, insbesondere über den Zugriff auf bestimmte Informationen entstehen und benötigt werden. Diese Daten könnten ausgewertet und zu Mediennutzungsprofilen zusammengeführt werden (vgl. 12.TB 4.2).

Bei der konkreten Ausgestaltung des Pilotprojektes sollen Abrechnungsverfahren erprobt werden, bei denen keine oder möglichst wenige Daten über das Informations-, Fernseh- und Kommunikationsverhalten der Betroffenen entstehen. Wir würden es begrüßen, wenn für die Entgeltabrechnung anonyme Bezahlungsverfahren – insbesondere Prepaid-Verfahren – eingesetzt würden, bei denen die Gebühren für die in Anspruch genommenen Leistungen direkt von einer wiederaufladbaren Chipkarte des Benutzers abgebucht werden. Ein derartiges Verfahren würde weitgehend ohne zentrale Speicherung von personenbezogenen Verbindungs- und Abrechnungsdaten auskommen. Es hätte den zusätzlichen Vorteil, daß bei gemeinsamer Nutzung eines Anschlusses durch mehrere Personen diese nicht erfahren, welche Angebote die anderen Nutzer in Anspruch genommen haben.

Derartige anonyme Techniken würden zudem – anders etwa als eine vollständige zentrale Speicherung der Verbindungs- und Abrechnungsdaten – den rechtlichen Vorgaben des Hamburgischen Mediengesetzes für „rundfunkähnliche Kommunikationsdienste" (vgl. 4.2) genügen.

4.2 Neuregelung von rundfunkähnlichen Diensten

Das am 1. Mai 1994 in Kraft getretene neue Hamburgische Mediengesetz (HmbMedienG) enthält spezifische Vorschriften über „rundfunkähnliche Kommunikationsdienste". Darunter sind solche Dienste zu verstehen, mit denen Texte, stehende und bewegte Bilder, Tondarbietungen (Musik und Sprache) entweder aus einem Speicher zum Abruf bereitgestellt oder fortlaufend zum Zugriff verbreitet werden und die nicht Rundfunk sind (vgl. 12.TB, 4.3.2).

Zu den rundfunkähnlichen Kommunikationsdiensten gehören sowohl Mailbox-Systeme, die sich öffentlicher Kommunikationsnetze bedienen und die nicht nur zur internen Kommunikation (etwa einer Firma oder eines Vereins) benutzt werden (vgl. 11.TB, 4.6.1), als auch interaktives Fernsehen (vgl. 4.1 und 12.TB, 4.2).

Angesichts der Möglichkeit des überregionalen Zugriffs auf derartige neue Dienste wäre es erstrebenswert, zumindest auf nationaler Ebene zu einer Harmonisierung der rechtlichen Vorgaben zu kommen. Es wäre zweckmäßig, die entsprechenden Regelungen durch Änderung des Rundfunkstaatsvertrags zu treffen.

Zu dieser ländereinheitlichen Regelung gehören dann auch ergänzende Datenschutzvorschriften, wie jetzt in den §§ 53 ff. HmbMedienG. Wichtig ist dabei insbesondere für interaktive Dienste, daß personenbezogene Daten über die Inanspruchnahme einzelner Programmangebote nur erhoben, verarbeitet und genutzt werden dürfen, soweit und solange dies erforderlich ist für den Abruf der Angebote oder die Abrechnung der Entgelte. An Informationen über Zeitpunkt und Art der Mediennutzung könnten nämlich sowohl die Veranstalter als auch Angehörige, Arbeitgeber, Polizei und Staatsanwaltschaft, persönliche und politische Gegner interessiert sein.

Das datenschutzrechtliche Ziel, ein Mediennutzungsprofil der Teilnehmer zu verhindern, könnte durch derartige ländereinheitliche Regelungen weitgehend erreicht werden. Auf diese Weise könnte außerdem verhindert werden, daß die persönlichen Daten über die Mediennutzung von anderen legal oder mißbräuchlich ausgewertet werden.

Noch wirksamer wäre der Schutz, wenn technisch sichergestellt würde, daß gar nicht erst personenbezogene Daten entstehen. Dies könnte durch anonyme Bezahlungssysteme erreicht werden, indem auch für die Nutzung interaktiver Dienste Prepaid-Karten verwendet werden (vgl. dazu generell 26.2). Wir

werden uns für die Erprobung von Prepaid-Verfahren bei dem in Hamburg geplanten Pilotprojekt „Digitales Fernsehen" einsetzen (vgl. 4.1).

4.3 Ständige Videoübertragung von Straßen und Plätzen

Ein Hamburger Fernsehsender beabsichtigt, an zentralen Punkten der Stadt Videokameras zu installieren und die von diesen aufgenommenen Bilder als Verkehrsübersichten zu verbreiten. Während der Verkehrsnachrichten werden jeweils einzelne Kameras auf Sendung geschaltet und das dortige Verkehrsgeschehen durch einen Moderator erläutert.

Ferner ist vorgesehen, von drei erhöhten Standorten während der Zeiten ohne redaktionelles Programm Live-Aufnahmen eines Hamburg-Panoramas zu senden. Die Aufnahmen werden per Standleitung in guter Qualität an den Sender übertragen.

4.3.1 Datenschutzrechtliche Rahmenbedingungen

Die Aufnahme, Übertragung und Aufzeichnung von Videobildern ist datenschutzrechtlich relevant, wenn auf den Bildern einzelne Personen zu erkennen sind oder die Bilder Rückschlüsse über sachliche oder persönliche Verhältnisse natürlicher Personen erlauben. Dies wäre z.B. dann gegeben, wenn Autokennzeichen abgelesen werden können.

Jede personenbezogene Video-Aufnahme ist als Datenerhebung im Sinne von § 3 Abs. 4 BDSG anzusehen, auch wenn es sich um durchlaufende Bilder handelt.

Soweit Videoaufnahmen auf einem Datenträger (sei es auf einem Videoband oder auf einer magnetischen oder optischen Platte) aufgezeichnet werden, handelt es sich um eine Datenspeicherung im Sinne von § 3 Abs. 5 Nr. 1 BDSG. Dies gilt auch dann, wenn die Aufnahmen nach begrenzter Zeit wieder gelöscht werden. Hingegen ist das bloße „Durchlaufen" einer Videoaufnahme mit schneller Bildfolge keine Speicherung.

Werden personenbezogene Videoaufnahmen Dritten zugänglich gemacht, also z.B. gesendet, handelt es sich um eine Übermittlung.

§ 55 Hamburgisches Mediengesetz (HmbMedienG) enthält Ausnahmeregelungen für die Verarbeitung und Nutzung personenbezogener Daten im journalistisch-redaktionellen Bereich. Es gelten von den Vorschriften des BDSG nur die Regelungen über das Datengeheimnis und die technischen und organisatorischen Maßnahmen (§§ 5 und 9).

Auch wenn die Videoaufnahmen dazu dienen, die nicht anderweitig genutzten Sendezeiten zu füllen – also im weitesten Sinne zum Programm beitragen –, hängt es von der konkreten Gestaltung der Sendungen ab, inwieweit überhaupt eine journalistisch-redaktionelle Tätigkeit ausgeübt wird, die unter den

Schutz von Art. 5 GG fällt. Wie in § 41 Abs. 1 Satz 2 BDSG bezüglich der Herausgabe von Adressen-, Telefon-, Branchen- oder vergleichbaren Verzeichnissen deklaratorisch festgestellt wird, gilt das Medienprivileg nur, wenn mit der Herausgabe zugleich eine journalistisch-redaktionelle Tätigkeit verbunden ist.

Wenn man zugunsten der Rundfunkfreiheit minimale Anforderungen an die Programmgestaltung ausreichen läßt, sind die von „unbemannten" Kameras aufgenommenen Verkehrsübersichten allenfalls am Rande des Medienprivilegs einzuordnen.

4.3.2 Mögliche Beeinträchtigungen des Persönlichkeitsrechts

Das Persönlichkeitsrecht ist gemäß § 8 HmbMedienG bei Sendungen zu wahren, auch wenn aufgrund des Medienprivilegs nur die BDSG-Bestimmungen über die Datengeheimhaltung und Datensicherung gelten.

Die Intensität des Eingriffs würde erhöht, wenn die Aufnahmen von fest installierten Kameras erfolgen, so daß an immer denselben Orten eine mehr oder minder regelmäßige „Überwachung" stattfindet. Da anzunehmen ist, daß sich bestimmte Personen an den jeweiligen Orten häufiger aufhalten (z.B. weil es sich um ihren Arbeitsweg handelt), würden diese Personen wiederholt erfaßt und ihr Verhalten würde kontrollierbar, z.B. durch nachträgliche polizeiliche Auswertung der Aufnahmen in Strafverfahren.

Gegebenenfalls kann auch das „Recht am eigenen Bild" verletzt werden. Die geltenden Bestimmungen, welche die Verwendung von Bildern regeln, sind alt und unvollständig. Die einzige spezielle gesetzliche Grundlage ist das „Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photografie" vom 9. Januar 1907 (Kunsturhebergesetz – KunstUrhG).

Nach § 22 KunstUrhG darf ein Bildnis einer Person ohne deren Einwilligung weder verbreitet noch öffentlich zur Schau gestellt werden. Die Herstellung von Bildnissen – also die Videoaufnahme als solche – wird vom Wortlaut dieser Bestimmung jedoch nicht erfaßt. Mit der herrschenden Meinung und Rechtsprechung ergibt sich das grundsätzliche Verbot ungenehmigter Bildaufnahmen deshalb auch nicht aus den Regelungen des KunstUrhG, sondern direkt aus dem allgemeinen Persönlichkeitsrecht. Bei den vorgesehenen Sendungen handelt es sich um die öffentliche Verbreitung der Bilder, so daß auch § 22 KunstUrhG zu beachten ist.

Das Recht am eigenen Bild wurde bisher in der Literatur und in der Rechtsprechung allerdings fast ausschließlich unter dem Gesichtspunkt von Schadensersatz und Schmerzensgeld nach den §§ 823, 847 BGB diskutiert.

4.3.3 Gebot zum Ausgleich zwischen Persönlichkeitsrecht und Berichterstattungsfreiheit

Bei den Sendungen sind die Vorgaben des HmbMedienG zu beachten. Die in § 8 HmbMedienG formulierten Programmgrundsätze verpflichten die Anbieter u.a. zur Einhaltung der allgemeinen Gesetze, der Bestimmungen zum Schutze der Jugend und des Rechts der persönlichen Ehre.

Das Persönlichkeitsrecht umfaßt die Möglichkeit, sich ohne Kontrolle durch Dritte im öffentlichen Raum zu bewegen und mit anderen Menschen zu kommunizieren. Eingriffe sind im Interesse anderer Rechtgüter nur zulässig, soweit sie sich auf das unabdingbar Notwendige beschränken.

Es würde zu einem unzulässigen Überwachungsdruck führen, wenn man jederzeit damit rechnen muß, aufgenommen zu werden. Deshalb hat die Rechtsprechung selbst bei der Kameraüberwachung gegen Diebstähle verlangt, daß die in dem überwachten Gebäude ständig Beschäftigten Gelegenheit haben müssen, sich in einen unbeobachteten Bereich zurückzuziehen. Im öffentlichen Raum kann aber von dem Betroffenen nicht verlangt werden, die von den installierten Kameras erfaßten Bereiche zu umgehen oder zu umfahren.

Damit ergibt sich die Verpflichtung für den Programmveranstalter, zwischen dem aus Art. 5 GG abzuleitenden Anspruch auf freie Berichterstattung und dem allgemeinen Persönlichkeitsrecht der Betroffenen nach Art. 2 GG abzuwägen. Dabei ist das Interesse an einer ungehinderten Berichterstattung jeweils konkret mit der verbundenen Eingriffstiefe in die Persönlichkeitsrechte abzuwägen.

Im Hinblick darauf, daß die Sendungen mit Verkehrsübersichten und Panorama-Blicke nur einen geringen journalistisch-redaktionellen Anteil haben, haben wir angeregt, die Aufnahmen so aufzunehmen und zu senden, daß kein Personenbezug besteht.

Der Fernsehsender ist auf diesen Vorschlag eingegangen. Anhand eines Demo-Videos konnten wir uns davon überzeugen, daß keine Fahrzeugkennzeichen und keine Personen erkennbar waren. Bei den Aufnahmen aus der Totalen waren auch Autotypen praktisch nicht auszumachen.

Aufgrund der Aufnahmeperspektive und der Kamerastandorte sind Personen oder Fahrzeuge auch bei dem geplanten Hamburg-Panorama nicht identifizierbar. Soweit also durch die Aufnahmetechnik gewährleistet ist, daß keine personenbezogenen Informationen aufgenommen und übertragen werden, sind Persönlichkeitsrechte nicht beeinträchtigt.

Die Vertreter des Fernsehsenders haben ausgeführt, daß sie keinerlei Interesse an individueller Videoüberwachung hätten und daß ein derartiger Eindruck stark imageschädigend wäre. Aus diesem Grund werde man darauf achten, daß weder Personen noch Fahrzeuge identifizierbar aufgenommen oder

übertragen werden. Ferner werde sich die Videoaufzeichnung auf die durch § 13 HmbMedienG vorgeschriebene sechswöchige Speicherung des Sendesignals beschränken; die nicht gesendeten Aufnahmen würden nicht gespeichert.

Unter diesen Voraussetzungen bestehen gegen die geplanten neuen Sendeformen keine datenschutzrechtlichen Bedenken.

4.4 Verfahren zur Befreiung von der Rundfunkgebührenpflicht

Anläßlich einer Eingabe hatten wir uns mit dem Verfahren zur Befreiung von der Rundfunkgebührenpflicht zu beschäftigen. Die Praxis richtet sich in Hamburg nach der Verordnung über die Befreiung von der Rundfunkgebührenpflicht vom 5. Februar 1980 sowie nach der Fachlichen Weisung SR 24/87 der Behörde für Arbeit, Gesundheit und Soziales (BAGS).

Bei Gebührenbefreiung aus sozialen Gründen ist danach in der Regel ein Antrag an das zuständige Sozialamt zu richten. Dieses ist vom Norddeutschen Rundfunk (NDR) generell ermächtigt, bei Vorliegen der Voraussetzungen für die Gebührenbefreiung dem Antragsteller den Gebührenbefreiungsbescheid auszuhändigen und lediglich Ausfertigungen des Bescheides an den NDR und an die Gebühreneinzugszentrale (GEZ) zu senden.

Ein abweichendes Verfahren gilt allerdings bei Anträgen von Personen, die nicht Haushaltsvorstand oder Ehepartner des Haushaltsvorstandes sind. In diesen Fällen ist der Antrag mit einer Stellungnahme des Sozialamts dem NDR zur Entscheidung zuzuleiten.

Gegen diese Verfahrensweisen haben wir Bedenken. Der Rundfunkgebührenstaatsvertrag vom 5. Dezember 1974, auf dessen Artikel 7 sich die angewendete Verordnung stützt, ist bereits außer Kraft getreten; es gilt der Rundfunkgebührenstaatsvertrag vom 31. August 1991. Die Verordnung vom 5. Februar 1980 ist zwar weiterhin gültig; sie trägt der heutigen Vorstellung des Gesetzgebers über den Regelungsinhalt einer solchen Verordnung aber nicht mehr ausreichend Rechnung. Die entsprechende Verordnungsermächtigung in § 6 des derzeit gültigen Rundfunkgebührenstaatsvertrages sieht nämlich vor, daß in der Verordnung auch geregelt wird, welche personenbezogenen Daten die für die Entscheidung zuständige Stelle (Sozialamt) der Landesrundfunkanstalt (dem NDR) zu übermitteln hat. Zudem ist die fachliche Weisung SR 24/87 gemäß § 5 Abs.2 Satz 4 Bezirksverwaltungsgesetz bereits am 31. Dezember 1992 außer Kraft getreten.

Zweifelhaft ist, ob die derzeitigen Verfahrensweisen überhaupt sachgerecht sind. Vorstellbar erscheint das eigentlich nur in den Fällen, in denen das Sozialamt aufgrund ohnehin dort vorliegender Informationen (insbesondere über die wirtschaftlichen Verhältnisse) zu einer abschließenden und rechtsverbindlichen Entscheidung über den Antrag in der Lage ist. Sobald dem Sozial-

amt zur Entscheidung über den Antrag zusätzliche Informationen gegeben werden müssen, wäre es naheliegender, den Antrag direkt beim NDR stellen zu lassen. Nicht überzeugen kann auch das angesprochene Verfahren, bei dem der Antrag beim Sozialamt zu stellen ist, obwohl dieses über den Antrag gar nicht entscheiden darf.

Die BAGS hat ebenfalls Bedenken dagegen, daß die Sozialämter grundsätzlich alle Anträge auf Befreiung von der Rundfunkgebührenpflicht entgegennehmen.

Die Senatskanzlei, die für die Änderung der Verordnung über die Befreiung von der Rundfunkgebührenpflicht zuständig ist, hat uns darauf hingewiesen, daß aufgrund des neuen Rundfunkgebührenstaatsvertrags vom 31. August 1991 in den Ländern möglichst übereinstimmende Gebührenbefreiungsverordnungen geschaffen werden müssen. Sie will in der dafür zu führenden Diskussion auch den Vorschlag behandeln, die Sozialämter von der Bearbeitung der Gebührenbefreiungsanträge zu befreien.

Wegen der notwendigen weitgehenden Übereinstimmung der Verordnungen haben wir auch die Datenschutzbeauftragten der anderen Länder informiert, da die Realisierung unserer Änderungsvorstellungen erleichtert würde, wenn sie von möglichst vielen Ländern unterstützt werden.

5. Umwelt

5.1 Umweltinformationsgesetz des Bundes

Mit dem im Juli 1994 in Kraft getretenen Umweltinformationsgesetz des Bundes (UIG) ist die EG-Umweltinformationsrichtlinie (UIR) nunmehr verspätet auch in Deutschland – zumindest teilweise – umgesetzt worden. Leider wurde den Bedenken gegen den Gesetzentwurf (vgl. 12.TB. 5.2.1) im wesentlichen nicht Rechnung getragen.

Problematisch sind insbesondere die Regelungen bezüglich der Gebührenerstattung. Art. 5 UIR ermächtigt die Mitgliedsstaaten nur zur Gebührenerhebung für die Übermittlung von Informationen. Die Gebühren dürfen eine angemessene Höhe nicht überschreiten. Mit dieser Bestimmung wird dem Äquivalenzprinzip Rechnung getragen, wonach die Gebühr den Wert des tatsächlichen Vorteils, den der Gebührenpflichtige erlangt hat, nicht überschreiten darf. Dagegen erlaubt es § 10 UIG, kostendeckende Gebühren für Amtshandlungen aufgrund des Gesetzes zu erheben, also auch für die Ablehnung des Informationszugangs.

Es ist zu hoffen, daß der Senat in der anstehenden Überarbeitung der Gebührenordnung die Gebühren für den Zugang zu Umweltinformationen senkt.

5.2 Initiativen zur Schaffung eines Hamburgischen Umweltinformationsgesetzes

Die GAL-Fraktion hat im Juni 1994 vor dem Inkrafttreten des Umweltinformationsgesetzes des Bundes (vgl. 5.1) einen Gesetzentwurf für ein Hamburgisches Umweltinformationsgesetz vorgelegt.

Die in diesem Gesetzentwurf enthaltenen Informationszugangsregelungen sind weiter gefaßt als diejenigen im Umweltinformationsgesetz des Bundes (UIG). Insbesondere sollen die Personen, die den Zugang zu einer Umweltinformation begehren, grundsätzlich selbst entscheiden können, ob der Informationszugang durch Akteneinsicht oder durch Auskunft der Behörde erfolgt. Anders als im UIG des Bundes soll sich die Kostenerstattung auf Selbstkosten für Kopien und vergleichbare Verwaltungskosten beschränken; darüberhinausgehende Gebühren – insbesondere auch für die Ablehnung eines Informationszugangs – sollen nicht erhoben werden.

In den Beratungen der Bürgerschaft haben sich die Senatsvertreter dahingehend geäußert, daß sie nach dem Inkrafttreten des UIG des Bundes keinen Raum für ein Landesgesetz über den Zugang zu Umweltinformationen sehen. Im übrigen seien die Bestimmungen des Bundesgesetzes auch inhaltlich zufriedenstellend.

Bei Redaktionsschluß für den TB waren die bürgerschaftlichen Beratungen über den Gesetzentwurf noch nicht abgeschlossen.

5.3 Datenabgleich zwischen Wirtschafts- und Umweltbehörde

In seiner Prüfungsmitteilung „Staatliche Aufgaben in der Landwirtschaft" vom 4. Februar 1994 hat der Rechnungshof die Umweltbehörde und die Wirtschaftsbehörde aufgefordert, zur Vermeidung unrechtmäßiger Förderungen von Landwirten auch die der jeweils anderen Behörde vorliegenden Daten heranzuziehen. Er hat bemängelt, daß eine Abstimmung zwischen den Behörden nicht in ausreichendem Maße stattfinde.

Ein solcher präventiver Datenabgleich ist nur möglich, wenn dies gesetzlich ausdrücklich zugelassen ist. Daran fehlt es jedoch bei den in Frage kommenden Förderprogrammen. Wir haben Einigkeit erzielt, daß Übermittlungen im Rahmen dieser Programme nur bei konkreten Anhaltspunkten für unrichtige Angaben erfolgen dürfen, oder wenn die Betroffenen vorab in eine Übermittlung eingewilligt haben.

6. Sozialwesen

6.1 Projekt Sozialhilfe-Automation (PROSA)

Im Zusammenhang mit PROSA haben uns vor allem die Vorhaben mehrerer Stellen beschäftigt, im automatisierten Online-Abrufverfahren auf den PROSA-

Datenbestand zugreifen zu können. Das Verlangen nach einem solchen automatisierten Direktabruf besteht nach unserer Kenntnis

— bei dem Rechnungshof der Freien und Hansestadt,

— bei der Vorprüfungsstelle (zugleich Fachlicher Prüfdienst) der Behörde für Arbeit, Gesundheit und Soziales (BAGS)

und

— bei der Prüfungsabteilung der Finanzbehörde für das Kassen- und Rechnungswesen.

Nach § 79 Sozialgesetzbuch/Zehntes Buch (SGB-X) ist ein automatisiertes Abrufverfahren zulässig, wenn es angemessen ist. Für eine solche Angemessenheit kommt es zunächst darauf an, ob eine Vielzahl von Übermittlungen erfolgt oder eine besondere Eilbedürftigkeit vorliegt und die schutzwürdigen Interessen der Betroffenen gewahrt bleiben. Diese Voraussetzungen müssen von den Stellen, die den Abruf begehren, nachprüfbar dargelegt werden.

Im Hinblick auf die zu wahrenden schutzwürdigen Interessen der Betroffenen ist zu beachten, daß zwar durch die Automatisierung des Sozialhilfeverfahrens bestehende Prüfungsrechte z.B. des Rechnungshofes nicht beeinträchtigt werden dürfen. Gemäß dem Ansatz des Bundesverfassungsgerichts, daß gerade die automatisierte Datenverarbeitung das informationelle Selbstbestimmungsrecht gefährdet, sollte die Umstellung eines Verfahrens auf eine automatisierte Abrufmöglichkeit aber auch nicht zu einer Erweiterung der Datenzugriffe führen.

Sofern die Grundvoraussetzungen für ein Abrufverfahren gegeben sind, müssen die Bedingungen des Abrufverfahrens in einer gesetzlich vorgeschriebenen Vereinbarung zwischen der abrufenden Stelle einerseits und der speichernden Stelle andererseits festgelegt werden. Die Vereinbarung über ein Abrufverfahren bedarf der Genehmigung durch die zuständige Fachaufsichtsbehörde.

In der Vereinbarung sind Anlaß und Umfang des Abrufverfahrens (einschließlich der Datenkränze) sowie die erforderlichen technischen und organisatorischen Maßnahmen festzulegen. Der Abruf muß zumindest stichprobenweise durch Protokollierung überprüft werden. Dabei hat die Stichprobe mindestens 10% der Abrufe zu umfassen.

In Diskussionen mit den genannten Stellen haben wir Einvernehmen darüber erzielt, daß für das Abrufverfahren spezielle Kennungen geschaffen werden müssen und daß der Zugriff nur lesend, nicht aber schreibend bzw. ändernd erfolgen darf. Einvernehmen wurde auch darüber erzielt, daß es im Regelfall für die abrufenden Stellen ohne Bedeutung ist, welchen konkreten Hilfeempfänger die abgerufenen Daten betreffen. Daher wird unterschieden zwischen Datei- und Einzelfallabrufen.

Bei Dateiabrufen bietet das System zu bestimmten Suchkriterien die jeweiligen Fälle an, ohne die unmittelbaren Identifizierungsdaten, insbesondere Name und Anschrift kenntlich zu machen. Damit wird den schutzwürdigen Interessen der Betroffenen sogar besser entsprochen als bei einer konventionellen Aktenprüfung. Nur bei Bedarf kann über eine kennzeichnende Nummer ein umfassender Einzelfallabruf erfolgen.

Als weitere Maßnahme zur Wahrung der schutzwürdigen Interessen der Hilfeempfänger halten wir es für grundsätzlich geboten, die Abrufmöglichkeit auf die Dauer einer Prüfung zu befristen. Der tatsächliche Zugriff sollte dann durch die speichernde Stelle auf schriftlich begründete Anforderung aktiviert werden.

Der erste uns vorgelegte Vereinbarungsentwurf für das Abrufverfahren, das für die Vorprüfungsstelle/Fachlicher Prüfdienst der BAGS eingerichtet werden soll, hat den datenschutzrechtlichen Anforderungen weitgehend Rechnung getragen. Abweichend von den oben genannten Anforderungen sieht er allerdings eine unbefristete Abrufmöglichkeit vor. Dies wurde mit der Fachaufsicht nach § 5 Abs.2 Satz 2 Bezirksverwaltungsgesetz begründet, die die Vorprüfungsstelle zugleich wahrnimmt. Diese Begründung haben wir akzeptiert. Sie wird sich auf die weiteren vorgesehenen Abrufverfahren aber nicht übertragen lassen. Dies haben wir dem Rechnungshof auch mitgeteilt, nachdem uns ein Vereinbarungsentwurf für das Abrufverfahren des Rechnungshofes im Vorwege der formellen Beteiligung zur Kenntnis gebracht wurde.

6.2 Datenverarbeitung in Wohngeldstellen

Im Berichtszeitraum haben wir zwei Wohngeldstellen überprüft, eine aus dem Bezirksamtsbereich Bergedorf, die andere aus dem Bezirksamtsbereich Altona.

Das Wohngeldverfahren bot dabei keinen Anlaß zu grundsätzlicher Kritik. Hauptproblem sind Anfragen beim Vermieter des Wohngeldempfängers, mit denen die Wohngeldbedürftigkeit des Mieters offenbart wird. Diese Anfragen sind aber in den vielen Fällen erforderlich, in denen nur der Vermieter das Datum der Bezugsfertigkeit des Wohnraumes kennt, das für die Wohngeldgewährung wesentlich ist. In gleicher Weise problematisch sind Anfragen beim Arbeitgeber. Diese sind dann erforderlich, wenn der Wohngeldempfänger sein Einkommen nicht im notwendigen Umfang spezifizieren kann.

In einer Wohngeldstelle fielen in den Akten Kontoauszüge auf, die zum Nachweis finanzieller Angaben zur Akte genommen worden waren. Diese enthielten teilweise auch irrelevante Angaben, z.B. über ein Zeitungsabonnement und eine Parteimitgliedschaft. Das Bezirksamt will unseren Hinweis beachten, daß solche Unterlagen nicht zur Akte zu nehmen sind.

Verbesserungsbedürftig sind die räumlichen Verhältnisse, die wir in den Wohngeldstellen antrafen. Sie bieten keine ausreichende Sicherung der Unterlagen,

sondern erlauben mit geringem Aufwand einen unbefugten Zugriff. Zudem werden in beiden geprüften Wohngeldstellen Doppel- und Mehrfachzimmer genutzt, die eine Vertraulichkeit des Gesprächs mit dem Wohngeldbezieher schwerlich ermöglichen.

Uns ist bewußt, daß sich diese räumlichen Verhältnisse nicht kurzfristig ändern lassen, erst recht nicht in Zeiten finanzieller Mittelknappheit. Gleichwohl halten wir es für unerläßlich, auf die notwendigen Verbesserungen kontinuierlich hinzuarbeiten.

Besonders bemerkenswert sind die Verhältnisse in der geprüften Altonaer Wohngeldstelle. Hier hatten wir bereits 1987 Kritik an den äußeren Sicherungsmaßnahmen geübt. Daraufhin war uns mitgeteilt worden, es würden Mittel für die Beschaffung von Stahlmöbeln zur Sicherung der Datenbestände eingeworben werden. Das ist leider bis heute folgenlos geblieben, da eingeworbene Mittel nicht bewilligt wurden. So werden weiterhin Akten offen in nicht-verschließbaren Schränken verwahrt, teilweise sogar in einem ebenerdigen Toilettenvorraum, der als Fahrradabstellraum dient und von Mitarbeiterinnen verschiedener Dienststellen genutzt wird. Wir haben das Bezirksamt nachdrücklich aufgefordert, unverzüglich für Abhilfe zu sorgen.

In der Altonaer Wohngeldstelle waren außerdem zur Jahresmitte die Akten noch vorhanden, die bereits am Jahresanfang hätten ausgesondert und vernichtet werden müssen. Damit wurden die Akten über die fünfjährige Aufbewahrungsfrist hinaus und entgegen § 84 Abs.2 Sozialgesetzbuch/Zehntes Buch aufbewahrt. Verwunderlich war das in Anbetracht der Ablagesystematik allerdings nicht. Die Archivierung erfolgt dort nämlich ausschließlich nach buchstabenmäßiger Ordnung. Für eine Vernichtung müssen daher sämtliche vorhandenen Akten auf ihr Vernichtungsjahr durchgesehen werden. Da das sehr zeitaufwendig ist, bleiben erhebliche Verzögerungen nicht aus.

Die Ablagesystematik im Archiv der Bergedorfer Wohngeldstelle ist dagegen vorbildlich; sie erfolgt nach Vernichtungsjahrgängen. Dadurch können die Akten jahrgangsweise ohne großen Aufwand ausgesondert und fristgerecht vernichtet werden.

6.3 Prüfung zweier Betriebskrankenkassen

Hinsichtlich der im 12. TB (6.4) dargestellten datenschutzrechtlichen Probleme bei zwei geprüften Betriebskrankenkassen (BKKen) sind unsere Zweifel an der Existenzberechtigung einer der beiden Kassen inzwischen durch eine Stellungnahme der Behörde für Arbeit, Gesundheit und Soziales (BAGS) ausgeräumt worden. Auch unsere Bedenken gegen Prüfungen durch den Landesverband der Betriebskrankenkassen bestehen nicht mehr. Der Landesverband und die BAGS haben klargestellt, daß diese Prüfungen nicht aufgrund eines eigenen Rechts des Landesverbandes, sondern im Auftrag des Krankenkassenvorstandes erfolgen. Sie lassen sich daher auf § 31 der Verordnung über das Haushaltswesen in der Sozialversicherung stützen.

Hinsichtlich der Lösung der weiteren von uns aufgezeigten Probleme tuen sich die BKKen schwer. Erst nach acht Monaten und nur auf ausdrückliche Erinnerung erhielten wir eine – völlig unbefriedigende – Stellungnahme zu unseren Änderungsvorschlägen.

— Personalkrankenkasse

Die Problematik wollten die BKKen zunächst dadurch lösen, daß sich die Mitarbeiter mit der Bearbeitung ihrer Krankheitsfälle durch ihren Vorgesetzten (den Geschäftsführer) einverstanden erklären. Wir haben darauf hingewiesen, daß dieser Weg unzulässig ist. Der Gesetzgeber hatte bereits in § 284 Abs.4 Sozialgesetzbuch/Fünftes Buch (SGB-V) zwingend vorgesehen, daß die Daten der Beschäftigten und ihrer Angehörigen den Personen, die kasseninterne Personalentscheidungen treffen oder an ihnen mitwirken können, nicht zugänglich gemacht werden dürfen.

Eine Abänderung dieser Regelung durch Einwilligungen der Betroffenen war nicht vorgesehen. Sie würde auch keinen Sinn ergeben, da die Freiwilligkeit einer Einwilligung aufgrund der arbeitsrechtlichen Abhängigkeit der Mitarbeiter nicht ernsthaft angenommen werden kann.

Durch das Zweite Gesetz zur Änderung des Sozialgesetzbuches (vgl. 12. TB, 6.2) sollte diese zwingende Regelung zunächst aufgeweicht werden: Bei gleichzeitiger Übernahme des § 284 Abs.4 SGB-V in § 35 Abs.1 SGB-I sollte die Formulierung „dürfen nicht" durch „sollen nicht" ersetzt werden. Ausdrücklich erklärter Zweck dieser Aufweichung war es, auf den Verwaltungsablauf kleinerer Leistungsträger Rücksicht zu nehmen und diesen Ausnahmen von der bisherigen Regelung zu erlauben. Im weiteren Gesetzgebungsverfahren ist dann aber auf Betreiben des Bundesrates die Formulierung des § 284 Abs.4 SGB-V doch unverändert in § 35 Abs.1 SGB-I übernommen worden, so daß sich eine Aufweichung der bisherigen Regelung nicht durchsetzen konnte.

Aufgrund dieser zwingenden Gesetzeslage sehen wir als allein möglichen Weg zur Lösung des Problems der Personalkrankenkasse, einen sozialrechtlichen Auftrag nach § 88 SGB-X an einen anderen Leistungsträger (z.B. eine andere BKK) oder an einen Verband der BKKen zu erteilen. Die BKKen streben jetzt eine Aufgabenwahrnehmung durch den Landesverband an.

— Dienstanweisungen

Auf unsere Änderungsvorschläge zur Dienstanweisung für die automatisierte Datenverarbeitung hatten uns die BKKen eine Überarbeitung zugesagt. Als wir um Übersendung eines geänderten Entwurfs baten, erhielten wir je-

doch eine Fassung, die aus der Zeit vor unserer Prüfung datierte und in der dementsprechend kein einziger unserer Vorschläge umgesetzt war.

— Löschungen

Mit der Vernichtung von Unterlagen, deren Aufbewahrungsfrist abgelaufen ist, haben die BKKen nach ihren Angaben inzwischen begonnen.

— Vordrucke

Zu unseren im einzelnen dargestellten Bedenken gegen zahlreiche verwendete Vordrucke teilten uns die BKKen zunächst nur mit, diese Vordrucke seien mit dem Bundesverband der Ortskrankenkassen abgestimmt. Auf unseren Hinweis, daß dies ggf. unerheblich sei, haben uns die BKKen dann mitgeteilt, sie hätten von den Fachverlagen geänderte Vordrucke angefordert.

Es bleibt also abzuwarten, inwieweit unsere Vorschläge tatsächlich umgesetzt werden.

6.4 Mangelhafte Zugriffssperren für Beitrags- und Leistungsdaten bei Krankenkassen

Im Berichtszeitraum hatten wir uns mit der Frage zu befassen, inwieweit eine große Hamburger Krankenkasse für ihre automatisierte Datenverarbeitung ausreichende technische Sicherungsmaßnahmen getroffen hat. Dabei stellten wir fest, daß der Zugriff auf Datensätze einer viel zu großen Zahl von Personen möglich ist. Bei der Diskussion dieses Problems wurde dann deutlich, daß es sich um ein bundesweit bei sehr vielen Krankenkassen auftretendes Problem handelt.

Die Krankenkasse speichert die Datensätze ihrer Versicherten zentral auf einem Großrechner. Es handelt sich um eine umfassende Verarbeitung von Versichertendaten, die nicht nur Stammdaten wie Name, Anschrift und Versicherungsnummer, sondern eine Fülle weiterer sensibelster Daten umfaßt, bis hin zu Arbeitsunfähigkeitszeiten, Krankenhausaufenthalten einschließlich Schlüsselnummer der Fachabteilung, einweisendem Arzt und Diagnoseangaben (auch im Klartext). An das Verfahren angeschlossen sind alle im Stadtgebiet vorhandenen Geschäftsstellen der Krankenkasse. Es ist gegenwärtig technisch nicht möglich, eine Beschränkung des Zugriffs auf einzelne Geschäftsstellen vorzunehmen. Die lesenden Zugriffe der Geschäftsstellen werden auch nicht protokolliert. Wenn eine Geschäftsstelle auf die Daten eines Versicherten zugreift, ohne dafür einen zulässigen Grund zu haben, ist dies daher im nachhinein nicht feststellbar.

Die Krankenkasse hatte diese Ausgestaltung des Verfahrens zunächst damit begründet, daß es notwendig sei, jeden Versicherten von jeder Geschäftsstelle aus umfassend betreuen zu können. Es entspreche ihren Erfahrungen, daß

Versicherte von dieser Möglichkeit Gebrauch machen.

Diese Begründung halten wir für nicht stichhaltig. Die Krankenkasse hat zwar organisatorisch auch dafür Sorge zu tragen, daß die Versicherten ihre Leistungen einfach und schnell erhalten (§ 17 Abs.1 Nr.1 und 3 Sozialgesetzbuch/Erstes Buch (SGB-I)). Dieser Verpflichtung kann sie aber auch nachkommen, wenn sie den Versicherten eine Wahlmöglichkeit einräumt und sie selbst über die Zugriffsmöglichkeiten auf ihre Daten bestimmen läßt. Im Grundsatz genügt es nach unserer Auffassung, wenn jeder Versicherte von einer Geschäftsstelle umfassend betreut wird. Ausreichend wäre es demnach, wenn die Zugriffsmöglichkeit grundsätzlich nur für eine Geschäftsstelle besteht und für weitere Geschäftsstellen nur dann, wenn der Versicherte sich damit ausdrücklich schriftlich einverstanden erklärt hat. Für diese Einschätzung sind folgende Überlegungen maßgebend:

Krankenkassenbesuche erfolgen in aller Regel planmäßig und nicht spontan, so daß in einer Vielzahl von Fällen die Betreuung des Versicherten durch eine einzige Geschäftsstelle ausreichend ist. Der Versicherte wird diese Geschäftsstelle typischerweise so wählen, daß er sie unter Berücksichtigung seiner Tagesabläufe gut erreichen kann. Zudem ist es den Versicherten innerhalb des flächenmäßig kleinen Stadtstaates Hamburg von praktisch jedem Ort aus mit vertretbarem Zeitaufwand möglich, die ihn betreuende Geschäftsstelle aufzusuchen.

Wenn ein Versicherter – aus welchen Gründen auch immer – es bevorzugt, von mehreren oder von allen Geschäftsstellen der Krankenkasse umfassend betreut zu werden, kann ihm diese Möglichkeit selbstverständlich eröffnet werden. Dieser Wunsch muß aber durch eine entsprechende schriftliche Einwilligungserklärung dokumentiert sein.

Das gegenwärtige Verfahren ist sachlich nicht zwingend geboten. Es entspricht nicht den Anforderungen, die der Gesetzgeber in der Anlage zu § 78a SGB-X beschrieben hat. Die dort geforderten technischen Maßnahmen bei automatisierter Datenverarbeitung müssen u.a. geeignet sein,

— zu verhindern, daß Datenträger unbefugt gelesen werden können (Datenträgerkontrolle),

— die unbefugte Kenntnisnahme gespeicherter personenbezogener Daten bzw. Sozialdaten zu verhindern (Speicherkontrolle),

— zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer – rechtlichen – Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),

— die innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

Diese Anforderungen wurden festgelegt in Kenntnis und unter Berücksichtigung des Umstands, daß die Mitarbeiter der Krankenkassen zur Verschwiegenheit verpflichtet sind, und sind daher uneingeschränkt einzuhalten.

Vom Bundesbeauftragten für den Datenschutz haben wir im übrigen erfahren, daß die seiner Kontrolle unterliegenden überregionalen Krankenkassen den unzuständigen Geschäftsstellen nur den Zugriff auf einen Stammdatensatz erlauben, der aus dem Namen, dem Geburtsdatum, der Versicherungsnummer und der für die Betreuung zuständigen Geschäftsstelle besteht.

Wir haben die Krankenkasse daher aufgefordert, ihre eingesetzte Technik so zu ändern, daß die rechtlich gebotene Beschränkung der Zugriffsmöglichkeit realisiert werden kann. Eine besonders komfortable Möglichkeit wäre es dabei, wenn die technische Gewährung des Zugriffs in den Geschäftsstellen davon abhängig ist, daß ein Versicherter seine Krankenversichertenkarte vorlegt, die dann von einem Chipkartenlesegerät gelesen wird und dabei den Zugriff auf den Datensatz des Versicherten eröffnet.

Die Krankenkasse steht bei der Umsetzung unserer Forderung allerdings vor dem Problem, daß ihr EDV-System von ihrem Bundesverband entwickelt wurde. Es wäre für sie leichter, wenn eine bundeseinheitliche Lösung realisiert würde. Sie ist daher an ihren Bundesverband herangetreten, um entsprechende Änderungen zu veranlassen. Parallel dazu hat sich auf unsere Bitte der Bundesbeauftragte für den Datenschutz an diesen Bundesverband gewandt, um eine datenschutzgerechte Weiterentwicklung des EDV-Verfahrens zu erreichen. Der Bundesverband zeigte sich in ersten Stellungnahmen allerdings ablehnend.

Wir werden uns im Zusammenwirken mit den Datenschutzbeauftragten des Bundes und der anderen Länder weiterhin um eine bundeseinheitliche Lösung bemühen. Sollte diese nicht erreicht werden können, müßte die Krankenkasse im Rahmen ihrer datenschutzrechtlichen Eigenverantwortlichkeit tätig werden.

6.5 Prüfung der Feuerwehr-Unfallkasse

Die Feuerwehr-Unfallkasse ist als eine rechtsfähige Körperschaft des öffentlichen Rechts Träger der gesetzlichen Unfallversicherung für die Angehörigen der Freiwilligen Feuerwehren. Sie hat eine schriftliche Vereinbarung mit der Hamburger Feuerkasse getroffen, nach der ihr die Hamburger Feuerkasse verschiedene Leistungen erbringt. Diese Vereinbarung erfolgte wegen der Umwandlung der Feuerkasse in eine privatrechtlich organisierte Aktiengesellschaft. Die darin aufgeführten Leistungen sollen mindestens bis zum Ende des Jahres 2010 erfolgen.

Bei einer Überprüfung der Feuerwehr-Unfallkasse war unser zentrales Anliegen die Frage, inwieweit der Feuerkassen AG als nicht-öffentlicher Stelle Sozialdaten zugänglich sind. Dies ist nach den Regelungen des Sozialgesetzbuches nur sehr eingeschränkt zulässig.

Festgestellt haben wir bei der Prüfung, daß die Feuerwehr-Unfallkasse sämtliche Versichertenunterlagen seit 1930 archiviert. Es fehlt eine Festlegung der Aufbewahrungsfrist für diese Unterlagen. Bei der zu treffenden Regelung wird sich die Feuerwehr-Unfallkasse nach dem Sozialgesetzbuch daran zu orientieren haben, wie lange sie die Unterlagen zur Aufgabenerfüllung benötigt. Der Wunsch nach statistischer Auswertung der Unterlagen darf für die Aufbewahrungsfrist keine Rolle spielen.

Eine Offenbarung von Sozialdaten an die Feuerkassen AG erfolgt bei der Abwicklung des Zahlungsverkehrs. Hierbei werden schriftliche Zahlungsanweisungen von der Feuerwehr-Unfallkasse an die Feuerkasse zur weiteren Erledigung übergeben. Ein personenbezogener Rückschluß auf den Leistungsfall läßt sich aus den Zahlungsanweisungen insofern ziehen, als im Verwendungszweck neben der Unfallnummer auch der Name des Empfängers bzw. des Verletzten enthalten sind. Die Feuerwehr-Unfallkasse hat uns zugesagt, dieses Verfahren so zu ändern, daß die Überweisungsträger künftig von Mitarbeitern der Feuerwehr-Unfallkasse erstellt werden.

Bei der automatisierten Datenverarbeitung der Feuerwehr-Unfallkasse mußten wir erhebliche technische und strukturelle Mängel feststellen. Die Unfall- und Buchhaltungsdateien wurden automatisiert im Rechenzentrum der Feuerkasse geführt. Die Speicherung erfolgte auf einem UNIX-Mehrplatzsystem. Die Programmierung und die Systemverwaltung wurden durch Mitarbeiter der Feuerkasse im Rechenzentrum der Feuerkasse wahrgenommen. Es lag insoweit eine Auftragsdatenverarbeitung durch die Feuerkasse vor.

Diese Auftragsdatenverarbeitung wurde mit der Umwandlung der Feuerkasse in eine Feuerkassen AG unzulässig. Nach dem Sozialgesetzbuch wäre eine solche Auftragsdatenverarbeitung durch eine nichtöffentliche Stelle zum einen zulässig, wenn beim Auftraggeber sonst kurzfristige und unvorhersehbare Störungen im Betriebsablauf auftreten können, was vorliegend eindeutig nicht der Fall war. Zum anderen wäre sie auch zulässig, wenn die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden könnten und der überwiegende Teil des gesamten Datenbestandes beim Auftraggeber oder bei einer anderen öffentlichen Stelle als Auftragnehmer verbliebe. Auch dies war vorliegend nicht der Fall, denn der überwiegende Datenbestand wurde bei der Feuerkasse gespeichert.

Die Feuerwehr-Unfallkasse rechtfertigte sich zunächst damit, es handele sich um eine erst seit dem 1. Juli 1994 geltende Regelung des Sozialgesetzbuches. Daher benötige sie eine Übergangsfrist. Diese Einschätzung ist jedoch unzutreffend, denn die zum 1. Juli 1994 erfolgte Änderung des Sozialgesetzbuches

hatte insoweit nur klarstellenden Charakter; in der Sache galt vorher nichts anderes.

Wir haben der Feuerwehr-Unfallkasse mitgeteilt, daß wir von einer förmlichen Beanstandung dieses rechtswidrigen Zustands absehen werden, wenn er in absehbarer Zeit, d.h. spätestens bis zum 31. März 1995, abgestellt wird. Die Feuerwehr-Unfallkasse hat uns dazu inzwischen mitgeteilt, sie strebe einen rechtskonformen Zustand an, sei aber nicht sicher, ob dieser bis zum 31. März 1995 realisiert werden könne.

Wenngleich wir die automatisierte Datenverarbeitung nicht eingehend geprüft haben, stießen wir auf mehrere – zwischenzeitlich abgestellte – Mängel in der Datensicherung.

So liefen auf dem von der Feuerwehr-Unfallkasse genutzten UNIX-Rechner auch Verfahren der Feuerkasse. Eine Kennung der Feuerwehr-Unfallkasse war einer Benutzergruppe zugeordnet, zu der sowohl mehrere Anwender der Feuerkasse als auch drei Standardbenutzer gehörten. Aufgrund der vorgegebenen Zugriffsrechte in den jeweiligen Benutzerverzeichnissen war zumindest die unbefugte gegenseitige Kenntnisnahme von Dateien nicht auszuschließen. Zudem hatten fast alle zugelassenen Benutzer des Rechners grundsätzlich die Möglichkeit, auf die Betriebssystemebene zu gelangen.

Die bei Auslieferung des Betriebssystems bereits standardmäßig vorhandenen und allgemein bekannten Benutzerkennungen waren noch nicht auf ausschließlich den berechtigten Benutzern bekannte Paßworte geändert worden. Für die Benutzung einer dieser Kennungen (mit direktem Aufruf der Shell-Ebene) war sogar überhaupt kein Paßwort vorgegeben.

6.6 Teleworking bei der Landesversicherungsanstalt (LVA)

Im Juni 1994 unterrichtete uns die LVA darüber, daß sie die Möglichkeiten des Einsatzes von Teleworking prüfe. Bei diesem Teleworking handelt es sich begrifflich um eine Form von Heimarbeit, die allerdings nicht unter das Heimarbeitsgesetz fällt. Die Mitarbeiter/innen arbeiten in ihrer Wohnung, in der ihnen ein Bildschirmarbeitsplatz eingerichtet wird. Von diesem aus sind sie im Online-Verfahren mit der LVA verbunden. Die für die Sachbearbeitung erforderlichen Akten werden durch einen Fahrdienst regelmäßig zwischen Wohnung und LVA transportiert.

Die LVA erhofft sich durch Teleworking eine Aktivierung von Mitarbeitern und vor allem Mitarbeiterinnen, die sonst wegen Kindererziehung aus dem Arbeitsprozeß ausscheiden würden. Gegen diese Zielvorstellung ist grundsätzlich nichts einzuwenden. Wir haben die LVA aber darauf hingewiesen, daß Teleworking in der von ihr vorgesehenen Form eine Fülle datenschutzrechtlicher Probleme und Risiken birgt.

Die LVA unterliegt als Sozialleistungsträger der Pflicht aus §§ 35 Abs.1 Satz 2 SGB-I, 78 a SGB-X, durch technische und organisatorische Maßnahmen sicherzustellen, daß die Vorschriften zum Sozialdatenschutz auch tatsächlich eingehalten werden. Dies wird sich bei Teleworking nicht in gleichem Maße durchführen lassen, wie bei Arbeitsplätzen, die unmittelbar im Betrieb angesiedelt sind. Eine effektive Kontrolle der Teleworker durch die LVA und auch durch den Hamburgischen Datenschutzbeauftragten wird durch den grundgesetzlichen Schutz der Unverletzlichkeit der Wohnung sehr erschwert. Um eine stichprobenhafte datenschutzrechtliche Überprüfung der häuslichen Datenverarbeitungsgeräte vornehmen zu können, müßten diese ggf. in die LVA gebracht werden.

Als Rentenversicherungsträger arbeitet die LVA notwendigerweise mit einer Fülle sensibelster Sozialdaten bis hin zu medizinischen Gutachten. Der häusliche Bereich ist aber üblicherweise nicht darauf eingerichtet, solche Unterlagen angemessen zu schützen. Ein solcher Schutz ist im häuslichen Bereich von besonderer Bedeutung, denn Bekannte und Verwandte dürfen keinesfalls Kenntnis von den Sozialdaten erhalten. Risiken bestehen auch durch die im häuslichen Bereich allgegenwärtigen Störfaktoren: Das Telefon klingelt, die Kinder schreien, Postbote oder Nachbarin begehren Einlaß. Solche Störungen werden auch bei bestem Willen der Teleworker unvermeidbar dazu führen, daß notwendige Sicherungsmaßnahmen (Verschließen von Akten, Dunkelschaltung des Bildschirms u.ä.) nicht immer eingehalten werden und die zu schützenden Sozialdaten von anderen Personen in der Wohnung wahrgenommen werden können.

Um die auftretenden datenschutzrechtlichen Risiken zu vermindern, haben wir in Gesprächen mit der LVA bestimmte Anforderungen entwickelt.

Medizinische Daten müssen aus dem Projekt ganz ausgeklammert werden. Dabei muß strukturell sichergestellt werden, daß solche Daten nicht an den häuslichen Arbeitsplatz gelangen. Im übrigen will die LVA auch bei ihr befindliche Akten anderer Stellen, z.B. des Versorgungsamtes, nicht an den häuslichen Arbeitsplatz transportieren.

Teleworking darf nur für einen begrenzten Kreis von Mitarbeiter/innen in Betracht kommen. Die LVA will insoweit eine Beschränkung auf Mütter und Väter vornehmen, die wegen Kindererziehung im Erziehungsurlaub oder beurlaubt sind.

Damit nicht durch routinebedingte Sorglosigkeit Nachlässigkeit bei den Datensicherungsmaßnahmen eintritt, ist zudem eine Befristung der Teilnahme an Teleworking geboten. Jedenfalls zu Beginn des Projekts sollte keine längere Frist als drei Jahre gewählt werden; dies entspricht der geltenden Höchstdauer des Erziehungsurlaubes. Es muß aber auch sichergestellt sein, daß die Teilnahme am Projekt durch die LVA jederzeit beendet werden kann.

Hinsichtlich der häuslichen Voraussetzungen bei den Teleworkern ist es erforderlich, daß ein Raum zur Verfügung steht, in den sich der Teleworker allein zurückziehen und ungestört arbeiten kann. Vor Einrichtung des Teleworking-Arbeitsplatzes muß sich die LVA durch eine Ortsbesichtigung davon überzeugen, daß datenschutzgerechte äußere Arbeitsbedingungen realisierbar sind. Es müssen auch ausreichende Möglichkeiten bestehen, die dienstlichen Unterlagen unter Verschluß zu nehmen.

Für den Transport der Unterlagen von der LVA zum Teleworker und zurück müssen abschließbare Behältnisse verwendet werden. Diese dürfen nicht in öffentlichen Verkehrsmitteln transportiert werden, sondern es muß für den Transport ein Fahr- oder Kurierdienst in Anspruch genommen werden; in Betracht kommen auch Privat-PKW von LVA-Mitarbeitern.

Es muß eine schriftlich dokumentierte Kontrolle darüber geben, welche Unterlagen wann zu wem transportiert wurden, und es muß eine Rücklaufkontrolle erfolgen. Nur die jeweils zur Bearbeitung anstehenden Vorgänge dürfen beim Teleworker sein; er baut keine Registratur auf. Ebenfalls in die LVA zurücktransportiert werden etwaige zu vernichtende Unterlagen, wie Fehlausdrucke.

Hinsichtlich der technischen Gestaltung des Verfahrens muß die LVA sicherstellen, daß ein unbefugter Zugriff (z.B. durch Abhören oder Anzapfen der Leitung) auf die Datenbestände ausgeschlossen ist. Dazu muß auch eine Verschlüsselung aller Daten, die über das öffentliche Netz gesendet werden, ernsthaft in Erwägung gezogen werden. Für die Authentifizierungsdaten (User-ID und Paßwort) ist eine Verschlüsselung unabdingbar, da diese Daten einen unberechtigten Zugriff auf die Datenbank ermöglichen würden.

Um den besonderen Gefahren zu begegnen, die mit der Öffnung des Großrechnerverfahrens für einen externen Zugriff über Telekommunikationsnetze verbunden sind, muß eine strikte automatische Protokollierung der Systemanmeldungen und der mißglückten Anmeldeversuche erfolgen. Es muß nicht nur die Speicherung von Daten, sondern auch der lesende Zugriff von außen (über Telekommunikationsnetze) automatisch protokolliert werden, um einen Mißbrauch bzw. Mißbrauchsversuche möglichst frühzeitig zu erkennen. Zu diesem Zweck müssen Kriterien entwickelt werden, die die automatische Erkennung eines maschinell gestützten Mißbrauchs erkennen lassen (z.B. systematisches Ausprobieren von Kennungen oder Paßwörtern, Abruf größerer Datenmengen usw.). Bei Eintritt entsprechender Konstellationen muß ein Alarm bei dem Systemoperating ausgelöst und die betroffene Kennung bis zur Aufklärung des Falles gesperrt werden. Eine Verwendung der Protokolldaten für Leistungs- und Verhaltenskontrollen könnte und sollte im Rahmen der zu schließenden Dienstvereinbarung ausgeschlossen werden.

Damit die Teleworker eine unberechtigte Kenntnisnahme durch Dritte gezielt unterbinden können, muß eine Dunkelschaltung des Bildschirms nicht nur nach Zeitablauf automatisch erfolgen, sondern auch individuell gezielt erfolgen können. Die Dunkelschaltung darf nur durch Paßworteingabe wieder aufgehoben werden können.

Grundsätzlich denkbare Probleme des Personaldatenschutzes sind bei dem Projekt der LVA kaum zu erwarten. Es erfolgt keine besondere Erfassung der Arbeitszeit, -einteilung und -leistung. Die Teleworker erhalten bestimmte Arbeitskontingente zugewiesen, die sie sich praktisch frei einteilen können.

Um den Personaldatenschutz auch für dienstliche Telefongespräche sicherzustellen, werden zwei Möglichkeiten erwogen. Solange der private häusliche Telefonanschluß vom Teleworker für Dienstgespräche genutzt wird, wird der Telefonverkehr in der Regel so realisiert, daß Anrufer bei der LVA anrufen und vom Teleworker zurückgerufen werden. Den Versicherten wird die private Telefonnummer des Arbeitnehmers grundsätzlich nicht bekanntgegeben. Auch die Tatsache, daß sich eine Akte in häuslicher Bearbeitung befindet, wird nicht preisgegeben, damit keine Rückschlüsse auf das Privatleben des Teleworkers (Erziehungsurlaub, Kinder) gezogen werden können. Die Abrechnung des Telefons erfolgt über eine Pauschale. Alternativ kann dem Teleworker ein zweites Telefon für Dienstgespräche zur Verfügung gestellt werden. In der LVA eingehende Anrufe können auf dieses häusliche Diensttelefon umgeleitet werden.

Wir haben die LVA gebeten, das Projekt datenschutzgerecht weiterzuentwickeln und die bisher sehr positive Weise unserer Beteiligung fortzusetzen. Dafür wäre es sachgerecht, wenn uns die zu erstellenden Papiere (Dienstvereinbarung, -anweisung u.ä.) im Entwurf überlassen würden, damit etwa erforderliche Anregungen noch eingearbeitet werden können.

6.7 Ausforschung des Adoptionsgeheimnisses bei der Überprüfung des Kindergeldanspruchs

Im April 1994 erhielten wir einen Hinweis auf eine bundesweite Aktion zur Überprüfung des Kindergeldanspruchs, bei der auch die Hamburger Behörden ihre Mitarbeiter befragten, sofern sie Kindergeld bezogen. Hintergrund der Aktion war eine Gesetzesänderung. Verwendet wurde ein Vordruck, der auch nähere Angaben zum Verhältnis des Kindes zum Kindergeldberechtigten und zu dessen Ehegatten vorsah.

Dieser Vordruck ließ zum einen den gesetzlich geforderten Hinweis vermissen, ob eine Rechtsvorschrift zur Beantwortung der Fragen verpflichtet. Der schwerwiegendste Mangel des Vordrucks bestand aber in der Frage, ob die Kinder adoptiert waren.

Wir wiesen das Senatsamt für den Verwaltungsdienst (SfV) umgehend darauf hin, daß diese Fragestellung wegen des Adoptionsgeheimnisses schweren datenschutzrechtlichen Bedenken begegnet.

Das SfV hielt es nicht für nötig, sich mit diesen inhaltlichen Bedenken auseinanderzusetzen. Es beschränkte sich auf den Hinweis, die Zahlung von Kindergeld an Angehörige des öffentlichen Dienstes erfolge im Auftrag des Bundes, von dem auch der fragliche Vordruck stamme (zu den datenschutzrechtlichen Handlungsmöglichkeiten bei Auftragsverwaltung nach Art. 84 ff. Grundgesetz siehe 1.6).

Wir bekräftigten gegenüber dem SfV daraufhin unsere Auffassung, daß die Frage nach einem Adoptionsverhältnis in dem Vordruck eine unzulässige Datenerhebung sei, da die Adoptivkindeigenschaft für die Überprüfung des Kindergeldanspruchs nach § 1754 Bürgerliches Gesetzbuch und § 1 Bundeskindergeldgesetz ohne Bedeutung ist. Es war für uns überraschend, daß ein so offensichtlich unzulässiges Verfahren offenbar ohne weiteres ausgeführt wurde. Es wäre unerläßlich gewesen, daß sich das SfV vor Durchführung der Überprüfungsaktion umgehend bei den zuständigen Bundesministerien für eine datenschutzgerechte Gestaltung des Vordrucks eingesetzt hätte.

Nachdem aber „das Kind in den Brunnen gefallen" war, hätte das SfV umgehend in Absprache mit den zuständigen Bundesministerien veranlassen müssen, daß die bereits verwendeten Vordrucke vollständig darauf durchgesehen werden, ob ein Adoptionsverhältnis angegeben wurde. In diesen Fällen hätten die Vordrucke vernichtet und durch einen datenschutzgerechten Vordruck ersetzt werden oder wenigstens die Angaben zum Adoptionsverhältnis wirksam gelöscht werden müssen.

Die Bremer Senatskommission für das Personalwesen veranlaßte bereits am 24. Mai 1994, daß Fragebögen mit offengelegten Adoptivkindverhältnissen gegen neue, datenschutzgerechte Fragebögen ausgetauscht werden. Das Finanzministerium Nordrhein-Westfalens gab am 9. Juni 1994 die Anweisung, daß Angaben über erstmalig offengelegte Adoptivkindverhältnisse zu löschen seien. Das Bundesministerium für Familie und Senioren hatte spätestens am 22. Juni 1994 keine Bedenken mehr dagegen, daß Angaben über erstmals offengelegte Adoptivkindverhältnisse wieder gelöscht werden. Gleichwohl wartete das SfV auch Ende August immer noch eine Stellungnahme des Bundesministeriums für Familie und Senioren ab.

Erst am 20. September 1994 teilte das SfV den nachgeordneten Behörden mit, daß Angaben über ein erstmalig offengelegtes Adoptivkindverhältnis zu löschen seien. Inwieweit dieser Aufforderung Folge geleistet wurde, entzieht sich unserer Kenntnis. Mit einer bloßen Schwärzung der unzulässigen Angaben würde eine Löschung im Rechtssinn nicht erreicht werden, da weiterhin erkennbar bliebe, daß Angaben über ein Adoptivkindverhältnis gemacht wurden.

7. Personalwesen

7.1 Projekt Personalwesen (PROPERS)

In den letzten Berichten (vgl. 11. und 12. TB, 7.1) sind wir ausführlich auf die Entwicklungen beim Projekt Personalwesen (PROPERS) eingegangen. Mittlerweile sind bereits verschiedene Behörden mit IuK-Technik ausgestattet und Mitarbeiter geschult worden, so daß bereits auf einer Reihe von Arbeitsplätzen technikunterstützt mit der Nutzung von Textbausteinen für die Erstellung von Schreibwerk gearbeitet werden kann.

Demnächst wird darüber hinaus in der Behörde für Schule, Jugend und Berufsbildung (BSJB) die Pilotierung der automatisierten Personal-Stammdatenverarbeitung beginnen, allerdings noch ohne Bezügeabrechnung. In diesem Zusammenhang sind wir an der Abstimmung verschiedener Datenkataloge intensiv beteiligt gewesen.

Beim jetzt pilotierten Datenkatalog Personalverwaltung sind unsere Anregungen und Hinweise aufgegriffen worden. So wurde sichergestellt, daß bei Wiedervorlagen aus medizinischem Anlaß Angaben über Untersuchungsgründe nicht ausgewertet werden können und nicht zum Nachteil des Betroffenen verarbeitet werden. Außerdem wurde zugesichert, bei den Wiedervorlagegründen die Möglichkeiten zur Eingabe von Freitexten auf das unbedingt erforderliche Maß zu begrenzen und deutliche Erläuterungen zu ihrer datenschutzrechtlichen Problematik in Hilfetexten, Handbuch und Schulungen aufzunehmen. Anders als bei vorgegebenen Merkmalsausprägungen kann der Sachbearbeiter in Freitexten beliebige Informationen eingeben, die jedenfalls nicht maschinell abgeprüft werden. Damit bestünde die besondere Gefahr, daß an sich unzulässige Daten im Einzelfall doch gespeichert werden könnten.

Daneben haben wir uns zum vorgelegten logischen Datenmodell „Personalplanung und Personalentwicklung" geäußert. Wir begrüßen, daß in diesem empfindlichen Bereich nur die erforderlichen und nicht etwa alle wünschenswerten Daten erhoben werden sollen und dabei ganz auf sogenannte „weiche Daten" verzichtet wird, deren Aussage sich nur aus ihrem Kontext erschließen läßt. In einem weiteren Verfahrensschritt, in dem auch die Historientiefe und die Relevanz für das Berichtswesen abgestimmt werden soll, haben wir allerdings deutliche Zweifel angemeldet (vgl. 7.6.2).

Verschiedene Hinweise haben wir auch zur Leistungsbeschreibung für die Ausschreibung einer Softwareunterstützung des Bereichs Fortbildung gegeben. Es ist beabsichtigt, für diesen Bereich ein Standardprodukt einzusetzen, das den spezifischen hamburgischen Erfordernissen anzupassen ist. Es ist vorgesehen, regelmäßig einen gewissen Grunddatensatz für die Dozenten- und Teilnehmerverwaltung aus dem Datenkatalog Personalverwaltung zu ziehen.

Aus datenschutzrechtlicher Sicht ist es zunächst erforderlich, Daten, die nur für Planungszwecke gebraucht werden, auch nur anonymisiert auszuwerten. Beispielsweise ist es für die Klärung der Frage, ob sich das Angebot verschiedener Seminare mit Kinderbetreuungsangebot lohnt , nicht erforderlich, regelmäßig personenbezogene Angaben über beurlaubte und teilzeitbeschäftigte Mitarbeiter , ihre Kinderzahl und das Alter der Kinder zu erhalten. Darüber hinaus ist es auch sinnvoll, die Datenfelder und Verwaltungabläufe danach zu differenzieren, ob es sich um verbindliche Schulungen oder um freigestellte Fortbildungsangebote handelt. Je verbindlicher die Fortbildungsmaßnahme ist, desto umfassender können die dafür erforderlichen Daten verwaltet werden; besteht jedoch nur die theoretische Möglichkeit einer Teilnahme, sollten untypische und nicht regelmäßig erforderliche Angaben erst bei der Anmeldung zu einem solchen Fortbildungsangebot auf freiwilliger Basis erhoben werden. Auch hierüber werden die Gespräche fortgesetzt.

Von PROPERS wird auch der Einsatz von „Electronic Mail" vorbereitet (vgl. hierzu näher 3.4.)

7.2 Projekt Automation der Stellenplanung (ProStep)

Im Januar 1994 wurde das Projekt „Automation der Stellenplanung" eingerichtet, in dessen Lenkungsgruppe ich vertreten bin. Ziel ist, das veraltete zentrale Stellenplanverfahren zu ersetzen und gleichzeitig Entscheidungsbefugnisse zu dezentralisieren.

Bisher besteht zentral lediglich ein automatisierter Soll-Stellenplan; der zentrale Ist-Stellenplan wird noch manuell über Karteikarten und Listen geführt. Daneben bestehen in verschiedenen Behörden dezentrale automatisierte Verfahren zur Führung des Ist-Stellenplans.

ProStep soll ermitteln, auf welche Weise technikunterstützt das Stellensoll, die Stellenbesetzung und die Aufgabengliederung umfassend dokumentiert und ausgewertet werden können. Das Verfahren muß so gestaltet werden, daß eine vollständige Revisionsfähigkeit der Abläufe gesichert ist. Daneben soll das System die dezentrale Stellenplanung in den Behörden unterstützen und vereinheitlichen.Mehrfache Solldatenhaltungen sollen ebenso vermieden werden wie weitere dezentrale Verfahrensentwicklungen.

Dabei soll zunächst von den derzeitigen rechtlichen Rahmenbedingungen ausgegangen werden.Gleichzeitig sollen abdingbare Rechtsvorschriften auf ihre Erforderlichkeit überprüft werden. Bei allem soll die Möglichkeit für eine Ergänzung oder spätere Ablösung der kameralistischen Stellenplanung durch eine Plan-Personalkostenrechnung mit Kostenstellen offen gehalten werden, wie sie das Neue Steuerungsmodell vorsieht.

Von datenschutzrechtlicher Relevanz ist der Zugriff auf die persönlichen Daten der Beschäftigten, die durch die Personalverwaltung erfaßt und zur Führung

des Ist-Stellenplans benötigt werden. Bisher darf das Organisationsamt als zentrale Verwaltungseinheit nur über stellenbezogene Daten der Behörden und Ämter verfügen, nicht jedoch über Daten der konkreten Inanspruchnahme der Stellen durch Personen. Der Zugriff soll durch eine Schnittstelle zum Personalverwaltungsverfahren von PROPERS realisiert werden.

Bereits in der ersten Sitzung der Lenkungsgruppe wurde der Auftrag erteilt, ein eigenes Datenschutzkonzept zu entwickeln. Ein abschließender Datenkatalog über die Auswertungen mit Personenbezug wurde angekündigt. Wir haben dringend empfohlen, das Datenschutzkonzept so rechtzeitig zu erstellen, daß seine Anforderungen bei der Bewertung der in Frage kommenden Produkte angemessen einfließen können.

Aus unserer Sicht müssen die Standards, die mit dem Datenschutzkonzept von PROPERS bereits 1990 vorgegeben wurden (Festlegung unter anderem zu Zwecken der Verarbeitung, Herkunft, Übermittlung, Zugriff und Auswertungen der Daten, Löschungsfristen, technischen und organisatorischen Maßnahmen zum Datenschutz), auch für ProStep gelten .

Die Übermittlung personenbezogener Daten im Einzelfall wird wesentlich von der künftigen Ausgestaltung der Zuständigkeiten im Stellenplanverfahren abhängen. Es wird sorgfältig zu prüfen sein, ob neue Übermittlungen zwischen zentraler und dezentraler Stelle, die bisher nicht stattfinden, tatsächlich erforderlich sind. Dies bezieht sich z.B. auf die Namen der Stelleninhaber im Verwaltungsgliederungsplan, auf den auch das Organisationsamt Zugriff haben soll. Darüber hinaus darf keine namensbezogene Stellenhistorie geführt werden. Schließlich sollte auch der vorgesehene Auswertungskatalog alle vordefinierten Auswertungen abschließend festlegen. Ad-hoc-Auswertungen mit Personenbezug müssen ausgeschlossen sein.

7.3 Neues Personalaktenrecht

Mit der Verabschiedung des Zweiten Gesetzes zur Änderung dienstrechtlicher Vorschriften ist das neue Personalaktenrecht (vgl. schon 11. und 12. TB, 7.2) für Beamte und Richter in Hamburg umgesetzt worden. Mit der anstehenden Novellierung des § 28 HmbDSG soll es auch auf alle übrigen Beschäftigten erstreckt werden.

Zur Umsetzung hat das Personalamt im September 1994 den Entwurf einer Anordnung über die Führung und Verwaltung der Personalakten der hamburgischen Beamten vorgelegt. Darin wird auf eine abschließende Regelung von Personalakteninhalten verzichtet, um Spielräume für spezielle Behördenbelange offenzuhalten.

Obwohl der Entwurf sich weitgehend an die Begründung des Zweiten Gesetzes zur Änderung dienstrechtlicher Vorschriften anlehnt, werden doch verschiedene Regelungen getroffen, die die datenschutzrechtlichen Belange der

Betroffenen zusätzlich verstärken. Dazu gehört die detaillierte Regelung zur Anlage von Teilakten, außerdem die Pflicht, Äußerungen des Beamten zur Personalakte zu nehmen, sowie die Pflicht, den Beamten über sein Antragsrecht nach § 96 f HmbBG zu belehren.

In unserer Stellungnahme haben wir aber auch verschiedene Bedenken geltend gemacht:

Vor allem ist angesichts des bereits seit dem 1. April 1994 geltenden Rechts eine Übergangsfrist zur Umsetzung der neuen Regelungen von 5 Jahren nach Inkrafttreten der Anordnung nicht vertretbar. Die Frist zur Umsetzung muß verhältnismäßig sein und darf die Betroffenen in ihren bereits bestehenden Rechten nicht beschneiden. Da Datenschutzbelange auch durch die Gliederung der Personalakte betroffen sind, halten wir eine Befristung der Übergangsvorschrift auf 2 Jahre nach Inkrafttreten des Gesetzes für noch vertretbar.

Ferner bedarf es einer konkreten Aussage, daß Zielvereinbarungen im Rahmen von Mitarbeiter- und Vorgesetztengesprächen (7.6.1) nicht zur Personalakte gehören. Schließlich kann auch das Recht des Beamten, selbst über die Bekanntgabe seiner Daten zu verfügen, ohne gesetzliche Grundlage nicht wirksam eingeschränkt werden. Im Zusammenhang mit dem Akteneinsichtsrecht ist daher die vorgesehene Regelung zu streichen, daß der betroffene Beamte seine Kenntnisse aus der Personalakte nur zur Wahrung berechtigter Belange nutzen darf und auf seine beamtenrechtliche Verschwiegenheitspflicht hinzuweisen ist.

7.4 Novellierung von § 28 Hamburgisches Datenschutzgesetz

Im Rahmen der Abstimmung von § 28 HmbDSG war unser wesentliches Anliegen, konkrete Regelungen zum Umgang mit Gesundheitsdaten künftig auch für bestehende Beschäftigungsverhältnisse zu treffen. Ziel war es, den inzwischen einvernehmlich erreichten datenschutzrechtlichen Standard beim Personalärztlichen Dienst (vgl.12.TB, 7.2.2, 7.3) zu sichern. Wir hatten vorgeschlagen, daß bei medizinischen oder psychologischen Untersuchungen möglichst tätigkeitsbezogene Risikofaktoren mitgeteilt werden, soweit sich entsprechende Bedenken ergeben. Wenn sich keine Bedenken ergeben, soll nach unserem Vorschlag nur das Ergebnis der Untersuchung ohne weitere Zusätze übermittelt werden.

Will man gemäß dem neuesten Entwurf erreichen, daß erforderlichenfalls auch darüber hinausgehende Daten wie z.B. Einzelbefunde und Anamnesedaten von der Personalstelle verlangt werden dürfen, darf sich das nur auf wenige begrenzte Ausnahmefälle beschränken und nur erfolgen, wenn die Kenntnis dieser besonders sensiblen Daten für die Entscheidung im Einzelfall unerläßlich ist.

Außerdem haben wir eine ausdrückliche Erstreckung der Planungsanforderungen nach § 30 HmbDSG auf die Datenverarbeitung im Beschäftigungsverhältnis verlangt. Hintergrund ist die zunehmende Bedeutung des Berichtswesens im Personalbereich (vgl. 7.6.2). Es muß klargestellt werden, daß Personaldaten bei der Erhebung von Planungsgrundlagen denselben Schutz genießen wie andere personenbezogene Daten.

7.5 Gleichstellung

Im Berichtsjahr haben wir uns mit verschiedenen Untersuchungsvorhaben des Senatsamts für die Gleichstellung (SfG) befaßt, die eine Vielzahl datenschutzrechtlicher Fragen sowohl hinsichtlich der Durchführung als auch hinsichtlich des Inhalts aufwarfen.

So hatten wir uns im Rahmen der Untersuchung zur Gestaltung von Stellenausschreibungstexten der Justizbehörde insbesondere damit zu beschäftigen, welche datenschutzrechtlichen Anforderungen bei Mitarbeiterbefragungen (vgl. 7.6.1) zu beachten sind und welchen Einfluß dies auf die Vertragsgestaltung bei der Auftragsvergabe an Externe hat. Wegen der offenbar steigenden Bedeutung des Instruments der Mitarbeiterbefragung haben diese Überlegungen zu unserer Empfehlung geführt, eine Datenschutzrichtlinie zur Personalentwicklung zu erlassen (vgl. 7.6.3).

Inhaltlich haben wir uns auch intensiv mit den Ergebnissen einer Untersuchung bei der Oberfinanzdirektion über Anforderungen an Potentialerkennung und Führungskultur sowie an Mitarbeiterinnen-Beurteilungen auseinandergesetzt.

Die vorgeschlagenen Neuerungen lehnen sich eng an die im privatwirtschaftlichen Bereich eingesetzten Beurteilungsmuster an. Sie sind wegen der strengeren gesetzlichen Vorgaben im öffentlichen Bereich aber nur sehr bedingt umsetzbar. Hierauf haben wir im einzelnen ausführlich hingewiesen. Wie wir jetzt erfahren haben, sollen die vorgeschlagenen Neuerungen nicht als Handreichung für einen Entwurf eines neuen Beurteilungswesens verstanden werden. Zusammen mit dem Erhebungsteil zum bestehenden Beurteilungssystem sollen sie vielmehr nur der Sensibilisierung gegenüber dem bestehenden System dienen, und zwar unter dem Aspekt, frauenspezifische Verhaltens- und Vorgehensweisen zu erkennen und angemessener zu würdigen. Unsere Hinweise bleiben gleichwohl für künftige Regelungen relevant.

7.6 Personalentwicklung

Im Berichtsjahr ist das strategische Personalentwicklungskonzept (vgl. 12. TB, 7.11) von 1991 in verschiedenen Bereichen weiter konkretisiert worden. Neben einer Untersuchung zur Neukonzeption der Führungsfortbildung und der Einrichtung eines Gesprächsforums Personalmanagement mit den leitenden Be-

amten der Behörden waren für uns die Weiterentwicklung des Mitarbeiter- und Vorgesetztengespräches (7.6.1) und die Einbeziehung des Berichtswesens (7.6.2) von besonderer Bedeutung.

7.6.1 Mitarbeiter- und Vorgesetztengespräch

Über den Entwurf eines Gesprächsleitfadens zur Führung von Mitarbeiter- und Vorgesetztengesprächen und unsere Stellungnahme dazu hatten wir im 12. TB (7.11) berichtet. Im Juli 1994 erreichte uns eine aus der Sicht des Personalamts abschließende Version des Leitfadens. Er besteht aus einer „Orientierungshilfe", die im wesentlichen dem Entwurf des Gesprächsleitfadens entspricht. Er umfaßt außerdem „Vorbereitungshilfen", die in Kürze die Inhalte der Orientierungshilfe wiedergeben sowie weitere konkrete Anweisungen und veränderte Formulare zur Dokumentation der Zielvereinbarungen enthalten.

Die „Vorbereitungshilfen" wirken wesentlich weniger datenschutzfreundlich, da sie an verschiedenen Stellen durch die Wortwahl ein größeres Maß an Verbindlichkeit vorgeben als die „Orientierungshilfe". Das Personalamt hat daraufhin insbesondere den freiwilligen Charakter des Gesprächs bestätigt. Wir haben weitere Klarstellungen und Hinweise verlangt, die sich unter anderem aus den gesetzlichen Anforderungen bei freiwilligen Angaben ergeben. Wir haben gebeten, diese zunächst mit einem ergänzenden Rundschreiben bekanntzugeben und bei nächster Gelegenheit in die „Orientierungshilfe" und die „Vorbereitungshilfen" aufzunehmen. Daneben haben wir wiederholt gebeten zu prüfen, ob die Zielvereinbarungen der Mitbestimmung unterliegen und ob sie nach den neuen Vorschriften zum Personalaktenrecht in die Personalakte aufgenommen werden müssen.

Das Personalamt hat darauf verwiesen, daß die Papiere einander ergänzten und im übrigen auch inhaltlich keine Notwendigkeit zu den von uns erbetenen Änderungen bestünde. Ein gemeinsames Gespräch brachte keine Klärung. Wir haben das Personalamt unter vertiefter Darlegung unsere Auffassung nochmals aufgefordert, die Papiere zu ergänzen und unter Fristsetzung unsere Ankündigung wiederholt, anderenfalls selbst ein Rundschreiben an denselben Empfängerkreis zu richten. Ein entsprechender Entwurf wurde beigefügt.

7.6.2 Berichtswesen

Im Zuge der Diskussion und der Erprobung des Neuen Steuerungsmodells (Bürgerschaftsdrucksache 15/1813 vom 13. September 1994) kommt dem Berichtswesen eine gesteigerte Bedeutung zu. Es wird verstanden als allgemeines betriebswirtschaftliches Steuerungsinstrument zur Unterstützung von Planung und Erfolgskontrolle. Als solches ist es grundsätzlich in allen Bereichen einsetzbar. Daraus folgt zunächst, daß es kein spezifisches Instrument des Personalwesens im Sinne des § 28 Abs. 1 HmbDSG ist. Es muß vielmehr in seiner

jeweiligen Ausformung allen einschlägigen datenschutzrechtlichen Bestimmungen entsprechen.

Zum Personalberichtswesen gehören nach einer Aufgabenbeschreibung des Projekts PROPERS (siehe 7.1) unter anderem Bestandsanalysen (Statistik) und die Motivationsforschung (Mitarbeiterbefragungen). Die Personalstatistik haben wir im Rahmen des Datenkatalogs zur Personalplanung und -entwicklung in einem ersten Durchlauf näher betrachtet. Außerdem haben wir uns mit verschiedenen Mitarbeiterbefragungen beschäftigt. Sie waren nicht immer im Personalentwicklungsbereich angesiedelt, warfen aber datenschutzrechtlich dieselben Fragen auf.

— Personalstatistik

Mit dem Datenkatalog Personalplanung und Personalentwicklung im Rahmen von PROPERS sollen auch alle für die Personalentwicklung berichtsrelevanten Daten festgelegt und mit einer Historie versehen werden, die an den Bedürfnissen des Berichtswesens ausgerichtet ist. Die vorgesehenen Zeiträume für die Historie übersteigen die zulässigen Speicherungsfristen für Aufgaben der personenbezogenen Personalentwicklung erheblich.

Wir haben deshalb gefordert, mit verschiedenen Löschungsfristen für personenbezogene Einzelfallbearbeitung einerseits und für personalstatistische Zwecke andererseits, eine Löschung der personenbezogenen Daten jeweils im Rahmen der gesetzlichen Vorschriften zu gewährleisten. Gleichzeitig ist sicherzustellen, daß die Mitarbeiter der Stelle, die die anonymisierten Einzeldaten längerfristig verwaltet und auswertet, diese Daten nicht einzelnen Personen zuordnen können. Diese Stelle ist deshalb organisatorisch und personell von der übrigen Personalverwaltung abzuschotten.

Es besteht Einigkeit mit PROPERS, daß die Daten nur anonymisiert zu Berichtszwecken verwendet werden sollen. Hierzu haben wir verschiedene Hinweise gegeben. Die Vorstellungen von PROPERS gehen dahin, mit den anonymisierten Daten sowohl regelmäßig wiederkehrende Auswertungen als auch Ad-hoc-Auswertungen vorzunehmen. Insbesondere sollen sowohl punktuelle Querschnittsanalysen als auch weit in die Vergangenheit zurückreichende Längsschnittanalysen möglich sein. Dafür sollen pro Person regelmäßig 70 berichtsrelevante Merkmale aufgenommen werden.

Ein besonderes Problem liegt in der Dauer der Speicherung: Nur 9 Merkmale werden zeitlich befristet (3 – 5 Jahre bei Fortbildung, Nebentätigkeit und Parlamentszugehörigkeit) gespeichert. Angaben zum Aufstiegsdatum und Aufstiegsgrund sowie zum maßgeblichen Tarifvertragsabschnitt sollen aktuell gespeichert werden. Alle anderen Daten sollen für die Dauer des Beschäftigungsverhältnisses oder unbegrenzt gespeichert werden. Dazu gehören Angaben zur Qualifikation, zum erlernten Beruf, zum Ausbildungs-

ende, zu Verwendungsbeginn und Verwendungsende je Stelle, zur Amtsbezeichnung inklusive Änderungsdaten, zu Unterbrechungsgründen und -zeiten, zu Teilzeitbeschäftigungszeiten und zu Vergütungs- und Lohngruppen.

Alle diese Daten können auch in anonymisierter Form so kodiert werden, daß sie im Statistikdatenbestand wieder pro Person verwaltet werden. Das bedeutet, daß ein detailliertes Bild über den Berufsverlauf der Person entsteht und zum Teil noch über Aussagen der Stellenbeschreibung, zum Beispiel über die wahrgenommenen Aufgaben und die Zahl der unterstellten Mitarbeiter ergänzt werden kann. Durch die längere Speicherungsdauer wird ein vollständigeres Abbild der Person erreicht, als es mit den Daten für Personalverwaltungs- und -entwicklungszwecke möglich ist.

Angesichts der Vielzahl der berichtsrelevanten Daten haben wir erhebliche Bedenken, ob die zunächst anonymisierten Einzeldaten auch in ihrer Gesamtheit anonymisiert bleiben oder durch dieses „Mosaik" nicht doch wieder auf eine bestimmte Person bezogen werden können. Sobald sie in ihrer Gesamtheit personenbeziehbar sind, gelten die allgemeinen Beschränkungen, die an personenbezogene Datensätze zu stellen sind. Wir haben deshalb in einer ersten Einschätzung empfohlen, auch die ohne Namen und Personalnummer gespeicherten Einzeldatensätze nicht länger zu speichern als die direkt personenbezogenen Daten, die für die konkrete Personalplanung benötigt werden.

Wie die geplante Anonymisierung der Berichtsdaten gewährleistet werden kann und ob der Katalog der berichtsrelevanten Daten zu reduzieren ist, muß noch weiter geklärt werden.

— Mitarbeiterbefragungen

Im Rahmen von Untersuchungen zur Personalentwicklung und zur Erstellung des Gleichstellungsberichts hat es bereits verschiedene Mitarbeiterbefragungen gegeben, so z.B. in den Untersuchungen des Senatsamts für die Gleichstellung (SfG) (7.5), aber auch in der Wirtschaftsbehörde zu Fragen der Behördenstruktur und Effizienzsteigerung sowie im Landesbetrieb Krankenhäuser (LBK) zur Unternehmenskultur und zum Personalcontrolling. Hierher gehören auch die Befragungen, die von den behördlichen Frauenbeauftragten oder Personalentwicklern durchgeführt werden, um Grundlagenmaterial zur Entscheidung über Zielgruppen und Fördermaßnahmen zu erhalten, das aus vorhandenen Daten nicht erschlossen werden kann.

Allen Befragungen war gemeinsam, daß sie Einschätzungen und Verbesserungsvorschläge von Mitarbeitern, also Meinungen, abgefragt haben. Auch Meinungen sind personenbezogene Daten und unterfallen dem Schutz des HmbDSG. Sie beziehen sich regelmäßig auf Auskünfte, die für den täglichen Arbeitsablauf nicht erforderlich sind, so daß sie von den allgemeinen

Zwecken der Personaldatenverarbeitung nach § 28 Abs. 1 HmbDSG nicht unmittelbar erfaßt sind.

Die Erhebungen müssen deshalb auf freiwilliger Basis erfolgen, und die Mitarbeiter sind über den genauen Zweck der Erhebung, die Art und Dauer der Speicherung der Daten und ihre Übermittlung aufzuklären. In der Regel muß ein schriftliches Einverständnis vorliegen. Mitarbeiterbefragungen sollten grundsätzlich nicht von Personalabteilungen oder deren Vorgesetzten betreut werden. Bei der Auftragsvergabe an Externe sind umfassende Vereinbarungen über die Datenverarbeitung, die Datensicherheit und insbesondere die sachgerechte Vernichtung der Datenträger durch den Auftragnehmer zu treffen. Beim Einsatz von Fragebögen ist das Mitbestimmungsrecht der Personalräte zu beachten.

Darüber hinaus können im Einzelfall sehr vielschichtige Fragen auftreten. So muß auch der Persönlichkeitsschutz Dritter beachtet werden: Beurteilungen über reidentifizierbare Vorgesetzte oder sonstige Dritte sind ohne deren Einverständnis unzulässig.

7.6.3 Datenschutzrichtlinie zur Personalentwicklung

Die vorgenannten Erfahrungen haben uns veranlaßt, beim Personalamt und beim Senatsamt für die Gleichstellung (SfG) den Erlaß einer Datenschutzrichtlinie zur Personalentwicklung anzuregen. Unsere Vorstellung ist, den Anwendern möglichst verbindliche, ablauforientierte Hinweise zu den regelmäßig betroffenen datenschutzrechtlichen Fragestellungen an die Hand zu geben.

Wir haben unter Hinweis auf das HmbDSG deshalb angeregt, folgende Punkte aufzunehmen:

— Personenbezogene Datenverarbeitung grundsätzlich nur für die Personalentwicklung im Einzelfall, für andere Zwecke möglichst nur anonymisierte Erhebungen und Auswertungen mit Aggregierung;

— frühestmögliche Anonymisierung, getrennte Verarbeitung und generelle Abschottung;

— Erhebung möglichst auf freiwilliger Grundlage mit Aufklärung und schriftlicher Einwilligung;

— Datenverarbeitung unter Beachtung des Datengeheimnisses getrennt vom Personalverwaltungsbereich, z.B. bei den Personalentwicklern;

— Beauftragung Dritter nur bei eindeutigen Vorgaben und Weisungen;

— Erstellung von Geschäftsstatistiken gemäß § 8 HmbStatG;

— Unterrichtung des HmbDSB nach § 23 Abs. 4 Satz 2 HmbDSG gemäß Beteiligungsrichtlinie.

Das Personalamt und das SfG haben sich ebenso wie die nachrichtlich beteiligte Finanzbehörde und Justizbehörde dafür ausgesprochen, angesichts der schon bestehenden Vorschriftenflut und der bereits geltenden einschlägigen Vorschriften keine Richtlinie zu erlassen. Keine Bedenken wurden gegen eine informierende Arbeitshilfe geltend gemacht. Dazu wurde darauf hingewiesen, daß Mitarbeiterbefragungen auch zu verschiedenen anderen Anlässen und nicht nur zur Personalentwicklung durchgeführt werden.

Uns geht es um die Sicherstellung einer datenschutzgerechten Praxis. Wenn auf der von uns vorgeschlagenen Grundlage Einigkeit über die anzuwendenden Vorschriften besteht, kann auch eine Arbeitshilfe weiterführen. Sie wäre dann auf alle Anwendungsfälle von Mitarbeiterbefragungen zu beziehen. Demgemäß werden wir uns weiter für eine datenschutzgerechte Verfahrensweise bei Mitarbeiterbefragungen einsetzen.

7.7 Personaldatenverarbeitung bei den Personalräten

7.7.1 Stammdatensätze

Im 12. TB (7.8) haben wir uns mit der Frage beschäftigt, ob und in welchem Umfang der Personalrat personenbezogene Beschäftigtendaten regelmäßig benötigt und in welcher Form er sie verarbeiten darf. Wir hatten mit dem Personalamt seinerzeit Einigkeit erzielt über die einzelnen Daten eines Stammdatenkatalogs, nicht aber über die Frage, ob diese dem Personalrat auch automatisiert zur Verfügung gestellt und von ihm weiterverarbeitet werden können.

Der Sachstand ist unverändert. Nach Auffassung des Personalamts wird eine solche Regelung dem Gesetzgeber vorbehalten bleiben müssen. Wir haben sie deshalb in unsere Vorschläge zur Novellierung des Hamburgischen Personalvertretungsgesetzes (HmbPersVG) aufgenommen.

7.7.2 Verwaltung von personenbezogenen Unterlagen

Wie wir in Beratungsgesprächen wiederholt erfahren haben, besteht bei den Personalräten große Unsicherheit über den Umgang mit personenbezogenen Daten im eigenen Bereich. Bisher gibt es hierzu noch keine bereichsspezifischen Regelungen; erfreulicherweise haben aber die Personalräte offenbar ein zunehmendes Problembewußtsein.

Nach unserer Erfahrung fordern die Dienststellen Unterlagen über Mitbestimmungsverfahren einschließlich Schlichtungs- und Einigungsstellenverhandlungen sowie auch die detaillierten Deputationsunterlagen nicht von den Personalräten zurück. Bei weiterer Verwaltung dieser Unterlagen entstehen Abbilder der Beschäftigten, die außerhalb der Personalakten nicht geführt werden dürfen. Spätestens seit Inkrafttreten des neuen Personalaktenrechts ist auch gesetzlich geklärt, daß Unterlagen, die Personalaktendaten sind, nicht mehr außerhalb der Personalakten geführt werden dürfen.

Auch mehr als 10 Jahre nach dem Volkszählungsurteil war noch unklar, ob die in § 9 HmbPersVG geregelte Verschwiegenheitspflicht des Personalrats auch gegenüber dem Betroffenen zum Schutz des Beratungsgeheimnisses gelte oder ob sein Akteneinsichts- und Auskunftsanspruch nach §§ 96 d Abs. 2 HmbBG, 29 HmbVwVfG, 18 HmbDSG Vorrang habe.

In Anbetracht der bevorstehenden Novellierung des HmbPersVG haben wir dem Personalamt kürzlich Vorschläge unterbreitet, die die Verschwiegenheitspflicht konkretisieren und die Möglichkeit vorsehen, daß der Betroffene zu den ihn betreffenden Beratungen hinzugezogen werden kann. Weiter soll der Umfang der Unterrichtungspflicht abschließend festgelegt werden, der Umgang mit personenbezogenen Daten während der Sitzung klargestellt werden und festgelegt werden, daß personenbezogene Unterlagen aus Mitbestimmungsverfahren und der Deputationsbeteiligung nach deren Beendigung zurückzugeben sind. Andere Unterlagen sollen spätestens nach 2 Wahlperioden vernichtet werden. Geregelt werden soll auch die Verantwortlichkeit für die Einhaltung des Datenschutzes. Ferner soll gesetzlich vorgesehen werden, daß der Personalrat sich jederzeit direkt an den Hamburgischen Datenschutzbeauftragten wenden kann.

Wir haben bewußt auf generalklauselartige Darstellungen verzichtet. Nach unserer Erfahrung ist es wichtig, den Personalratsmitgliedern klare, möglichst abschließende Regelungen an die Hand zu geben. Nur so kann der Datenschutz auch nach Neuwahlen jederzeit gesichert bleiben.

7.8 Ärztlicher Dienst der Behörde für Inneres (Bfl)

7.8.1 Defizite bei der Datensicherung

Polizisten und Feuerwehrbeamte genießen freie Heilfürsorge. Das bedeutet, daß der Dienstherr ihnen grundsätzlich jede erforderliche medizinische Behandlung zukommen läßt und die Beamten nur im Ausnahmefällen berechtigt sind, andere als die sog. Polizeiärzte in Anspruch zu nehmen. So entstehen beim Ärztlichen Dienst der Bfl Krankenakten, die alle Gesundheitsdaten der Betroffenen in einem Umfang enthalten, der sonst nur bei Hausärzten besteht.

Anfang 1993 wurde dieses Regel-Ausnahme-Verhältnis umgekehrt und allen Beamten die freie Arztwahl ermöglicht. Dadurch verschoben sich die Aufgaben des für die freie Heilfürsorge zuständigen Ärztlichen Dienstes der Bfl: Ärztliche Praxen wurden geschlossen, die dort geführten Krankenakten wurden zentral archiviert, die Abrechnungsabteilung des Ärztlichen Dienstes wurde erweitert, und die personalärztlichen und arbeitsmedizinischen Aufgaben erhielten stärkeres Gewicht. Mit dieser Umstrukturierung ging eine Funktionstrennung der einzelnen Bereiche einher, die auch eine jeweils eigene Aktenführung erforderte.

Durch eine Eingabe wurden wir auf die Archivierung der nicht mehr weitergeführten Krankenakten aufmerksam gemacht. Sie werden in einem Gebäude gelagert, in dem die meisten Abteilungen des Ärztlichen Dienstes untergebracht sind. 3 der 5 Abteilungen haben täglich Publikumsverkehr, überwiegend nach Terminabsprache.

Dort haben wir erhebliche Defizite bei der äußeren Datensicherheit festgestellt. So war die Eingangstür zwischen 6.30 Uhr und 15.30 Uhr für jedermann geöffnet . Eine Kontrolle der Berechtigung war weder vorgesehen noch möglich. In den Räumen der Ärztlichen Praxis können mangels Schallschutzes Patientengespräche in der Wartezone mitgehört werden.

Die Archivräume für die nicht mehr fortgeführten Krankenakten liegen im Keller und auf dem Boden. Sie wurden zum Teil auch für Unterlagen des Personalärztlichen und des Arbeitsmedizinischen Dienstes genutzt. Jeder Mitarbeiter hatte Zugang zum Archiv, ein Schlüssel war sogar frei im Keller zugänglich deponiert. Daneben war auch die Abschottung der einzelnen Bereiche gegeneinander unzureichend: Nur die Räume der Verwaltungsabteilung waren durch einen eigenen Schließkreis vor dem Zugriff Dritter gesichert.

Regelmäßig wurden für Aufgaben des Arbeitsmedzinischen Dienstes und des Personalärztlichen Dienstes die Krankenakten der Ärztlichen Praxen herangezogen.

Als Sofortmaßnahme hatten wir hinreichende Regelungen zum Umgang mit den personenbezogenen Unterlagen gefordert sowie den Einbau einer elektronischen Klingel- und Schließanlage, mit der das Gebäude jederzeit geschlossen werden kann. Außerdem sollte auch durch den Einbau eigener Schließkreise die Abschottung der einzelnen Bereiche sichergestellt werden. Der Zugriff auf die Archivunterlagen sollte sachgerecht begrenzt und dokumentiert werden.

Die Umsetzung dieser Maßnahmen hat sich zum Teil erheblich verzögert, so daß wir mehrfach eine förmliche Beanstandung androhen mußten. Nachdem wir uns in nachfolgenden Gesprächen auf den Einsatz einer Archivkraft einigen konnten, die allein Zugriff auf die archivierten Krankenakten hat und einzelne Unterlagen nur auf Anforderung zur Verfügung stellt, haben wir von einer Beanstandung abgesehen. Leider verzögerte sich auch der Einsatz dieser Kraft wieder erheblich.

Zu Redaktionsschluß erreichte uns die Nachricht, daß die Unterlagen anderer Abteilungen aus dem Archivraum entfernt worden sind, so daß jetzt nur noch die Archivkraft Zutritt zu den Archivräumen hat.

Wir haben jetzt unsere weitergehenden, grundsätzlichen Anforderungen an die Datensicherungsmaßnahmen formuliert. Dabei haben wir uns davon leiten lassen, daß der Ärztliche Dienst mit den Krankenakten über Vorgänge von ein-

maliger Sensibilität verfügt; daher sind zum Teil höhere Anforderungen als beim Personalärztlichen Dienst des Senatsamts für den Verwaltungsdienst erforderlich.

Im wesentlichen werden noch folgende Anforderungen zu erfüllen sein: Wir halten eine Unterbringung der Krankenakten und der Krankenkassenunterlagen in Stahlschränken für erforderlich. Dies gilt auch für die Krankenakten im Bereich der Ärztlichen Praxis und auch für das Archiv, wenn, wie zur Zeit geplant, die Archivkraft später wieder abgezogen werden sollte.

Zum Schutz vor unberechtigtem Eintritt müssen die Untersuchungsräume und die Archivräume durch Türknäufe geschützt werden. Im Bereich der Ärztlichen Praxis ist der Schallschutz und auch die Absicherung der Fenster zu verbessern.

Schließlich sind auch die Aufbewahrungsfristen von zur Zeit 30 Jahren zu überprüfen. Für uns sind keine Umstände ersichtlich, die eine regelhaft längere Aufbewahrung als in privaten ärztlichen Praxen und beim Personalärztlichen Dienst des Senatsamts für den Verwaltungsdienst erfordern. Dort betragen sie regelmäßig 10 Jahre; lediglich für Dienstunfallangelegenheiten und arbeitsmedizinische Unterlagen gelten längere Fristen.

7.8.2 Bewerberdaten

Bereits im 12. TB (7.10) haben wir über den Umgang mit Bewerberdaten bei der Polizei berichtet. Im Berichtsjahr haben wir uns zur weiteren Abklärung intensiv mit den Bestimmungen der bundesweit geltenden Polizeidienstvorschrift 300 (PDV 300) auseinandergesetzt, die die ärztliche Beurteilung der Polizeidiensttauglichkeit und der Polizeidienstfähigkeit regeln. Darin ist genau festgehalten, welche Störungen und Erkrankungen („Fehler") zu einer Untauglichkeit führen und in welcher Form (ärztliches Gesundheitszeugnis) sie der personalverwaltenden Stelle mitzuteilen sind.

Nach unserer Auffassung reicht für die ordnungsgemäße Ermessensausübung auch in ablehnenden Fällen die Übermittlung der „Fehlerangaben" an die Einstellungsstelle, im Einzelfall ggf. mit erläuternden Hinweisen. Mit Verfügung vom 1. Oktober 1991 wurde die PDV 300 für Hamburg jedoch insoweit geändert, als das gesamte ärztliche Gutachten, also auch Befund- und Anamnesedaten, regelmäßig an die Einstellungsstelle weiterzuleiten waren.

Hiergegen haben wir Bedenken erhoben und die Aufhebung der Verfügung vom 1. Oktober 1991 gefordert. Nach Auffassung der Polizei ist die Verfügung bereits in der Vergangenheit datenschutzgerecht ausgelegt worden: es würden ausschließlich Daten, Befunde und Diagnosen in Form einer gutachterlichen Stellungnahme mitgeteilt, soweit sie Risikofaktoren darstellten.Auch dies geht noch über die Anforderungen hinaus, wie wir sie in die Novellierung von § 28

HmbDSG eingebracht haben. Hierauf haben wir die Behörde für Inneres (Bfl) hingewiesen.

Verzichten Bewerber auf das weitere Bewerbungsverfahren, werden ärztliche Unterlagen zwei Jahre lang aufgehoben. Diese Frist erscheint sachgerecht im Hinblick auf die auch von uns unterstützte Forderung (vgl. 12. TB, 7.2.3), Bewerberdaten bei der Polizei länger speichern zu können. Bisher wurde dem Grunde nach Einvernehmen erzielt, die Aufbewahrungsfrist der Bewerber-Karteikarten auf die Zeitspanne zu begrenzen, in der erfahrungsgemäß die meisten Wiederholungsbewerbungen eingehen.

7.9 Anamnesebögen der ärztlichen Dienste

Im 12. TB (7.3) haben wir über die Erörterung der Anamnesebögen mit den ärztlichen Diensten berichtet. Anlaß waren wiederkehrende kritische Fragen zur Zulässigkeit einzelner Fragestellungen gewesen, so etwa nach Selbstmordversuchen, Geschlechtskrankheiten und Drogenkonsum, und zwar zum Teil auch über Verwandte. Hinsichtlich solcher Fragestellungen konnte jetzt Einvernehmen erzielt werden:

Wie berichtet, erreichte uns Ende 1993 ein Entwurf des Personalärztlichen Dienstes (PÄD), der den datenschutzrechtlichen Anforderungen gerecht wurde. Darin wird auf die oben genannten Fragestellungen verzichtet; lediglich die Behandlung im Zusammenhang mit einer Suchtkrankheit wird erfragt. Auch der Arbeitsmedizinische Dienst hat zwischenzeitlich seinen Fragebogen geändert und darin letztlich auch auf die Angabe des behandelnden Hausarztes verzichtet. Der Personalärztliche Dienst der Behörde für Inneres (Bfl) hat den Fragebogen des PÄD übernommen mit der Maßgabe, daß auch nach dem Konsum von Drogen gefragt wird. Hiergegen haben wir wegen der besonderen körperlichen und geistigen Anforderungen im Polizei- und Feuerwehrdienst keine Bedenken erhoben.

Noch offengeblieben ist aber die Frage nach dem Umfang der an die personalverwaltenden Stellen weiterzugebenden Daten.

Der Fragebogen des PÄD beinhaltet den Hinweis, daß die Grundlagen des Untersuchungsergebnisses, also auch Befunde und Vorgeschichte, und deren medizinische Bewertung mitgeteilt werden, soweit es für die auftraggebende Stelle erforderlich ist. Der Fragebogen der Bfl enthält eine Einverständniserklärung zur Weitergabe des ärztlichen Zeugnisses.

Wir haben demgegenüber eine differenzierte Vorgehensweise gefordert, wie sie auch in unserem Novellierungsvorschlag zu § 28 HmbDSG enthalten ist (7.4). Insoweit ist die Einwilligungserklärung im Formular der Bfl nicht zu beanstanden.

Unzulässig und unwirksam ist nach unserer Auffassung aber die weitergehende pauschale Einwilligung in die Weitergabe der Untersuchungsbefunde innerhalb des ärztlichen Dienstes. Zum ärztlichen Dienst der Bfl gehören auch die Ärztlichen Praxen, die die Hausarztfunktion für diejenigen Beamten wahrnehmen, welche das Angebot, niedergelassene Ärzte aufzusuchen, nicht nutzen.

Für diesen Personenkreis bedeutet die Einwilligung, daß der Dienstherr, vertreten durch den Personalärztlichen Dienst der Bfl, jederzeit Zugriff hat auf alle kurativen Daten, die sonst beim Hausarzt zusammenlaufen und zum Teil über Jahrzehnte entstanden sind. Es ist offenkundig, daß der Zugriff in diesem Umfang für den Dienstherrn nicht erforderlich und damit unzulässig ist. Er bedeutet auch eine Ungleichbehandlung gegenüber all denjenigen, die sich nicht mehr in den Ärztlichen Praxen der Bfl versorgen lassen.

Wir haben deshalb darauf hingewiesen, daß eine Einwilligungserklärung grundsätzlich nicht dazu führen kann, eine an sich unzulässige Datenverarbeitung zu sanktionieren. Die Bfl kündigte jetzt eine datenschutzgerechte Überarbeitung der Einwilligungserklärung an.

8. Statistik, Wahlen

8.1 Prüfung der Wahlstatistik zur Europawahl 1994

Bei der Wahl zum Europäischen Parlament am 12. Juni 1994 wurde vom Statistischen Landesamt eine repräsentative Wahlstatistik durchgeführt. Gemäß § 78 Abs. 1 Europawahlordnung müssen die Stimmbezirke so ausgewählt und die Auszählungen so durchgeführt werden, daß das Wahlgeheimnis gewahrt ist. Gemäß § 78 Abs. 2 Europawahlordnung dürfen die Ergebnisse für einzelne Stimmbezirke nicht bekanntgegeben werden.

Wir haben im Sommer 1994 geprüft, ob diese rechtlichen Vorgaben eingehalten wurden. Die Prüfung hat ergeben, daß das Wahlgeheimnis gewahrt wurde.

Dagegen war die Unterrichtung der Betroffenen über die Wahlstatistik nicht ausreichend: Der Bundeswahlleiter hatte ein Faltblatt über die Durchführung der repräsentativen Wahlstatistik nur in einer Auflage von 5.000 Exemplaren für Hamburg zur Verfügung gestellt. Zur Unterrichtung der in die Statistik einbezogenen 13.700 Wahlberechtigten reichte diese Anzahl jedoch nicht aus.

Das Statistische Landesamt hat zugesagt, daß bei zukünftigen Wahlstatistiken Informationsblätter in ausreichender Auflage zur Verfügung stehen.

8.2 Keine Wahlstatistik bei der Bundestagswahl

Bei der Bundestagswahl am 16. Oktober 1994 hat es keine Wahlstatistik mit Stimmzetteln gegeben, die nach Geschlecht und Altersgruppen markiert waren. Es gab auch keine besonderen differenzierten statistischen Auszählun-

gen über die Wahlbeteiligung. Der Bundestag hatte die entsprechenden Vorschriften des Bundeswahlgesetzes und der Bundeswahlordnung ausgesetzt, weil befürchtet wurde, daß durch eine derartige Zwangsstatistik die Gleichheit der Wahl und das Wahlgeheimnis beeinträchtigt würden. Der Bundesrat hatte sich mit seiner Forderung, die Wahlstatistik gleichwohl bei der Bundestagswahl durchzuführen, im Vermittlungsausschuß nicht durchsetzen können.

8.3 Speicherung von Unterstützungsunterschriften

Für die Bundestagswahl am 16. Oktober 1994 konnten kleine Parteien, die nicht im Bundestag oder in einem Landtag vertreten sind, nur kandidieren, wenn sie die Unterstützung einer ausreichenden Zahl von Wahlberechtigten nachwiesen.

Das Wahlrecht der Unterstützer mußte durch die zuständige Gemeindebehörde geprüft und bescheinigt werden. § 34 Abs. 6 Bundeswahlordnung verbietet es der für die Wahlrechtsbescheinigung in Hamburg zuständigen Behörde für Inneres festzuhalten, für welchen Wahlvorschlag – z.B. der Partei A – die Wahlrechtsbescheinigung – z.B. des Bürgers Z – bestimmt ist. Die Behörde für Inneres hatte auf den von ihr alphabetisch geführten Prüfbogen, auf denen das Ergebnis der Prüfung des Wahlrechts vermerkt ist, jeweils auch eine „Kontrollistennummer" verzeichnet.

In denselben Räumen, in denen diese Unterlagen verwahrt wurden, wurde auch die gesamte Kontrolliste gesondert und verschlossen aufbewahrt. Zu der Kontrolliste hatten die Mitarbeiter der Behörde für Inneres Zugang, die für die Geschäftsstelle des Landeswahlamts tätig waren. Anhand der Kontrollistennummern konnten sie nachvollziehen, für welchen Wahlvorschlag die Bescheinigung jeweils bestimmt war, d.h. für welche Partei ein Bürger eine Unterstützungsunterschrift abgegeben hat.

Wir haben die Behörde für Inneres aufgefordert, das Verfahren zur Prüfung von Unterstützungsunterschriften zu ändern und datenschutzrechtlich einwandfrei zu gestalten. Insbesondere ist sicherzustellen, daß in Zukunft nicht mehr dieselben Mitarbeiter der Behörde für Inneres zunächst als Gemeindebehörde und später als Landeswahlamt tätig werden dürfen. Der Landeswahlleiter hat zugesagt, daß eine Personenidentität künftig ausgeschlossen wird

8.4 Gewinnung von Wahlhelfern

Aufgrund einer Eingabe haben wir uns damit beschäftigt, auf welche Weise Wahlhelfer zur Wahl zum Europäischen Parlament gewonnen wurden.

Ein Bezirksamt hatte im Rahmen der „freiwilligen" Gewinnung von Mitgliedern der Wahlvorstände seine Mitarbeiterinnen und Mitarbeiter dazu aufgefordert, sich entweder für diese Aufgabe zur Verfügung zu stellen oder aber Gründe zu benennen, weshalb sie daran gehindert seien. Die Bediensteten sollten diese

schriftlichen Erklärungen mit zum Teil sensiblen persönlichen Informationen, die in keinem Zusammenhang mit dem Dienst- und Beschäftigungsverhältnis standen, jeweils über ihre Vorgesetzten abgeben.

Diese Erhebung personenbezogener Daten verstieß gegen § 28 Abs. 1 HmbDSG, der die Verarbeitung von Beschäftigtendaten grundsätzlich nur erlaubt, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses erforderlich ist.

Zwar sieht § 11 Bundeswahlgesetz vor, daß jeder Wahlberechtigte als Wahlhelfer verpflichtet werden kann; jedoch läßt sich aus dieser Vorschrift keine besondere Ermächtigung für die Verarbeitung der Daten von Mitarbeitern des öffentlichen Dienstes außerhalb des Verfahrens der formellen Verpflichtung herleiten. Da auch keine andere Rechtsvorschrift die Erhebung dieser Daten durch das Bezirksamt erlaubte, war die Datenerhebung unzulässig.

Das Bezirksamt hat versichert, daß die Fragebögen nicht zu den Personalakten genommen sondern vernichtet worden seien. Unsere Intervention hat ferner bewirkt, daß die Bezirksamtsleitung die Vorgesetzten angewiesen hat, die aufgrund der Rückläufe erworbenen Kenntnisse nicht zu verwerten .

Die Wahlhelfergewinnung für die Bundestagswahl 1994 erfolgte auch in diesem Bezirksamt auf freiwilliger Basis ohne schriftliche Mitarbeiterbefragungen und ohne unzulässige Verarbeitung von Personaldaten.

8.5 Novellierung des Mikrozensusgesetzes

Das Bundesministerium des Innern (BMI) hat im April 1994 einen Arbeitsentwurf für ein neues Gesetz zur Durchführung einer Repräsentativererhebung über die Bevölkerung und den Arbeitsmarkt (Mikrozensusgesetz) vorgelegt. Dieser Entwurf sieht die Ausweitung der Auskunftspflicht auch auf solche Erhebungsmerkmale vor, deren Beantwortung bislang freiwillig war. Ferner soll in Zukunft beim Mikrozensus eine große Anzahl neuer Merkmale erhoben werden, deren Angabe ebenfalls Pflicht ist.

Die starke Ausweitung der mit Auskunftspflicht versehenen Fragen wird mit der allgemeinen Formulierung begründet, es dürfte „nach den bisher vorliegenden Ergebnissen der noch laufenden Untersuchungen des Statistischen Bundesamts einerseits, aber auch aufgrund der sich bei der Interpretation der „freiwilligen Fragen" selbst ergebenden Probleme kein Zweifel darüber bestehen, daß die Ergebnisqualität von Merkmalen mit freiwilliger Auskunftserteilung im Vergleich zu „Pflichtmerkmalen" i.d.R. deutlich vermindert ist."

Die Gesetzesnovelle würde zu zusätzlichen Eingriffen in das Recht auf informationelle Selbstbestimmung führen. Dafür ist eine derartig pauschale Begründung völlig inakzeptabel. Einschränkungen des Rechts auf informationelle Selbstbestimmung sind nach der Rechtsprechung des Bundesver-

fassungsgerichts im Volkszählungsurteil (BVerfGE 65, 1) nur im überwiegenden Allgemeininteresse zulässig. Die Entscheidung über den Umfang des Erhebungskatalogs und über die Auskunftspflicht müssen im Detail begründet sein.

Es besteht die Gefahr, daß mit der Ausweitung des Datenkatalogs eine zwangsweise Registrierung des Menschen in seiner Persönlichkeit stattfindet. Dies wäre gemäß der Rechtsprechung des Bundesverfassungsgerichts in seinem Mikrozensusurteil (BVerfGE 27, 1) unvereinbar mit dem Persönlichkeitsrecht.

Bei der Beurteilung der Eingriffstiefe ist die Entwicklung der Verarbeitungstechnik zu berücksichtigen, die sich seit 1969 – als das Bundesverfassungsgericht über die Verfassungsmäßigkeit des Mikrozensus zu entscheiden hatte – stark verändert hat. Die heutige miniaturisierte Datenverarbeitungstechnik durchdringt immer weitere Lebensbereiche; eine individuelle Verhaltenskontrolle wird auf diese Weise erleichtert.

In einem derartigen Umfeld mit vielfältigen neuen Datenschutzrisiken tritt die Notwendigkeit zur Datenvermeidung wesentlich stärker in den Vordergrund. Anstatt die Aufblähung des Mikrozensus-Datenkatalogs zu betreiben, sollte besser geprüft werden, ob nicht angesichts des Fortschritts in den Sozialwissenschaften Einschränkungen bei der Befragung möglich sind.

Wir haben die Behörde für Inneres darum gebeten, unsere Bedenken gegenüber dem BMI und im Bundesrat zu vertreten.

9. Schulwesen

9.1 Schulgesetzentwurf

Die nun seit über zehn Jahren währende Diskussion mit der Behörde für Schule, Jugend und Berufsbildung (BSJB) um bereichsspezifische Regelungen zur Schülerdatenverarbeitung (vgl. zuerst 3. TB, 3.5.2, zuletzt 12. TB, 9.1) dauert leider immer noch an.

Im Oktober 1994 erfuhren wir von der BSJB, daß aus der vorgesehenen Novellierung des Schulgesetzes einzelne Punkte vorgezogen werden, damit diese zum Schuljahr 1995/1996 wirksam werden können. Die datenschutzrechtlichen Regelungen gehören jedoch nicht dazu. Der Unterausschuß „Datenschutz" des bürgerschaftlichen Rechtsausschusses hat – in Übereinstimmung mit unserer Forderung – in seiner Sitzung am 28. Oktober 1994 geäußert, daß die Regelungen zum Datenschutz ab dem Schuljahr 1995/1996 wirksam werden sollen. Die BSJB erwägt, ab dem Schuljahr 1995/1996 – vorbehaltlich des Ergebnisses der derzeitigen Diskussion zum Entwurf eines neuen Schulgesetzes – bereits gemäß den mit uns abgestimmten Regelungen zu verfahren.

10. Finanzen und Steuern

10.1 Stand der Gesetzgebung im Steuerbereich

10.1.1 Abgabenordnung

Im letzten Tätigkeitsbericht (vgl. 12. TB, 10.1) haben wir ausführlich über anstehende datenschutzrelevante Änderungen der Abgabenordnung (AO) berichtet. Trotz erheblicher Bedenken der Datenschutzbeauftragten des Bundes und der Länder sind einige Änderungen mit dem Gesetz zur Bekämpfung des Mißbrauchs und zur Bereinigung des Steuerrechts vom 21. Dezember 1993 in Kraft getreten. Dazu gehören die neuen Regelungen in § 88 a und § 249 Abs. 2 AO.

Zum einen handelt es sich dabei um die Sammlung geschützter Daten in Dateien oder Akten „für Zwecke zukünftiger Verfahren" und deren Offenbarung an andere Finanzbehörden. Welche Verfahren mit dieser Formulierung tatsächlich gemeint sein sollen, wird nur beispielhaft in der Begründung des Gesetzes aufgeführt (u.a. die Einrichtung einer automatisiert geführten bundesweiten Fahndungsdatei). Eine normenklare gesetzliche Festlegung des Verwendungszweckes der gesammelten Daten, der zugelassenen Datenarten, des betroffenen Personenkreises und der Datenempfänger ist jedoch nicht erfolgt. Zum anderen dürfen die Finanzbehörden nunmehr Kenntnisse, die sie in einem Besteuerungsverfahren erlangt haben, auch für die Vollstreckung außersteuerlicher Rückstände verwenden. Die bisherige Zweckbindung von Steuerdaten an steuerrechtliche Tatbestände ist damit aufgehoben.

Im 12. TB (10.1.2) hatten wir kritisiert, daß beabsichtigt sei, die bislang mit dem Entwurf eines Gesetzes zur Änderung der Abgabenordnung verfolgte Ergänzung und Präzisierung der bereichsspezifischen Datenschutzvorschriften vorerst zurückzustellen. Bereits eine solche Verzögerung haben wir angesichts der hierüber seit Jahren geführten Diskussion für nicht vertretbar gehalten. Ende Februar 1994 hat das Bundesministerium der Finanzen dem Bundesministerium der Justiz sogar mitgeteilt, daß nach Auffassung der zuständigen Vertreter der obersten Finanzbehörden der Länder zur Zeit kein Handlungsbedarf für Änderungen der AO in datenschutzrechtlicher Sicht bestehen würde. Es sei deshalb nicht vorgesehen, den gesetzgebenden Körperschaften in absehbarer Zeit eine Änderung der AO auf dem Gebiet des Datenschutzes vorzuschlagen.

Wir werden uns trotzdem weiter dafür einsetzen, daß die AO der neueren Datenschutzgesetzgebung angepaßt und der Umgang mit Daten, die dem Steuergeheimnis unterliegen, deutlicher und verständlicher als bisher geregelt wird.

10.1.2 Mitteilungsverordnung

Am 1. Januar 1994 ist die Mitteilungsverordnung in Kraft getreten. Sie verpflichtet alle Behörden und die öffentlich-rechtlichen Rundfunkanstalten, den Finanzbehörden unter bestimmten Voraussetzungen alle Zahlungen für Lieferungen oder Leistungen mitzuteilen. Meldepflichtig sind außerdem Honorare der Rundfunkanstalten für Leistungen freier Mitarbeiter, Verwaltungsakte, die den Wegfall oder die Einschränkung einer steuerlicher Vergünstigung bewirken, Ausgleichs- und Abfindungszahlungen nach dem Flurbereinigungsgesetz sowie gewerberechtliche Erlaubnisse und Gestattungen.

Diese Rechtsverordnung beruht auf einer bereits im Dezember 1985 beschlossenen Ergänzung der Abgabenordnung (§ 93 a). Ohne den Erlaß einer solchen bereichsspezifischen Regelung durften die Finanzämter bislang von den Behörden keine sogenannten Kontrollmitteilungen verlangen.

Die Mitteilungen müssen neben dem Grund und dem Tag der Zahlung die Bezeichnung (Name, Vorname, Firma) und die Anschrift des Zahlungsempfängers sowie – falls bekannt – auch dessen Steuernummer und Geburtsdatum enthalten.

Aufgrund einer Änderung des § 93 a AO im Zuge des Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetzes ist nach entsprechender Anpassung der Mitteilungsverordnung zukünftig auch die Höhe der jeweiligen Zahlung an die Finanzbehörden zu übermitteln. Ein diesbezüglicher Regierungsentwurf liegt dem Bundesrat bereits zur Zustimmung vor.

Aus datenschutzrechtlicher Sicht ist zu begrüßen, daß die mitteilungspflichtigen Stellen den Betroffenen von ihrer Verpflichtung, Mitteilungen zu erstellen, spätestens bei der Übersendung der ersten Mitteilung an die Finanzbehörden zu unterrichten haben.

10.2 Prüfung des Verfahrens zur Erhebung der Zweitwohnungsteuer

Im letzten Tätigkeitsbericht (vgl. 12. TB, 10.2) hatten wir über bestehende Probleme bei der Übermittlung von Meldedaten zwischen dem Amt für zentrale Meldeangelegenheiten und dem Finanzamt für Verkehrsteuern und Grundbesitz im Rahmen der Umsetzung des Zweitwohnungsteuergesetzes berichtet. Im Interesse der Richtigkeit des für die Erhebung der Zweitwohnungsteuer verwendeten Datenbestandes und der Aktualisierung des Melderegisters haben wir im Mai 1994 gemeinsam mit Vertretern der betroffenen Dienststellen Lösungswege erörtert. Dabei haben wir vor Ort anhand von ausgewählten Beispielfällen auch den Verarbeitungsverlauf im automatisierten Verfahren der Steuerverwaltung näher untersucht.

Das Amt für zentrale Meldeangelegenheiten erstellt alle zwei Wochen ein Magnetband mit den Veränderungen im Melderegister, die für das Zweitwohnungsteuerverfahren relevant sind. Dieser Datenträger wird nach den Vorgaben der Steuerverwaltung im Landesamt für Informationstechnik ausgewertet. Die aktualisierten Meldedaten werden in den Speicherkontenbestand der Steuerverwaltung übernommen.

Diese Vorgehensweise bei der Übernahme von Meldedaten in das Zweitwohnungsteuerverfahren wird von der Steuerverwaltung erst seit April 1994 praktiziert. Bis zu diesem Zeitpunkt lag den Ermittlungen des Finanzamtes für Verkehrsteuern und Grundbesitz lediglich der vom Amt für zentrale Meldeangelegenheiten bereits im März 1993 zur Verfügung gestellte Erstdatenbestand zugrunde (per Stichtag 1. Januar 1993 im Melderegister mit Nebenwohnung gespeicherte Einwohner). Dies galt somit auch für die ersten Erinnerungsschreiben. Die seit April 1993 regelmäßig zur Verfügung gestellten Änderungsmitteilungen des Meldewesens wurden erst in einem Gesamtlauf am 11. April 1994 eingespielt. Hierbei ist es zu Problemen gekommen, weil in zahlreichen Fällen Mehrfachänderungen von Datensätzen vorlagen. Diese sind seitens der Steuerverwaltung nicht in der Reihenfolge abgearbeitet worden, wie sie in der meldebehördlichen Datenübermittlung vorgegeben wurden.

Die Vertreter der Finanzbehörde teilten mit, daß die geschilderten Probleme durch Vorkehrungen auf Seiten des Zweitwohnungsteuerverfahrens inzwischen behoben seien. Anhand der Überprüfung ausgewählter Datensätze im Speicherkontenbestand der Steuerverwaltung konnten wir feststellen, daß die aus dem Melderegister übermittelten Anschriftenänderungen im Ergebnis umgesetzt worden sind.

Der am 1. April 1993 in Kraft getretene § 12 Zweitwohnungsteuergesetz schreibt vor, daß das Finanzamt für Verkehrsteuern und Grundbesitz die zuständige Meldebehörde zu informieren hat, wenn sich aus seinen Ermittlungen ergibt, daß eine mit Nebenwohnung gemeldete Person diese nicht mehr innehat. Die Einwohnerdienststellen bekommen aber erst seit Anfang Februar 1994 Rückmeldungen des Finanzamtes über die unzustellbaren Fälle (in Papierform). Seit dem 28. März 1994 enthalten diese Übermittlungen – soweit vorhanden – auch Hinweise auf den Grund der Unzustellbarkeit. Sie bieten eine wesentliche Hilfe für die Aktualisierung des Melderegisters.

Bei Mitteilungen der Meldebehörden über die Aufgabe einer Nebenwohnung oder von Statusänderungen besteht nach Auffassung der Steuerverwaltung und des Finanzamtes weiterhin das Erfordernis zu überprüfen, ob die melderechtliche Mitteilung bezogen auf die Wohnung den tatsächlichen Verhältnissen entspricht. Dies könne in der Regel nur vor Ort durch Ermittlungen von Außendienstmitarbeitern festgestellt werden. Die entsprechenden Datensätze könnten deshalb erst dann gelöscht werden, wenn zweifelsfrei feststeht, daß die betreffende Person tatsächlich ausgezogen ist.

Für diese Überprüfung sind aus datenschutzrechtlicher Sicht jedoch angemessene Fristen vorzusehen. Liegen bis dahin keine gegenteiligen Erkenntnisse vor, ist eine unwiderrufliche Löschung vorzunehmen. Eine solche ist darüberhinaus bei Mitteilung über den Tod der Betroffenen unverzüglich vorzunehmen.

Bei der Überprüfung einzelner Beispielsfälle ist uns aufgefallen, daß auf Datensätze weiterhin zugegriffen werden konnte, die eigentlich im Speicherkontenbestand der Finanzbehörde bereits zu löschen waren. Diese enthielten lediglich den Vermerk „gelöscht am" mit einem Wirkungsdatum. Die Datensätze waren für die Sachbearbeiter im Finanzamt jedoch vollen Inhalts weiter verfügbar.

Die Steuerverwaltung teilte uns dazu mit, daß sie sich bei der Löschung von Speicherkonten aus dem Zweitwohnungsteuerbereich an den im bundeseinheitlichen Verfahren geltenden Kriterien orientieren würde. Der erstmalige Löschungslauf sei für Ende 1994 vorgesehen.

Aus datenschutzrechtlicher Sicht stellt eine solche Verfahrensweise keine Löschung dar. Löschung würde in diesem Fall die Unkenntlichmachung der Personendaten erfordern (§ 4 Abs. 2 Nr. 6 HmbDSG). Die Löschungsverpflichtung tritt immer dann ein, wenn die Kenntnis der Daten zur Aufgabenerfüllung im Verfahren zur Erhebung der Zweitwohnungsteuer nicht mehr erforderlich ist.

11. Wissenschaft, Forschung und Kultur

11.1 Semesterticket des Hamburger Verkehrsverbunds (HVV)

Das 1994 erstmalig ausgegebene HVV-Semesterticket hat auch uns beschäftigt. Es ist im Regelfall datenschutzrechtlich unproblematisch.

Das Semesterticket wird aus den – erhöhten – Studentenschaftsbeiträgen finanziert. Die jeweilige verfaßte Studentenschaft, vertreten durch ihren Allgemeinen Studentenausschuß (AStA), erwirbt vom HVV die Fahrberechtigungen für alle immatrikulierten Studenten. Die Tickets werden von der Hochschulverwaltung ausgestellt und den Studenten mit den Semesterunterlagen zugesandt. Das Ticket ist zusammen mit einem Lichtbildausweis gültig. Die Bezahlung der Tickets erfolgt im Auftrag des AStA durch die Hochschulverwaltung, die aber nur den summierten Betrag (ohne Personenbezug) an den HVV überweist. Wer wegen Diebstahls, Feuers, Raubs, einer Explosion, höherer Gewalt oder des Abhandenkommens des Tickets ein Ersatzticket benötigt, kann das auf einem speziellen Formular beim Studentensekretariat beantragen.

Bei diesem Verfahren benötigen im Regelfall weder die Hochschule noch die Studentenschaft zusätzliche Daten der Studenten. Der HVV erhält in aller Regel überhaupt keine personenbezogenen Daten der Studenten. Er erhält Daten über die Studenten aber dann, wenn wegen Tod oder Exmatrikulation

das Ticket zurückgegeben wird. Bei entsprechendem Nachweis erstattet er dann – ggf. anteilig – die Kosten des Semestertickets.

Datenschutzrechtliche Fragen stellen sich in erster Linie im Zusammenhang mit dem Semesterticket-Härtefonds. Aus diesem können sich Studenten im Einzelfall den Beitrag für das Semesterticket erstatten lassen, wenn sie aus gesundheitlichen, örtlichen oder sozialen Gründen öffentliche Verkehrsmittel nicht benutzen können oder müssen und daher kein Ticket benötigen. Über die genannten drei Erstattungstatbestände hinaus können in besonders begründeten Härtefällen weitere Beitragserstattungen erfolgen.

Einzelheiten des Härtefonds regeln Richtlinien der Studentenparlamente, die von der Behörde für Wissenschaft und Forschung (BWF) genehmigt wurden (Härtefonds-Richtlinie), und eine Vereinbarung zwischen Studentenwerk und ASten (Härtefonds-Vereinbarung). Der Härtefonds wird im Auftrag der ASten vom Studentenwerk verwaltet. Der Erstattungsantrag ist mittels eines speziellen Formulars zu stellen. Der Antrag muß neben gewissen Grunddaten (Name, Bankverbindung u.ä.) eine Begründung enthalten. Gegebenenfalls sind ihm Nachweise beizufügen.

Bei einzelnen Problemfällen kann das Studentenwerk die Stellungnahme eines Härtefonds-Ausschusses einholen. Der Härtefonds-Ausschuß muß zudem vom AStA in Widerspruchsverfahren stets beteiligt werden; der AStA entscheidet über Widersprüche, denen nicht abgeholfen wurde. Der Ausschuß setzt sich zusammen aus Vertretern der Studenten, der jeweiligen Hochschule und des Studentenwerks und tagt nur nicht-öffentlich. Seine Mitglieder sind nach der Härtefonds- Richtlinie zur Verschwiegenheit verpflichtet.

Wir hatten die BWF und das Studentenwerk darauf hingewiesen, daß im Rahmen dieses Erstattungsverfahrens teilweise recht sensible Daten zu verarbeiten sein werden. Dem sollte durch klare Datenverarbeitungsregelungen in der Härtefonds-Richtlinie oder wenigstens in der Härtefonds-Vereinbarung Rechnung getragen werden, und zwar insbesondere zur Aufbewahrungsdauer der Unterlagen und zur Rückgabe von Unterlagen, die zu Nachweiszwecken eingereicht wurden. Leider sind wir mit diesen Empfehlungen nicht durchgedrungen.

Gegenwärtig existiert daher zu diesen Fragen nur ein Hinweis im Antragsformular, daß eingereichte Originalunterlagen zurückgesandt werden, wenn ein Freiumschlag dafür beigefügt wurde. Die BWF hat uns im übrigen mitgeteilt, daß nach Bestandskraft einer Entscheidung die eingereichten Nachweise vernichtet werden.

Das Studentenwerk hat datenschutzrechtlichen Gesichtspunkten aber immerhin dadurch Rechnung getragen, daß zwar die Verwaltung des Härtefonds organisatorisch im Amt für Ausbildungsförderung erfolgt, aber durch speziell dafür abgestellte Mitarbeiter. In der Härtefonds-Vereinbarung ist zudem aus-

drücklich geregelt, daß ein Datenaustausch zwischen der Härtefonds-Stelle und der BAföG- bzw. Wohnabteilung nur mit Einwilligung des Antragstellers stattfindet. Das Studentenwerk hält die Regelung von Aufbewahrungsfristen in der Härtefonds-Richtlinie für geboten, möchte dafür aber zunächst die Erfahrungen aus der zweijährigen Modellphase des Semestertickets abwarten. Auch die BWF möchte zunächst die Erfahrungen aus ein oder zwei Antragsperioden abwarten, ehe Aufbewahrungsfristen geregelt werden.

11.2 Datenverarbeitung in den Fachbereichen der Universität Hamburg

Im 12. TB (11.2) hatten wir darüber berichtet, daß wir bei einer Prüfung in den Fachbereichen Wirtschaftswissenschaften und Psychologie der Universität Hamburg auf IuK-Verfahren gestoßen waren, die den Anforderungen des Hamburgischen Datenschutzgesetzes nicht in allen Punkten entsprachen. U.a. wurde mit Echtdaten entwickelt und getestet. Wir hielten es bereits damals für möglich, daß es sich bei unseren Funden nicht um Einzelfälle handelte, sondern daß in unkontrollierter Weise auch in anderen dezentralen Bereichen der Universität personenbezogene Daten automatisiert für Verwaltungs- und Prüfungszwecke verarbeitet werden.

Wir haben gesprächsweise mit der Verwaltung der Universität die Frage problematisiert, wie solcher „Wildwuchs", von dem auch die Verwaltung der Universität vor unserer Prüfung nichts gewußt hatte, vermieden werden kann. Aufgrund unserer Erörterungen hat die Verwaltung der Universität mit einem Rundschreiben versucht, sich einen aktualisierten Überblick über die automatisierten Datenverarbeitungsverfahren zu verschaffen. Die große Zahl der darauf ergangenen Rückmeldungen macht deutlich, daß in den Fachbereichen der Universität tatsächlich in großem Umfang personenbezogene Daten verarbeitet werden, ohne daß dies der Universitätsverwaltung bekannt war und ohne daß die nach §§ 9, 24 Hamburgisches Datenschutzgesetz erforderlichen Dateibeschreibungen und -meldungen erfolgt waren.

Eine längerfristig tragfähige Lösung dieses strukturellen Problems konnte bislang nicht erarbeitet werden. Sie müßte den Besonderheiten der Universität Rechnung tragen, zu denen insoweit auch eine gewisse Autonomie der Fachbereiche und Institute gehört.

11.3 Veröffentlichung von Daten über Häftlinge des ehemaligen Konzentrationslagers Neuengamme

Bereits seit mehreren Jahren bereitet die KZ-Gedenkstätte Neuengamme die möglichst vollständige Erfassung der Daten von Häftlingen des früheren Konzentrationslagers vor. Als Quellen werden neben den im KZ selbst gefertigten Unterlagen und verschiedenen zeitgenössischen Dokumenten auch die Sterbebücher des Standesamtes Bergedorf und des zwischen 1941 und 1945 eingerichteten Sonderstandesamtes für das KZ Neuengamme herangezogen.

Es ist beabsichtigt, auf dieser Grundlage ein Totenbuch zu erstellen, das folgende Angaben enthält: Vorname, Familienname, Geburtsdatum, Geburtsort, ggf. Ort der Inhaftierung in einem Außenlager des KZ Neuengamme und Todesdatum. Gruppenzugehörigkeit und Todesursache werden nicht angegeben. Dieses Totenbuch soll in zehn Exemplaren gedruckt und als Geschenk der Freien und Hansestadt Hamburg zum 50. Jahrestag an die Amicale Internationale de Neuengamme, die Historischen Kommissionen der französischen und polnischen Lagergemeinschaften überreicht werden. Die weiteren Exemplare sind für die Senatskanzlei, das Staatsarchiv, die Staatsbibliothek und die Forschungstätte für die Geschichte des Nationalsozialismus gedacht.

Darüber hinaus ist anläßlich des 50.Jahrestages der Befreiung vom Nationalsozialismus im Mai 1995 eine Neugestaltung der Gedenkstätte geplant: Im Eingangsbereich sollen Fahnen mit den Namen und dem jeweiligen Sterbedatum die große Zahl der bisher anonymen ca. 55.000 Opfer veranschaulichen.

Gegen diese Vorhaben haben wir keine datenschutzrechtlichen Bedenken. Dies gilt auch, soweit einzelne Angaben auf personenstandsrechtlichen Unterlagen beruhen: Die Vorschriften des allgemeinen Datenschutzrechts finden auf Verstorbene keine direkte Anwendung. Die über den Tod hinaus wirkende Menschenwürde wird durch die Veröffentlichungen nicht verletzt, im Gegenteil: Die Initiative verfolgt gerade den Zweck, der Opfer des Konzentrationslagers in würdiger Form zu gedenken.

§ 61 Personenstandsgesetz (PStG) begrenzt zwar Einsichtnahmen und Auskünfte aus den Personenstandsbüchern auf die Betroffenen selbst, ihre Vorfahren oder Abkömmlinge, Behörden und Personen, deren rechtliche Interessen von den Eintragungen abhängen. Die Vorschrift betrifft nach ihrem Wortlaut nur die Frage des Zugangs zu den in Personenstandsbüchern verzeichneten Angaben. Eine unmittelbare Aussage über die weitere Verwendung der aus Personenstandsbüchern stammenden Angaben enthält sie nicht. Der Schutzzweck von § 61 PStG soll allerdings auch verhindern, daß die Verwendung von Personenstandsangaben dazu führt, daß unberechtigte Interessenten Informationen erhalten, die ihnen aus den Personenstandsbüchern unmittelbar nicht erteilt werden dürften.

Dies erscheint jedoch bei den geplanten Veröffentlichungen ausgeschlossen: Ein nach § 61 PStG nicht Berechtigter würde nur erfahren, daß eine bestimmte Person zu einem bestimmten Zeitpunkt im KZ Neuengamme verstorben ist. Rechtlich relevante Angaben z.B. über Vorfahren, Nachkommen oder sonstige Familienverhältnisse wären hieraus nicht zu gewinnen.

Um etwaige unvorhersehbare Beeinträchtigungen auszuschließen, haben wir folgendes vorgeschlagen : Bestehen in Einzelfällen Bedenken von Angehörigen gegen die Veröffentlichung, darf die Veröffentlichung nur mit ausdrücklicher Einwilligung der Verwandten erfolgen. Bei der Verwertung der einzelnen

Quellen sollte so weit wie möglich darauf geachtet werden, daß die jeweiligen Unterlagen mit anderen abgeglichen werden. Hierbei kann insbesondere den personenstandsrechtlichen Angaben die Funktion zukommen, andere Quellen zu verifizieren. Bei verbleibenden Zweifeln zu einzelnen Angaben sollte deren Veröffentlichung unterbleiben.

12. Bauwesen und Stadtentwicklung

12.1 Einrichtung des Flächenbezogenen Informationssystems (FIS) und Projekt Hamburgisches Automatisiertes Liegenschaftsbuch (HALB)

Das Flächenbezogene Informationssystem (FIS) besteht aus der Beschreibung und der maßstabsgetreuen Abbildung der Grundstücke und Gebäude (Liegenschaften) sowie den Verbindungsdaten zu anderen Dateien und Festsetzungen. Es soll unter Berücksichtigung des neuen Hamburgischen Vermessungsgesetzes (12. TB, 12.1) für alle flächenbezogenen Fachinformationssysteme in der hamburgischen Verwaltung als Basissystem genutzt werden.

Um diesen Anforderungen gerecht werden zu können, soll der bisher in Hamburg von der Kataster- und Vermessungsverwaltung geführte beschreibende Teil des FIS vollständig erneuert und durch ein einheitliches dialog- und batchgesteuertes Anwendungsprogrammsystem unter dem Datenbankverwaltungssystem ADABAS ersetzt werden (Projekt HALB = Hamburgisches Automatisiertes Liegenschaftsbuch). Der graphische Teil des FIS mit der digitalen Stadtgrundkarte (DSGK) soll nach derzeitigem Kenntnisstand unverändert bleiben.

Als wesentlicher Baustein des beschreibenden Teils ist hiervon das z.Z. eingesetzte Automatisierte Liegenschaftsbuch (ALB) betroffen, das im Kern Mitte der 70er Jahre als Programmsystem entwickelt wurde und insbesondere hinsichtlich des Datenschutzes und der Flexibilität nicht mehr den aktuellen Anforderungen gerecht wird.

Mit der Neuentwicklung soll die Funktionalität des Systems erheblich erweitert werden und damit u.a. vorhandenen und potentiellen Benutzern zusätzliche Möglichkeiten bieten, diffenziertere Anforderungen und Bedarfe abzudecken. Insbesondere soll es den Anforderungen als Basissystem für ein Flächenbezogenes Informationssystem gerecht werden.

Wie bereits im 12. TB (12.1) berichtet, ist für die Einrichtung und Erneuerung des FIS (Projekt HALB) eine Lenkungsgruppe eingerichtet worden. Neben Vertretern der Software-Firma und des Vermessungsamtes ist auch der Hamburgische Datenschutzbeauftragte beteiligt, so daß wir insbesondere bei der Erstellung der datenschutzrechtlichen Anforderungen von Anfang an teilnehmen können. Die Lenkungsgruppe dient als Steuerungsgremium für die Neuprogrammierung des beschreibenden Teils des FIS.

Das Projekt HALB befindet sich seit Juni 1993 als Vergabeauftrag in der konkreten Realisierung und soll nach der Projektplanung Anfang 1996 in die Produktion übernommen werden. Es umfaßt vollständig den beschreibenden Teil des FIS. Mit dem Projekt sollen insbesondere auch die technischen datenschutzrechtlichen Voraussetzungen für die umfassende Übermittlung und Nutzung der Daten gem. § 14 Hamburgisches Datenschutzgesetz (HmbDSG) geschaffen werden.

Für die Projektumsetzung gilt unverändert der revidierte Gesamtplan. Die Anforderungsanalyse und der Fachliche Entwurf liegen vor und sind vom Vermessungsamt abgenommen; die Funktionalität des Gesamtsystems ist im Prototyping-Verfahren abschließend erörtert. Der Technische Entwurf – Teil 1 wurde im November übergeben. Erste Tests für Teilkomponenten sollen im 2. Quartal 1995 beginnen.

Als Bestandteil des fachlichen Feinkonzepts wurden uns im März 1994 die geplanten Datenschutzanforderungen (HALB-Datenschutz) zugesandt. Dieses Konzept entsprach weitgehend unseren Erwartungen, so daß bisher nur geringer Erörterungsbedarf vorhanden war. Die Zusammenstellung der Datenelemente der im HALB zusammengefaßten Dateien wurde uns im April zugesandt. Nach bisherigem Kenntnisstand ist das HALB-Datenschutzkonzept für die weitere Projektrealisierung grundsätzlich geeignet.

Enge Kommunikationsbeziehungen bestehen seitens der Vermessungsverwaltung derzeit zu den IuK-Vorhaben „Vollautomation des Grundbuches" der Justizbehörde und „BACom" (Bau-Aufsicht mit Computerunterstützung) des Senatsamtes für Bezirksangelegenheiten. Für den zukünftigen Datenaustausch mit der Grundbuchverwaltung gilt es, bei schwierigen Rahmenbedingungen zeitgerechte Lösungen zu erarbeiten. Mit der Finanzbehörde – Steuerverwaltung – haben erste fachliche Vorgespräche stattgefunden.

Für die Schaffung der rechtlichen Voraussetzungen zur Übermittlung und Nutzung der FIS-Daten liegt die Federführung beim Baurechtsamt der Baubehörde. Wir gehen davon aus, daß die hierfür erforderlichen Abstimmungsverfahren von dort frühzeitig eingeleitet werden.

Über den Fortgang in diesem Projekt werden wir im nächsten TB berichten.

12.2 Projekt Bauaufsicht mit Computerunterstützung (BACom)

Bei der für Mitte 1993 vorgesehenen praktischen Einführung des computerunterstützten Baugenehmigungsverfahrens BACom (vgl. 11. TB, 12.4) haben sich Verzögerungen ergeben, die im wesentlichen auf die umfangreiche Erstellung der Anforderungen für die zum Einsatz kommende Software und die Abwicklung und Auswertung des Ausschreibungsverfahrens zurückzuführen waren. Nach Erteilung des Vergabeauftrages befindet sich das Projekt BACom in der konkreten Realisierung und soll 1995 zum Einsatz gebracht werden.

Das Verfahren BACom besteht im Kern aus einem Grundmodul und zwei weiteren, auf einander aufbauenden ergänzenden Berei chen, der Prüfhilfe und der Verfahrens hilfe.

Das Grundgerüst der Anwendung sind die Programme der Datenbank. Leitlinie ist, daß jede der 22 Bauprüfdienststellen eine eigenständige Einheit ist, die „lokal" und „autonom" arbeiten kann.

Die bauaufsichtlichen Verfahren werden schriftlich durchgeführt. Eine entsprechend hohe Bedeutung hat daher die Textverarbeitung, die von der Datenbank unterstützt wird. Die Vorgangsbearbeitung besteht aus der Ermittlung von Sachverhalten (bedingte Unterstützung durch Bereitstellung von Daten), das Treffen von Entscheidungen (bedingte Unterstützung durch die Bereitstellung von gesetzlichen Grundlagen über die Prüfhilfe) und die Niederlegung der Entscheidungen entweder in strukturierter (Unterstützung durch Eingabemasken und Funktionen der Datenverarbeitung) oder textlicher Form (Textverarbeitung, die eine leistungsfähige Bausteinverarbeitung mit Übernahme von Daten aus der Datenbank beinhaltet).

Da die Mitarbeiterinnen und Mitarbeiter der Bauprüfdienststellen bei der Vorgangsbearbeitung mit anderen hamburgischen Dienststellen kommunizieren müssen, sind in den Verfahrenskern auch Funktionen der elektronischen Post eingebettet. Hinsichtlich der Nutzung dieses Verfahrens für den behördenübergreifenden elektronischen Versand von Dokumenten und der damit verbundenen datenschutzrechtlichen Problematik wird auf auf das Projekt X.400-Dienst – elektronische Post in der hamburgischen Verwaltung – (3.4) verwiesen.

Die Prüfhilfe unterstützt den Sachbearbeiter bei der Entscheidungshilfe durch Bereitstellung von Gesetzestexten, Verordnungen und Fachlichen Weisungen. Die Verschlüsselung und der Zugriffspfad zu den einzelnen Vorschriften orientieren sich streng an den Gliederungsnummern des Bundesrechts. Die Rechtsquellen sind entweder in Form eines Quellenhinweises oder als Volltext verfügbar. Jede Information der Prüfhilfe kann vom Sachbearbeiter ausgedruckt werden.

Die Verfahrenshilfe geht über die Prüfhilfe hinaus. Sie gibt an, in welchen Arbeitschritten ein Vorgang bearbeitet werden soll. In Abhängigkeit davon werden dem Benutzer passende Masken und Datenverarbeitungsmöglichkeiten und/oder Schriftstücke zur Verfügung gestellt. Die Benutzung der Verfahrenshilfe wird dadurch nicht erzwungen. Der Benutzer kann auch über Menüs zu einzelnen Bereichen wie Baugrundstücksdaten oder bauliche Anlagen gelangen und dort Daten erfassen, ändern oder löschen. Dadurch kann ein Benutzer Arbeitsabläufe selbst bestimmen.

Der Kern der Applikation BACom (einschließlich Prüfhilfe) soll bis Ende 1994 fertiggestellt werden. Die Verfahrenshilfe soll bis Ende Februar 1995 zur Verfügung stehen. Anschließend soll im Bezirksamtbereich Hamburg-Wandsbek eine mehrmonatige Pilotierungphase erfolgen. Nach erfolgreichem Abschluß der Pilotierung soll mit dem flächendeckenden Einsatz des BACom-Verfahrens begonnen werden.

Die Informationsstrukturanalyse und das Datenmodell für das Projekt BACom liegen uns vor. Über den Projektfortgang werden wir weiter berichten.

12.3 Prüfung der Wohnraumkartei (WRK- Dialog)

Im 12. TB (12.4) hatten wir berichtet, daß die Wohnraumkartei-Führung auf ein neues automatisiertes Dialog-Verfahren umgestellt werden sollte.

Nachdem Mitte 1993 der Modellversuch erfolgreich abgeschlossen wurde, ist nach weiteren Optimierungen mit dem flächendeckenden Einsatz bei den Einwohnerämtern der Bezirksämter begonnen worden. Die Umstellung bei den Bezirksämtern Wandsbek und Harburg steht noch aus.

Im Oktober 1994 erfolgte eine Prüfung des neuen IuK-Verfahrens zur Führung der Wohnraumkartei (WRK-Dialog) beim Bezirksamt Hamburg-Mitte. Prüfungsgegenstand war die Gewährleistung der technischen und organisatorischen Maßnahmen gemäß § 8 Hamburgisches Datenschutzgesetz.

Für das WRK-Verfahren wird beim Bezirksamt Mitte ein UNIX-Rechner eingesetzt, der in ein Lokales Netz integriert ist, das den überwiegenden Teil der im Bezirksamt Mitte eingesetzten Hardware zusammenfaßt. Dazu zählen neben vier weiteren UNIX-Rechnern eine Reihe von TACLAN-Servern nebst angeschlossenen Terminals. Als zentrale Komponente dient ein sog. Multimedia-Lan-Linkbuilder, der die Funktion eines „Netzwerkverteilers" erfüllt. Auf das WRK-Verfahren wird z.Z. von drei Terminals aus zugegriffen.

Außer für das WRK-Verfahren wird der UNIX-Rechner auch für das Mittelbewirtschaftungsverfahren (MB-Verfahren) eingesetzt. Es sind zu diesem Zweck ca. 200 Benutzerkennungen auf dem Rechner eingerichtet worden, wovon der Großteil auf das MB-Verfahren entfällt. Weiterhin ist Standard-Software (Bürokommunikationssystem, Textverarbeitung und Tabellenkalkulation) installiert.

In dem Netzwerk findet keine Filterung auf Ethernet-Ebene statt, so daß durch das zugrundeliegende Broadcast-Prinzip sämtliche im Netz erzeugten Datenpakete an allen direkt am Netzwerk (d.h. per Ethernetprotokoll) angeschlossenen Komponenten sowie auf allen verlegten Kabellängen verfügbar sind. Ein direkter Zugang zu solchen Komponenten oder der direkte Zugriff auf ein Ethernet-Kabel ist aufgrund der baulichen Situation nur berechtigten Personen möglich. Es sind keine Anschlußpunkte für das lokale Netzwerk außerhalb besonders gesicherter Räumlichkeiten vorhanden.

Der Zugriff auf das WRK-Verfahren ist durch eine zweistufige Benutzerkontrolle geschützt. Zunächst ist eine Anmeldung auf Ebene des Betriebssystems erforderlich, anschließend eine davon unabhängige Anmeldung auf Ebene des Verfahrens selbst.

Die Anmeldung auf UNIX-Ebene erfolgt unter Verwendung eines Paßworts gemäß des von SINIX zur Verfügung gestellten Standards. Zusätzlich zu dieser betriebssystemeigenen Kontrolle wird eine Überprüfung der Nummer des Terminals durchgeführt, von dem aus die Anmeldung erfolgt. Dadurch ist die Anmeldung als WRK-Benutzer auf diejenigen Terminals begrenzt, die für diese Anwendung zugelassen sind.

Für die Anmeldung beim WRK-Verfahren ist zusätzlich die Eingabe einer Benutzerkennung und eines zugehörigen Paßworts erforderlich.

Die verwendeten Paßwörter werden unverschlüsselt als Tabelle gespeichert. Das Verfahren umfaßt eine automatische Paßwortkontrolle, die sicherstellt, daß die Paßwörter mindestens alle 35 Tage gewechselt werden müssen, mindestens sechs Zeichen lang sind und nicht nur aus Buchstaben bestehen.

Jeder Zugriff auf das System oder auf die im System gespeicherten Daten wird in einem Protokoll automatisch dokumentiert (Eingabekontrolle). Für den Protokollausdruck ist der WRK-Administrator zuständig. Ist nach 30 Tagen kein Ausdruck erfolgt, wird der WRK-Administrator durch eine Nachricht am WRK-Bildschirm daran erinnert.

Die Datensicherung wird von dem Systemadministrator wahrgenommen. Er hat dafür Sorge zu tragen, daß diese im Rahmen der routinemäßig ablaufenden „Nachtsicherung" durchgeführt wird (Datenabgangskontrolle). Die Datensicherung erfolgt unverschlüsselt. Dieses steht im Widerspruch zur Verfahrensdokumentation, wonach sicherzustellen ist, daß die Daten verschlüsselt werden.

Neben dem WRK-Verfahren haben WRK-Benutzer auch Zugriff auf andere Programme, die sie über eine Benutzeroberfläche aktivieren können. Eine Verbindung zwischen WRK-Verfahren und anderen Programmen (mit Datenübernahme o.ä.) besteht jedoch nicht. Die verwendete Benutzeroberfläche wird nicht nur den berechtigten WRK-Benutzern, sondern allen UNIX-Benutzern zur Verfügung gestellt. Die Auswahl des WRK-Verfahrens ist damit allen Benutzern möglich. Ein Aktivieren des WRK-Verfahrens und ein Zugriff auf die WRK-Daten wird allerdings durch die beschriebene WRK-eigene Benutzerverwaltung nur bei Kenntnis eines WRK-Paßworts gewährt. WRK-Benutzer haben keine Shell-Berechtigung; technisch ist dies durch eine entsprechende Belegung der Umgebungsvariablen SHELL sichergestellt.

Für die Systemverwaltung und -betreuung sind drei verschiedene Administratoren eingesetzt:

— der Systemadministrator (Systemverwalter) im Bezirksamt Hamburg-Mitte

— der Datenbankadministrator der programmierenden Stelle (Senatsamt für Bezirksangelegenheiten)

— der WRK-Administrator als WRK-Anwender mit besonderen Aufgaben, i.d.R. ein Sachgebietsleiter.

Angesichts der Sensibilität der gespeicherten Daten ist der festgestellte Sicherheitsstandard für die eigene Benutzerverwaltung im WRK-Verfahren positiv anzusehen. Darüber hinaus sind nachfolgende Punkte zu bemängeln:

Die Paßworte sind nach Ziffer 3 der Paßwortlichtlinie vom 21. März 1993 verschlüsselt zu speichern. Weil zu erwarten ist, daß WRK- und UNIX-Paßworte identisch sein können und keine Vorkehrungen dagegen getroffen wurden, sind auch die UNIX-Paßworte gefährdet.

Da über die Benutzeroberfläche allen Rechner-Benutzern das WRK-Verfahren zur Auswahl angeboten wird, sollte eine Differenzierung hinsichtlich der Benutzeroberfläche vorgenommen werden. Es ist nicht erforderlich und datenschutzrechtlich problematisch, daß alle Benutzer des Rechners die gleiche Benutzeroberfläche erhalten. Das WRK-Verfahren sollte nur den tatsächlichen WRK-Benutzern angeboten werden.

Die Datensicherung sollte, wie vom Senatsamt für Bezirksangelegenheiten in der Verfahrensdokumentation selbst gefordert, in verschlüsselter Form durchgeführt werden.

12.4 Prüfung der Vergabe von Sozialwohnungen

Die im 12. TB (12.5) bei der Prüfung der Vergabe von Sozialwohnungen aufgezeigten Organisationsmängel hinsichtlich der Aktenaufbewahrung sind weitgehend nicht behoben worden.

Die Baubehörde begründet dies mit dem bei der Einführung des neuen IuK-Verfahrens zur Führung der Wohnraumkartei (WRK-Dialog) verbundenen zusätzlichen Arbeitsanfall in den bezirklichen Einwohnerämtern, der es wenig sinnvoll erscheinen läßt, die aus der Umstellung auf das neue EDV-Verfahren sich ergebenden Fragen im Hinblick auf die künftige Handhabung und den einheitlichen Umgang mit Aktenvorgängen vor dieser Umstellung abschließend zu behandeln.

Nach der Umstellung bei allen Bezirksämtern ist daher vorgesehen, die noch offenen Fragen in einer Arbeitsgruppe, bestehend aus Vertretern der Bezirksämter, des Senatsamtes für Bezirksangelegenheiten und der Baubehör-

de, zu klären. Dabei sollen auch die Erfahrungen mit dem arbeitsaufwendigeren Berechnungsverfahren berücksichtigt werden, das sich aus der ab 1. Oktober 1994 geltenden Umstellung der Einkommensgrenzen-Berechnung nach §§ 25 bis 25 d des Zweiten Wohnungsbaugesetzes (WoBauG) ergibt.

Die Aufbewahrung der Akten beim Bezirksamt Eimsbüttel soll in den Stahlschränken erfolgen, die nach der Vernichtung der manuell geführten Wohnraumkartei frei werden.

Im Hinblick auf die Neuregelung der Fachlichen Weisung W3/83 über die Versorgung von vordringlich Wohnungssuchenden mit Wohnraum ist zu berichten, daß ein interner Entwurf bei der Baubehörde bis zum Jahresende fertiggestellt sein soll. Eine Entwurfsfassung soll uns zugeleitet werden.

Über die Ergebisse der Arbeitsgruppe und die Neuregelung der Fachlichen Weisung werden wir weiter berichten.

13. Meldewesen

13.1 Neuentwicklung des automatisierten Melderegisters

Nach unserer Kritik an der wachsenden Unzuverlässigkeit des Melderegisters im 11. TB (13.2) ist im Senatsamt für Bezirksangelegenheiten ein Projekt zur Neuentwicklung des IuK-Verfahrens Meldewesen („MEWES") eingerichtet worden.

Die vorliegende Informations- und Funktionsstrukturanalyse macht deutlich, daß die zukünftige Datenbank des Melderegisters nur jeweils einen logischen Personendatensatz zu einem Einwohner enthalten wird. Wenn z.B. ein Bürger umzieht, muß nur bei einem Datensatz die neue Adresse erfaßt werden. Aufgrund der relationalen Datenbankstruktur wirkt sich die Fortschreibung auf andere Eintragungen aus, die mit dem geänderten Datensatz in Beziehung stehen. Es ist dann nicht mehr nötig, wie bisher festzustellen, ob und mit welchen Beziehungen die Person noch gespeichert ist, um jeweils Einzelfortschreibungen vorzunehmen. Damit entfallen insbesondere fehlerträchtige Mitteilungen zwischen einzelnen Meldedienststellen.

Diese Konzeption setzt voraus, daß jeder Sachbearbeiter jeden Datensatz fortschreiben kann. Hierbei ist zu berücksichtigen, daß es sich lediglich um datenbankinterne Auswirkungen der Änderung eines Datensatzes handelt. Im Ergebnis erfolgen weniger Zugriffe auf die Datenbank, da nicht mehr unterschiedliche örtliche Meldedienststellen aus einem Anlaß mehrere getrennte Datensätze fortschreiben müssen.

Wir haben deutlich gemacht, daß diese Konzeption datenschutzrechtlich vorteilhaft ist, da hierdurch das bisherige Problem der mehrfachen und nicht eindeutigen Datensätze vermieden wird (vgl. 12. TB, 13.1.2).

13.2 Novellierung des Hamburgischen Meldegesetzes

Die neue Konzeption für das automatisierte Melderegister setzt voraus, daß die bisherige örtliche Bindung im Hamburgischen Meldegesetz (HmbMG) für die Folgeänderungen aus der Fortschreibung eines Datensatzes aufgegeben wird. Insofern müßte das Gesetz den rechtlichen Rahmen für die technische Änderung erweitern.

Von diesen datenverabeitungstechnischen Rahmenbedingungen zu trennen ist allerdings die Frage, ob die bisherige örtliche Zuständigkeit der Meldebehörden für die Entgegennahme von An- und Abmeldungen der Bürger aufgegeben werden soll (vgl. 10. TB, 13.1.1). Die oben beschriebene neue technische Konzeption läßt sich auch verwirklichen, wenn die bisherige fachliche Zuständigkeitsbegrenzung auf den örtlichen Einzugsbereich der Meldedienststellen beibehalten wird.

Ob die Absicht des Entwurfs für die Novellierung des HmbMG zur Aufgabe der bisherigen örtlichen Zuständigkeitsgrenzen tatsächlich zum Tragen kommt, ist nach wie vor offen. Der Senat hat sich noch nicht mit dem Entwurf befaßt.

Aus unserer Sicht ist daran festzuhalten, daß das Modell der überörtlichen Zuständigkeit der Meldebehörden nur dann verwirklicht werden sollte, wenn die Erwartung, dies liege im Interesse der Bürger, tatsächlich berechtigt ist. Wir haben deshalb vorgeschlagen, durch eine Umfrage in ausgewählten Meldebehörden zu ermitteln, ob eine nennenswerte Zahl von Bürgern lieber ein anderes Orts- oder Bezirksamt aufsuchen würde, um ihrer Meldepflicht nachzukommen, und ob der dadurch entstehende veränderte Publikumsverkehr in den Dienststellen ohne Probleme zu bewältigen wäre. Nur wenn dies der Fall ist, überwiegen die Interessen der Allgemeinheit gegenüber den Vorkehrungen zum Schutz der Daten, den die örtlich begrenzten Zugriffsrechte bisher gewährleistet haben.

13.3 Probleme mit melderechtlichen Auskunftssperren

13.3.1 Praxis beim Umgang der Behörden mit gesperrten Anschriften

Wenn Frauen eines der Hamburger Frauenhäuser beziehen, um der Gewaltanwendung durch ihre Ehemänner zu entgehen, ist dafür zu sorgen, daß ihr neuer Aufenthaltsort nicht offenbart wird. Im Melderegister sind daher die Adressen sämtlicher Frauenhäuser gesperrt, das heißt, die Meldebehörde verweigert Auskünfte an private Anfragende.

Eines der Frauenhäuser erkundigte sich, ob diese Auskunftssperre im Melderegister ausreicht. Es wurde die Gefahr gesehen, daß andere Behörden, die über die Anschriften der Bewohnerinnen von Frauenhäusern verfügen, diese in Unkenntnis des Sachverhalts herausgeben.

Dieses Problem ist für sämtliche Auskunftssperren nach § 34 Abs. 5 bis 7 des Hamburgischen Meldegesetzes (HmbMG) von Bedeutung, die wegen Gefährdung oder überwiegenden Interessen der Betroffenen von Amts wegen oder auf Antrag eingerichtet werden. Wir sind deshalb der Frage nachgegangen, wie die Stellen, die von der Meldebehörde über die Auskunftsperren unterrichtet werden, hiermit umgehen. Das für IuK-Angelegenheiten zuständige Amt 6 der Finanzbehörde hat dazu eine Behördenumfrage durchgeführt und uns die Antworten zusammengefaßt mitgeteilt. Aufgrund dieser Auswertung und weiterer Erfahrungen haben wir folgende Hinweise gegeben, durch welche Vorkehrungen die Geheimhaltung gesperrter Adressen durch die datenempfangenden Stellen gewährleistet werden kann:

Auskunftsperren nach dem Meldegesetz verhindern grundsätzlich nicht, daß die gesperrten Daten von der Meldebehörde an andere öffentliche Stellen übermittelt werden. Um zu vermeiden, daß die melderechtlichen Auskunftssperren von den datenempfangenden Stellen im Einzelfall übersehen werden, ist als wichtigster Grundsatz festzuhalten, daß nur die Meldebehörde Adreßauskünfte erteilt. Anfragen bei anderen Stellen nach der Anschrift eines Betroffenen sind daher stets an die zuständige Meldebehörde zu verweisen; dies gilt auch dann, wenn im Übrigen die Voraussetzungen für eine Datenübermittlung vorliegen. Die Mehrheit der Behörden und Ämter, die auf die Umfrage geantwortet haben, verfährt auch so.

Bei Übermittlungen aus dem Melderegister an andere öffentliche Stellen wird grundsätzlich die Tatsache, daß eine Auskunftsperre vorliegt, kenntlich gemacht. Dies gilt bei Einzelanfragen ebenso wie bei regelmäßigen Übermittlungen nach den entsprechenden Vorschriften der Meldedatenübermittlungsverordnung oder bei automatisierten Abrufen aus dem Melderegister nach der jeweiligen Rechtsverordnung.

Sofern Daten aus dem Melderegister durch automatisierte Abgleiche übernommen werden, ist darauf zu achten, daß die Tatsache der Auskunftssperre im automatisierten Verfahren der datenempfangenden Stelle erkennbar bleibt. Ist dies aus technischen Gründen nicht möglich, sind gesperrte Meldedaten von der automatisierten Übernahme auszuschließen und gesondert konventionell zu übermitteln (so verfährt z.B. die Bußgeldstelle).

Die besondere Kennzeichnung von Auskunftssperren bei Übermittlungen aus dem Melderegister hat den Zweck, die datenempfangenden Stellen darauf aufmerksam zu machen, daß bei der weiteren Verarbeitung der Daten geeignete Vorkehrungen zu treffen sind, um die Offenbarung der gesperrten Daten zu vermeiden. Derartige Vorkehrungen sind vor allem dann notwendig, wenn aufgrund besonderer Vorschriften Akteneinsichtnahmen durch Dritte in Betracht kommen (z.B. Ermittlungsakten in Straf- und Bußgeldsachen).

Als geeignete Verfahrensweise zur Sicherung von Auskunftssperren ist die von der Ausländerbehörde und den Sozialämtern geschilderte Praxis anzusehen: Akten mit gesperrten Daten werden gesondert gekennzeichnet bzw. getrennt aufbewahrt; vor der Gewährung von Akteneinsicht bzw. der Versendung der Akten werden diejenigen Blätter, aus denen die Anschrift hervorgeht, entweder entfernt oder es werden Kopien angefertigt, auf denen die Anschrift gelöscht ist.

Ähnlich verfährt das Familiengericht. Insbesondere in Scheidungsverfahren kommt der Geheimhaltung der Anschrift von Frauen, die durch ihre früheren Ehemänner bedroht werden, besondere Bedeutung zu. Es wäre höchst widersprüchlich, wenn aus dem Scheidungsurteil die neue Anschrift ersichtlich wäre, worauf die Bedrohung fortgesetzt werden könnte. Daher hat sich bei den Familiengerichten folgende Praxis entwickelt: Die Prozeßbevollmächtigten der Antragstellerinnen teilen überhaupt keine Anschriften mit oder nur, daß sich die Mandantin in einem Frauenhaus aufhält. In diesen Fällen werden Zustellungen nur über den Anwalt vorgenommen. Wenn so verfahren wird, ist die Angabe der Anschrift im Rubrum des Urteils entbehrlich.

Der Präsident des Amtsgerichts hat allerdings darauf hingewiesen, daß ein Verzicht auf die Anschriftenangabe nicht dazu führen darf, daß Verfahrensrechte der anderen Partei verkürzt werden oder das Grundrecht auf rechtliches Gehör verletzt wird. Nach der Rechtsprechung des Bundesgerichtshofes kann ein überwiegendes Geheimhaltungsinteresse der Bekanntgabe der Anschrift entgegenstehen. Dann müssen dem Gericht aber wenigstens die maßgeblichen Gründe für dieses überwiegende Interesse mitgeteilt werden, damit es die jeweiligen Rechtspositionen gegeneinander abwägen kann.

Da es bei dieser Verfahrensweise insbesondere auch auf die Kooperation der Anwälte ankommt, haben wir die Hanseatische Rechtsanwaltskammer auf diese Grundsätze hingewiesen.

13.3.2 Auskunftsperren bei Namensänderungen

In besonderen Fällen bezweckt eine Auskunftssperre nicht den Schutz der aktuellen Anschrift, sondern früherer Namensangaben. Dies gilt nach § 31 Abs. 7 HmbMG insbesondere bei Namensänderungen aufgrund einer Adoption (frühere Nachnamen) und nach dem Transsexuellengesetz (frühere Vornamen). In diesen Fällen ist es erforderlich, die Tatsache der Auskunftsperre bei Übermittlungen aus dem Melderegister gesondert zu kennzeichnen, wenn mit den früheren und jetzt gesperrten Namensangaben angefragt wird oder diese gesperrten Angaben aus dem Melderegister übermittelt werden. Letzteres kommt nur dann in Betracht, wenn im Einzelfall die Kenntnis der früheren Namen zur Aufgabenerfüllung erforderlich ist.

Bei Übermittlungen aus Anlaß der Namensänderung ist der Hinweis auf die Auskunftssperre immer dann erforderlich, wenn die datenempfangende Stelle die alte Namensangabe nicht vollständig löscht und durch die neue ersetzt, sondern aus fachlichen Gründen zulässigerweise in Dateien oder Akten weiterführt. Dann sind geeignete Vorkehrungen zu treffen, die eine Verwendung des früheren Namens gegenüber Dritten (öffentlichen wie nicht-öffentlichen Stellen) verhindern.

13.3.3 Namensänderungen besonders gefährdeter Personen

Das Gesetz über die Änderung von Familiennamen und Vornamen sieht die öffentlich-rechtliche Namensänderung auf Antrag vor, wenn ein wichtiger Grund die Änderung rechtfertigt.

Die Mehrzahl dieser Namensänderungen betrifft Aussiedler, die ins Bundesgebiet eingereist sind. Diese Namensänderungen werfen nach unserer bisherigen Kenntnis keine besonderen datenschutzrechtlichen Probleme auf. Daneben gibt es jedoch Einzelfälle (in Hamburg zwischen 10 und 20), in denen die Namensänderung erfolgt, um akute Bedrohungen für Leib und Leben der Betroffenen zu vermeiden. Derartige Namensänderungen wegen besonderer Bedrohung erfolgen überwiegend zum Zeugenschutz auf Veranlassung der Polizei. In einigen wenigen Fällen beruht die Namensänderung auf eigener Initiative der Betroffenen.

Im Frühjahr 1994 wurde uns ein Fall geschildert, der die Risiken bei dieser Personengruppe leider anschaulich deutlich gemacht hat. Die betroffene Frau hatte die Namensänderung vorgenommen, weil sie von ihrem früheren Ehemann akut bedroht wird und insbesondere die Gefahr besteht, daß versucht wird, den Sohn ins Ausland zu entführen. Der frühere Ehemann hatte sich nunmehr an eine Polizeidienststelle außerhalb Hamburgs gewandt mit der Angabe, die Ehefrau sei vermißt. Im Zuge der polizeilichen Vermißtensuche erfolgte unter dem früheren Namen und dem Geburtsdatum der Betroffenen eine Anfrage bei der Meldebehörde. Diese wurde gegenüber der Polizeidienststelle gemäß dem Hamburgischen Meldegesetz mit dem neuen Namen und der Anschrift unter Hinweis auf die bestehende Auskunftsperre beantwortet. Die Meldebehörde konnte nicht wissen, daß die Vermißtenmeldung nur fingiert war, um auf diesem Weg den Aufenthaltsort der Ehefrau ausfindig zu machen. Sie hatte daher keine Veranlassung, die Übermittlung der Daten an die anfragende Polizeidienststelle zu verweigern.

Der Fall macht deutlich, daß auch Auskunftsperren bei derartigen besonderen Gefährdungen keinen ausreichenden Schutz gewähren. Insbesondere wenn aufgrund einer Melderegisterabfrage mit früherem Namen und Geburtsdatum der neue Name und die Anschrift automatisch angezeigt werden, ist der durch den Vermerk über die Auskunftssperre erreichte Schutz unzureichend. Abfragenden Stellen wird dann aufgrund der leichten Zugänglichkeit der Daten die besondere Fallgestaltung nicht hinreichend deutlich.

Grundsätzlich trifft die Meldebehörde daher bei Namensänderungen wegen besonderer Gefährdung spezielle Vorkehrungen, die jeden Verweis vom früheren auf den jetzigen Namen ausschließt, Direktabfragen verhindert und die Weiterleitung von Anfragen an besonders instruierte Mitarbeiter der Meldebehörde vorsieht. Diese Verfahrensweise setzt allerdings voraus, daß die Meldebehörde Kenntnis davon erhält, daß die Namensänderung zum besonderen Schutz vorgenommen wurde, da angesichts der Vielzahl von „normalen" Namensänderungen, z.B. bei Aussiedlern, die bloße Tatsache der amtlichen Namensänderung nichts über die besondere Gefährdung aussagt.

Dieser besondere Hinweis an die Meldebehörde war im geschilderten Fall unterblieben und daher die spezielle Auskunftssperre nicht eingetragen. Inzwischen ist durch eine geeignete Verfahrensweise sichergestellt, daß derartige Pannen nicht mehr vorkommen.

Wir haben vorgeschlagen, daß die Meldebehörde bei Anfragen öffentlicher Stellen zu dieser Personengruppe folgende Grundsätze beachtet:

— keine Übermittlungen aufgrund mündlicher Anfragen,

— bei schriftlichen Anfragen Bestätigung der Erforderlichkeit durch die vorgesetzte Dienststelle verlangen,

— Unterrichtung der zuständigen Polizeidienststelle (insbesondere beim Zeugenschutz),

— in Zweifelsfällen Ablehnung der Übermittlung nach § 6 HmbMG.

Auch wenn durch die Einhaltung dieser Grundsätze die Ausforschung des neuen Namens und der Anschrift aus dem Melderegister verhindert werden kann, sind damit nicht alle Probleme gelöst.

Weitere Probleme ergeben sich aus den Verfahrensregelungen zu dem Namensänderungsgesetz. Wir verzichten an dieser Stelle auf deren Schilderung im Detail, um keine „Gebrauchsanweisung" zur Ausforschung zu geben. Aufgrund unserer Initiative ist die Problematik inzwischen auch in den für das Gesetz zuständigen Bund-/Ländergremien erörtert worden. Allerdings waren bei Redaktionsschluß dieses Berichts noch keine Ergebnisse bekannt.

14. Standesamt

14.1 Prüfung des Projekts Automation Standesämter (PASTA)

Eine im Dezember 1993 durchgeführte erneute Prüfung der Datenverarbeitung im Bereich der Standesämter hat ergeben, daß seit der ersten Prüfung im Oktober 1992 – entgegen der Ankündigung des Senats in seiner Stellungnah-

me zum 11. Tätigkeitsbericht zu 14. – keine wesentlichen Verbesserungen im Hinblick auf die Gewährleistung des Datenschutzes beim Projekt Automation Standesämter (PASTA) realisiert wurden.

Der Senat hatte in seiner Stellungnahme zu unserer Darstellung von Datenschutzmängeln im Standesamt des Bezirksamts Hamburg-Mitte (11. TB, 14.) mitgeteilt, er habe die von uns erkannte Lücke zum Anlaß genommen, die Zugriffsmöglichkeiten durch eine Änderung des Verfahrens weiter zu beschränken. Das neue Verfahren befinde sich bei einem Standesamt im Probebetrieb und solle nach erfolgreichem Abschluß in allen Standesämtern eingesetzt werden. Ferner hatte der Senat angekündigt, die als Entwürfe vorliegenden Dienstanweisungen für Systemverwalter und Benutzer unter Berücksichtigung der praktischen Erfahrungen zu überarbeiten und als Dienstanweisung des Senatsamts für Bezirksangelegenheiten zu erlassen.

Unsere Nachprüfung beim Bezirksamt Hamburg-Wandsbek hat ergeben, daß trotz Programmodifikation die Systemsicherheit bei PASTA noch nicht gewährleistet war und erhebliche Sicherheitslücken vorhanden waren.

Eine wesentliche Programmänderung zur Beschränkung der Zugriffsmöglichkeiten bestand darin, daß der Zugriff auf das Netzlaufwerk verhindert werden sollte. Dort sind u.a. die Daten des Programms AUTISTA, mit dessen Hilfe z.B. Beurkundungen von Geburten, Eheschließungen und Todesfälle wahrgenommen werden können, gespeichert. Der Zugriff wurde durch eine beim Start automatisch aufgerufene Batchdatei unterbunden. Diese Maßnahme ließ sich – wie das gesamte Sicherheitssystem – von jedem einigermaßen kundigen Benutzer mit einem Editor umgehen, so daß der Benutzer des Systems beim nächsten Start ohne Paßwortabfrage auf Betriebssystemebene gelangen und dort uneingeschränkt auf sämtliche im Netz vorhandenen Dateien zugreifen konnte.

Die zentrale Sicherheitslücke war weiterhin in dem integrierten Softwarepaket F&A zu sehen, dessen Betriebssystemausgang praktisch nicht abgeschaltet werden konnte. Ferner ermöglichte es F&A jedem Benutzer, eigene Dateien anzulegen und zu verwalten. Wie bei der ersten Prüfung von 1992 war auch beim Standesamt Wandsbek von dieser Möglichkeit Gebrauch gemacht worden. Diese Dateien wurden nach neuer Softwareeinspielung gelöscht.

Auch die angekündigte verbindliche Dienstanweisung für die Systemverwalter und Benutzer war zum Zeitpunkt unserer Prüfung noch nicht erlassen.

Als Konsequenz aus der vorgenommenen Nachprüfung wurden datenschutztechnische Nachbesserungen durch das Senatsamt für den Verwaltungsdienst vorgenommen, die durch uns im Januar 1994 beim Standesamt Altona überprüft wurden. Obwohl wesentliche Verbesserungen erzielt wurden, war das Gesamtergebnis der Verfahrenssicherheit von PASTA noch nicht befriedigend, so daß weitere Programmänderungen erforderlich wurden. Die Nachprüfung der Verfahrenssicherheit von PASTA im März 1994 beim Standesamt Barmbek-Uhlenhorst hat ergeben, daß die bei den vorhergehenden Prüfungen noch vorhandenen Sicherheitslücken nunmehr geschlossen sind.

Auch die angekündigte Dienstanweisung für die Systemverwalter und Benutzer ist im Juli 1994 in Kraft gesetzt worden.

15. Ausländerangelegenheiten

15.1 Automation der Ausländerverwaltung

Das Projekt „Automation des Ausländer- und Asylwesens" (PAULA) stand bei Redaktionsschluß dieses Berichts vor seinem Abschluß: Die Einführung des neuen automatisierten Verfahrens in der Ausländerbehörde ist in mehreren Phasen zwischen Ende November 1994 und Anfang Januar 1995 vorgesehen. Eine umfassende datenschutzrechtliche Prüfung war daher noch nicht möglich.

Der im 12. TB (15.1) beschriebene Test der Übernahme des Grunddatenbestandes hat gezeigt, daß die geplante Erstdatenerfassung durch einen Abgleich zwischen Melderegister und Ausländerzentralregister (AZR) nicht möglich ist.

Grund hierfür ist die Unzuverlässigkeit des im AZR gespeicherten Bestandes. Aufgrund der Tests hat die Projektgruppe geschätzt, daß die Datenübernahme in 30 bis 40 % der Fälle fehlerhaft wäre. Das heißt, bei Einführung des neuen Verfahrens wären die Grunddaten von bis zu 100 000 im Zuständigkeitsbereich der Behörde lebenden Ausländern zumindest höchst unvollständig oder sogar falsch gewesen.

Es bestand auch keine Aussicht, diese Fehler bei der Verfahrenseinführung zu bereinigen. Stattdessen hat die Lenkungsgruppe des Projekts mit unserer Zustimmung entschieden, auf die Erstdatenübernahme aus dem AZR zu verzichten. Vielmehr sollen die Daten bei Bedarf, z.B. wenn die Betroffenen vorsprechen, anhand ihrer Unterlagen, der Akten und Anfragen beim AZR überprüft und erforderlichenfalls berichtigt werden. Hierbei soll dann auch die Berichtigung des AZR erfolgen (vgl. unten 15.2. 2).

Auf diese Weise wird bei den mit PAULA arbeitenden Mitarbeitern der falsche Eindruck vermieden, sie könnten sich auf das verlassen, was im Verfahren gespeichert ist. Vielmehr werden sie angehalten, die Daten in PAULA wie im AZR anlaßabhängig zu pflegen.

15.2 Gesetz über das Ausländerzentralregister

15.2.1 Gesetzliche Schlechterstellung von Ausländern

Kurz vor Ende der 12. Legislaturperiode des Deutschen Bundestages ist das Gesetz über das Ausländerzentralregister (AZRG) verabschiedet worden und

am 1. Oktober 1994 in Kraft getreten. Damit wurde nach einer über zehnjährigen Diskussion um die Ausgestaltung dieses Registers, das bisher ohne normenklare Rechtsgrundlage geführt wurde, ein vorläufiger Schlußpunkt gesetzt. Festzustellen ist, daß die Verabschiedung des Gesetzes diese Diskussion zum Nachteil der Betroffenen und des Datenschutzes beendet hat.

Das Ausländerzentralregister (AZR) wird beim Bundesverwaltungsamt in Köln geführt. In ihm sind sämtliche Ausländer, die sich in der Bundesrepublik Deutschland nicht nur vorübergehend aufhalten, erfaßt. Auch über Ausländer, die Deutschland verlassen haben, werden noch zehn Jahre lang Daten gespeichert.

Bereits in den ersten Stellungnahmen des Hamburgischen Datenschutzbeauftragten zum AZR im Jahr 1984 (3. TB , 3.7.3.5 f.) war die Problematik angesprochen worden, daß dieses Register – neben Hinweisen auf die jeweils zuständige und aktenführende Ausländerbehörde (sogenannte Indexfunktion) – auch die Aufgabe erhalten sollte, Entscheidungen durch Direktabruf sofort ohne Heranziehung der Akten treffen zu können (sogenannte Substitutionsfunktion). Während eine Beschränkung des AZR auf die Indexfunktion datenschutzrechtlich akzeptabel wäre, entsteht durch die Substitutionsfunktion die Gefahr, daß aufgrund unrichtiger oder unvollständiger Registereintragungen Fehlentscheidungen zu Lasten der Betroffenen erfolgen.

Derartige unrichtige oder unvollständige Registereintragungen enthält das AZR nach den Schätzungen der Ausländerbehörde in Hamburg in 30 bis 40 % der Fälle (siehe oben 15.1). Ein Polizeibeamter, der aufgrund einer ergebnislosen Abfrage im AZR davon ausgeht, der Betroffene halte sich illegal hier auf, geht das erhebliche Risiko ein, einen Unschuldigen zu verfolgen, da auf das Schweigen des Registers sich niemand verlassen kann. Auch Eintragungen im AZR sind in vielen Fällen nicht zuverlässig.

Ungeachtet dieser Gefahren hat der Gesetzgeber den Kreis der Stellen, die sich mit Direktzugriffen des Registerinhalts für Sofortmaßnahmen bedienen können, erheblich ausgeweitet: In Zukunft sollen neben den Ausländer- und Asylbehörden, den Polizei- und Grenzschutzdienststellen sowie dem Bundesverwaltungsamt auch die Staatsanwaltschaften, das Zollkriminalamt, die Bundesanstalt für Arbeit, die Hauptzollämter, die Verfassungschutzbehörden des Bundes und der Länder, der militärische Abschirmdienst (MAD) und der Bundesnachrichtendienst (BND) im automatisierten Verfahren Daten aus dem AZR abrufen können.

Die Bedeutung dieser massiven Ausdehnung der Zugriffsberechtigungen anderer Stellen wird dann sichtbar, wenn man berücksichtigt, daß in Zukunft im AZR nicht nur ausländerrechtliche Sachverhalte gespeichert werden, sondern insbesondere auch polizeiliche und nachrichtendienstliche Angaben.

Vorgesehen ist zum einen die Speicherung von Daten über die polizeiliche Fahndung und die Grenzfahndung. Die hierfür zuständigen Polizei- und Grenzschutzdienststellen verfügen allerdings unabhängig vom AZR aufgrund des INPOL-Systems über sämtliche Fahndungsdaten, und zwar unabhängig von der Staatsangehörigkeit der Personen, nach denen gefahndet wird. Der im AZR zu speichernde Fahndungsbestand soll aus INPOL überspielt werden. Ferner werden Fahndungsdaten im Schengener Informationssystem (SIS) gespeichert, auf das die Polizeien und der Grenzschutz ebenfalls Zugriff haben werden. Also bestehen für Ausländer mindestens drei weitgehend identische Fahndungsdateien: INPOL, AZR und Schengener Informationssystem. Der Zweck der Speicherung von Fahndungsdaten im AZR besteht allein darin, auch Behörden, die für Fahndungsaufgaben nicht zuständig sind, an diesen polizeilichen Erkenntnissen teilhaben zu lassen. Während die für die Polizei geltenden Bestimmungen einen Direktzugriff anderer Behörden auf polizeiliche Daten verbieten, schreibt das AZRG diesen Direktzugriff unmittelbar vor.

Noch problematischer ist die in § 2 Abs. 2 Nr. 7 AZRG vorgesehene Speicherung von Verdachtsdaten. Sie ist möglich, wenn zureichende tatsächliche Anhaltspunkte für den Verdacht auf verbotene ausländische Vereinigungen, Rauschgifthandel, kriminelle und terroristische Vereinigungen bestehen. Auch in diesen Fällen verfügt die Polizei aufgrund des INPOL-Systems über alle erforderlichen Daten unabhängig von der Staatsangehörigkeit, benötigt also den Zugriff auf diese Daten im AZR zu eigenen Zwecken nicht. Die Speicherung dieser Verdachtsdaten im AZR dient vielmehr nur der Verdoppelung, um Zugriffe anderer Stellen zu ermöglichen, die keinen Zugang zu polizeilichen Dateien haben.

Die Verdachtsdaten werden jedoch nicht allein aus dem polizeilichen Informationssystem übernommen, sondern auch von den Verfassungsschutzbehörden eingespeist. Damit schafft das AZR einen Datenverbund zwischen Verfassungsschutzbehörden und Polizeien, der nach § 6 Satz 4 Bundesverfassungsschutzgesetz für das nachrichtendienstliche Informationssystem ausgeschlossen ist.

Auch die gesetzliche Zulassung von automatisierten Abrufen durch die Verfassungsschutzbehörden, den militärischen Abschirmdienst und den Bundesnachrichtendienst im AZRG führt zu Sonderbefugnissen zulasten von Ausländern. Bei der Novellierung des Bundesverfassungsschutzgesetzes im Jahre 1990 ist erwogen worden, ob befristete Online-Zugriffe des Verfassungsschutzes auf andere Datenbestände zugelassen werden sollten. Im damaligen Gesetzgebungsverfahren ist dies schließlich verworfen worden. Nunmehr werden im AZRG automatisierte Abrufverfahren sämtlicher Nachrichtendienste ohne jede Befristung zugelassen. Der Bundesnachrichtendienst hat nach dem BND-Gesetz zu Recht keine Befugnis zur konventionellen Registereinsicht im Inland, nach dem AZRG kann er sich problemlos im Direktabrufverfahren sämt-

liche Grunddaten von in Deutschland lebenden oder früher hier anwesenden Ausländern besorgen.

Hamburg hat im Bundesrat auf unseren Vorschlag die Streichung dieser Regelungen über polizeiliche Speicherungen im AZR und den Direktzugriff der Nachrichtendienste beantragt, ist hiermit allerdings erfolglos geblieben.

Eine weitere nur für Ausländer geltende Benachteiligung tritt durch die Regelung über Suchvermerke und Gruppenauskünfte ein. Im AZR können in Zukunft Suchvermerke anderer Behörden einschließlich der Nachrichtendienste über sämtliche Ausländer eingetragen werden. Derartige Suchvermerke, die zur sofortigen Benachrichtigung der Stellen führen, die sie eingegeben haben, können zwar auch im Bundeszentralregister gespeichert werden. Dort betreffen sie aber Deutsche und Ausländer gleichermaßen. An das Bundeszentralregister sind auch nicht vergleichbar viele Behörden online angeschlossen.

Wenn eine Strafverfolgungsbehörde zur Verfolgung schwerer Straftaten über Deutsche eine nach bestimmten Anfragekriterien zusammengestellte Auswertung aus einer automatisierten Datei haben möchte, die zum Abgleich mit anderen Dateien verwendet werden soll (Rasterfahndung), benötigt sie hierzu gemäß § 98 b StPO einen richterlichen Beschluß. § 12 Abs. 1 Nr. 2 AZRG läßt sogenannte Gruppenauskünfte über Ausländer zu Zwecken der Gefahrenabwehr oder Strafverfolgung ohne richterliche Anordnung zu. Mit bestimmten Anfragekriterien (z.B. alle Personen mit bestimmter Staatsangehörigkeit, die in einem bestimmten Zeitraum eingereist sind oder sich in bestimmten Gebieten aufhalten) erhält die ersuchende Polizei oder Staatsanwaltschaft damit faktisch schon das Ergebnis einer Rasterfahndung. Wenn derartige Auswertungen auch noch auf elektronischen Datenträgern übermittelt würden, stünde weiteren Abgleichen nichts mehr im Wege, auch wenn die gesetzlichen Voraussetzungen nach §§ 98a und b StPO nicht vorliegen. § 12 Abs. 1 Nr. 3 AZRG läßt sogar Gruppenauskünfte an den BND zu, um im Ausland die Gefahr der unbefugten Verbringung von Betäubungsmitteln in das Gebiet der Bundesrepublik Deutschland zu erkennen, obwohl dies nicht zu den Aufgaben des Bundesnachrichtendienstes nach dem BND-Gesetz gehört (siehe hierzu unten 18.4).

Lediglich die Daten von Personen mit Aufenthaltsberechtigung oder unbefristeter Aufenthaltserlaubnis sind von diesen Regelungen über erleichterte Rasterfahndungen gegen Ausländer nicht betroffen. Glücklicherweise hat sich Hamburg im Bundesrat nicht durchgesetzt mit seinem Antrag zur Streichung dieser Einschränkung, gegen den wir uns entschieden gewandt haben.

Die Summierung all dieser nur Ausländer betreffenden Sonderregelungen, die insgesamt zu einem empfindlichen Defizit beim Schutz personenbezogener Daten führen, weckt erhebliche Zweifel, ob diese Vorschriften mit dem auch für Ausländer geltenden Grundrecht auf Datenschutz nach Art. 1 Abs. 1 und Art. 2 Abs. 1 Grundgesetz und dem Gleichheitsgrundsatz nach Art. 3 Grundgesetz

vereinbar sind. Es bleibt abzuwarten, ob die neuen Regelungen bei einer etwaigen Verfassungsbeschwerde eines Betroffenen vor dem Bundesverfassungsgericht Bestand haben werden.

15.2.2 Datenschutzrechtliche Handlungsmöglichkeiten

Angesichts der weitreichenden gesetzlichen Eingriffe wird es in Zukunft darauf ankommen, die verbleibenden Handlungsmöglichkeiten zum Schutz personenbezogener Daten, die im AZR gespeichert sind, wahrzunehmen. Hierzu gehören insbesondere die Datenpflege zur Gewährleistung der Richtigkeit des Registerinhalts, Übermittlungssperren, die Beteiligung der Betroffenen bei Übermittlungen ins Ausland und an Private sowie die Datenschutzkontrolle. Erste Ansätze hierzu bieten Verfahrensregelungen des Gesetzes und der Entwurf für eine Durchführungsverordnung zum AZRG (AZRG-DV), zu dem wir Verbesserungsvorschläge eingebracht haben.

— Datenpflege

Im AZRG wird die Verantwortung für die Zulässigkeit und Richtigkeit der gespeicherten Daten zutreffend den Stellen zugewiesen, die Daten an das AZR anliefern. Dies sind in erster Linie die Ausländerbehörden. Sie haben in Zukunft die Möglichkeit, Fortschreibungen und Berichtigungen durch Direkteingaben in das Register vorzunehmen. Insbesondere mit dieser Regelung wird die Erwartung verbunden, daß sich die Zuverlässigkeit des AZR verbessert. Die Ausländerbehörde Hamburg wird daher das von ihr im Grundsatz erkannte Problem der massenhaften unrichtigen und unvollständigen Speicherungen im AZR sukzessive nach Kräften abarbeiten müssen, um den derzeitigen gesetzeswidrigen Zustand zu bereinigen.

Sofern andere Stellen – insbesondere die Polizei – bei Direktabrufen Unrichtigkeiten feststellen, sind sie gehalten, die zuständige Ausländerbehörde zu informieren, damit diese die notwendige Sachaufklärung und Berichtigung vornehmen kann. Zu begrüßen ist ferner, daß die Registerbehörde zusätzlich zu den datenanliefernden Stellen nach der AZRG-DV Hinweise auf eine mögliche Unrichtigkeit prüfen soll und Vorkehrungen zu treffen hat, die Fehlspeicherungen verhindern.

Nach dem bisher in der AZRG-DV vorgesehenen Datensatz werden nur die ausländerbehördlichen Entscheidungen, z.B. der Widerruf einer Aufenthaltsgenehmigung eingetragen, nicht jedoch, ob diese Entscheidung u.U. gerichtlich angefochten ist. Diese Informationen wären jedoch für die Aussagekraft des Registers wesentlich. Dies gilt insbesondere dann, wenn bei der Registerbehörde auch Begründungstexte gespeichert werden. Dann ist die Gefahr hoch, daß die nicht fachlich zuständige Registerbehörde in Einzelfällen nur überholte Begründungstexte, die gerichtlich aufgehoben sind, kennt und für Informationen an andere Stellen benutzt. Wir haben daher ge-

fordert, daß nur bestands- oder rechtskräftige Begründungstexte an das AZR gesandt werden.

— Übermittlungssperren

Das AZRG sieht die Speicherung von Übermittlungssperren auf Antrag des Betroffenen oder von Amts wegen vor. Sie verhindern Datenübermittlungen an Private oder ins Ausland, wenn hierdurch schutzwürdige Interessen beeinträchtigt würden. Bei besonderem öffentlichen Interesse sind auch Übermittlungssperren gegenüber Behörden möglich. In der Praxis werden Übermittlungssperren vor allem dann relevant werden, wenn auch melderechtliche Auskunftssperren vorliegen (siehe hierzu oben 13.3).

Voraussetzung für die Übernahme der melderechtlichen Auskunftssperren in das AZR ist jedoch, daß die zuständige Ausländerbehörde oder das AZR direkt Kenntnis von der Eintragung einer solchen Sperre im Melderegister erhält. Dies ist nach den bisherigen Regelungen nicht gesichert. Die Behörde für Inneres hat dieses Defizit erkannt und hat beim Bundesministerium des Innern eine Änderung angeregt.

— Datenschutzkontrolle

Die Zulässigkeit von Speicherungen in und Abrufen aus dem AZR wird nur dann wirksam kontrolliert werden können, wenn auch die jeweiligen Protokolle über Eingaben und Abrufe zur Datenschutzkontrolle herangezogen werden können. Der Entwurf der AZRG-DV enthält hierzu noch keine eindeutige Regelung. Es wird nur auf den Bundesbeauftragten für den Datenschutz Bezug genommen, der für die Registerbehörde selbst und die beteiligten Stellen des Bundes zuständig ist.

Für die Kontrolle der Stellen in Hamburg, die Daten direkt eingeben und abrufen – also insbesondere die Ausländerbehörde und die Polizei – ist jedoch der Hamburgische Datenschutzbeauftragte zuständig. Wir haben daher eine Klarstellung nach dem Vorbild der für die Datenverarbeitung beim Kraftfahrtbundesamt maßgeblichen Fahrzeugregisterverordnung vorgeschlagen, die eindeutig vorsieht, daß die Registerbehörde die bei ihr gefertigten Protokolle jeweils den zuständigen Bundes- und Landesdatenschutzbeauftragten auf Anforderung zur Verfügung stellt.

16. Verkehrswesen

16.1 Automation in der Bußgeldstelle

16.1.1 Einführung des neuen automatisierten Verfahrens

Im Oktober 1994 ist in der Bußgeldstelle des Einwohnerzentralamts ein neues automatisiertes System zur Bearbeitung von Verfahren wegen Ordnungswidrigkeiten im Straßenverkehr eingeführt worden. Das bisherige System „Owi-

HH" wurde durch „OPAL" abgelöst. Diese Kurzbezeichnung steht für: „Ordnungswidrigkeiten-Projekt-Abteilungsrechner-Lösung".

Die Bezeichnung hebt hervor, daß es sich nicht mehr um ein Großrechnerverfahren handelt, sondern UNIX-Abteilungsrechner benutzt werden. Von den sechs im Einwohnerzentralamt installierten Abteilungsrechnern wird einer für das Verfahren „OPAL", die übrigen für das Verfahren „PAULA" der Ausländerbehörde (15.1) benutzt. Das Verfahren „OPAL" ist im wesentlichen eine Übernahme des in Mannheim betriebenen Verfahrens „ORDWIN".

Die Umsetzung fachlicher Anforderungen zum Schutz personenbezogener Daten haben wir bei der Einführung geprüft. Sie sind im wesentlichen erfüllt. Klärungsbedürftig sind noch einige Detailfragen, auf die im folgenden jedoch nicht eingegangen werden soll.

16.1.2 Verarbeitung von Personendaten

„OPAL" ermöglicht die Bearbeitung von Ordnungswidrigkeitenfällen im Dialog. Anzeigen über Verkehrsordnungswidrigkeiten werden von den zuständigen Außendienstmitarbeitern der Polizei mit mobilen Datenerfassungsgeräten aufgenommen. Die gespeicherten Daten über Kraftfahrzeugkennzeichen, Art, Ort und Zeitpunkt der Ordnungswidrigkeiten werden automatisiert in „OPAL" übertragen. Schriftliche Anzeigen werden durch Datenerfassungskräfte gespeichert. Ferner besteht die Möglichkeit zur direkten Erfassung durch Mitarbeiter der polizeilichen Verkehrsstaffeln.

Die meisten dieser Anzeigen enthalten noch keine Angaben zu den für die Ordnungswidrigkeit verantwortlichen Personen, sondern nur die Kennzeichen der Kraftfahrzeuge. Die Halter der Fahrzeuge werden aus dem Zentralen Fahrzeugregister beim Kraftfahrtbundesamt ermittelt. Hierfür wird nach Erfassung der Daten in OPAL im Batch-Verfahren eine Datei erstellt, die automatisiert mit dem zentralen Fahrzeugregister abgeglichen wird. Der Datenträger mit den Personalien der Halter wird anschließend in „OPAL" eingelesen und ist dann für die Mitarbeiter der Bußgeldstelle verfügbar.

Auch die Adressen der Betroffenen mit Wohnsitz in Hamburg werden durch Abgleich einer im Batch-Verfahren erstellten Anfragedatei mit dem Melderegister ermittelt oder aktualisiert und dann in „OPAL" eingelesen. Bei Personen außerhalb Hamburgs wird mit Hilfe des Systems eine Papieranfrage erstellt. Diese Lösungen für die Datenübernahme aus anderen Verfahren sind zu begrüßen. Sie ermöglichen einerseits eine rationelle Ermittlung der erforderlichen Angaben im rechtlich zulässigen Umfang, vermeiden andererseits jedoch Direktzugriffe auf das Zentrale Fahrzeugregister oder das Melderegister. Insbesondere werden aufwendige technische und rechtliche Vorkehrungen vermieden, die bei Online-Abfagen aus anderen Dateien getroffen werden müssen, um mißbräuchliche Zugriffe zu verhindern. Noch 1992 waren Online-

Abfragen der Bußgeldstelle beim Melderegister geplant und durch Rechtsverordnung geregelt worden. Diese Verordnung über den automatisierten Abruf von Daten aus dem Melderegister durch die Bußgeldstelle ist nunmehr gegenstandslos und aufzuheben.

Die Personen werden von den Sachbearbeitern den jeweiligen erfaßten Taten zugeordnet und somit zu Betroffenen im Sinne des Ordnungswidrigkeitengesetzes (OwiG) erklärt. Neben den Betroffenen werden Personendaten über deren Vertreter (Anwälte, Erziehungsberechtigte, Vertretungsorgane bei Personenvereinigungen und juristischen Personen sowie sonstige Zustellungsbevollmächtigte) gespeichert. Zeugen und Anzeigenerstatter werden in eigenen Datenfeldern zum Tatbestand erfaßt. Als Personenzusatzinformationen werden die Beziehungen von Personen zu Kraftfahrzeugen (als Halter oder Führer) dargestellt.

Wenn sich im Zuge eines Verfahrens herausstellt, daß nicht die ursprünglich als Betroffener im Sinne des OwiG angesehene Person, sondern eine andere Verursacher der Ordnungswidrigkeit war, findet ein Betroffenenwechsel statt: Das Verfahren gegen den bisherigen Betroffenen wird eingestellt, der neue Betroffene wird der Tat zugeordnet. Der bisherige Betroffene wird nicht gelöscht, da erkennbar bleiben muß, daß gegen ihn ein inzwischen eingestelltes Verfahren geführt worden ist.

In den meisten Fällen von Verkehrsordnungswidrigkeiten sind Angaben über Zeugen, die den Sachverhalt als Mitarbeiter der Polizei festgestellt haben, erforderlich. Um die ständige Erfassung der jeweiligen Personalien zu ersparen, ist vorgesehen, daß die polizeilichen Zeugen nur ihre Dienstnummern eingeben. Anhand dieser Dienstnummern werden im Verfahren „OPAL" die erforderlichen Angaben zur Person (Name, Dienstrang und Dienststelle) ermittelt. Diese Angaben werden aus dem Verfahren „Personalplanungssystem der Polizei" (PPS) an „OPAL" übermittelt und in einer gesonderten Datei gespeichert. Durch automatisierten Abgleich anhand der Dienstnummern werden die entsprechenden Zeugendaten in die jeweiligen Dokumente der Bußgeldverfahren eingelesen. Diese Verfahrensweise ist gemäß § 11 Abs. 3 HmbDSG durch Dienstanweisung des Präses der Behörde für Inneres festgelegt.

Zugriff auf diese Datei hat nur die Leitstelle „OPAL", die Mitarbeiter der Bußgeldstelle können sie weder lesen noch ändern. Wir haben vorgeschlagen, aufgrund der praktischen Erfahrungen zu prüfen, ob in Zukunft regelmäßige automatisierte Aktualisierungen der Datei ausreichen, so daß auch Zugriffe der Leitstelle weitgehend entbehrlich werden.

Im Einwohnerzentralamt sind fast 100 Terminals dem Verfahren „OPAL" zugeordnet. Die Zugriffsrechte der Mitarbeiter sind entsprechend ihrer Aufgabenstellung abgestuft. Der Schreibdienst hat nur Zugang zur Texterfassung, nicht zu Verfahrensdaten. Datenerfassungskräfte haben begrenzten lesenden Zugriff auf Verfahrensdaten, Sachbearbeiter unbegrenzten lesenden und auf ihren Abschnitt begrenzten ändernden Zugriff. Nur die Abschnittsleiter können alle Verfahrensdaten unbegrenzt lesen und ändern. Eine Prüfung, ob diese Zugriffsdifferenzierung durch die erforderlichen technischen Maßnahmen gesichert ist, wurde von uns bis zum Abschluß der Einführungsphase zurückgestellt.

16.1.3 Ahndung von Mehrfachtätern

Ursprünglich waren für „OPAL" auch Funktionen vorgesehen, um sogenannte Mehrfachtäter zu erkennen und erforderlichenfalls besonders zu ahnden. Die Sachbearbeiter sollten immer dann, wenn mindestens drei noch nicht abgeschlossene Verfahren in OPAL gespeichert waren, diese laufenden Verfahren zur Entscheidung angeboten bekommen, ob z.B statt dreier einzelner Verwarngelder ein erhöhtes Bußgeld verhängt werden soll. Die Grundentscheidung hierüber war bereits 1992 getroffen und mit uns abgestimmt worden.

Die Funktionen zur Mehrfachtäterahndung sind jedoch nicht realisiert worden, da zunächst fachlich geklärt werden soll, welche Auswirkungen es hat, wenn eines der zur Mehrfachtäterahndung herangezogenen drei Verfahren wegfällt, etwa weil der Vorwurf gegen den Betroffenen nicht zu belegen ist. In diesen Fällen könnte die Ahndung als Mehrfachtäter bei nur zwei beweisbaren Ausgangsverfahren als ermessensfehlerhaft angesehen werden. Diese Fragen sind von der Behörde für Inneres als zuständiger Fachbehörde zu klären.

Wir haben deutlich gemacht, daß aus datenschutzrechtlicher Sicht keine Bedenken gegen die Realisierung der Funktionen zur Mehrfachtäterahndung bestehen, wenn folgende Voraussetzungen erfüllt sind:

— Nur laufende Verfahren können zur Mehrfachtäterahndung herangezogen werden. Abgeschlossen und deshalb nicht mehr zur Mehrfachtäterahndung zu verwenden sind Verwarnungsverfahren nach Zahlung des Verwarngeldes und Bußgeldverfahren nach Rechtskraft des Bußgeldbescheids bzw. der ihn ersetzenden gerichtlichen Entscheidung. Diese Abgrenzung muß in „OPAL" durch eindeutige Funktionen gesichert sein. Hierdurch ist auszuschließen, daß im System angeblich laufende Fälle vorgehalten und zur Mehrfachtäterahndung angezeigt werden, die tatsächlich und rechtlich abgeschlossen sind.

— Ferner muß ausgeschlossen sein, daß bereits abgeschlossene Fälle unabhängig von der automatisierten Mehrfachtäterfunktion „manuell" herangezogen werden, um sie entsprechend höher zu ahnden.

Nur unter diesen Voraussetzungen kann auch akzeptiert werden, daß die Speicherungsdauer im Online-Betrieb von „OPAL" erheblich verlängert werden soll. Im alten System wurden die Fälle nur einen Monat nach Abschluß vorgehalten, in Zukunft sollen dies drei Monate sein, um noch bestimmte Zahlungs-

modalitäten abwickeln zu können. Unfallvorgänge sollen für Verfahrensauskünfte an Berechtigte sogar bis zu einem Jahr nach Abschluß im Online-Zugriff stehen. Anschließend werden die Fälle archiviert und drei Jahre nach Verfahrensende gelöscht.

16.2 Automatisierte Verfahren zur Erhebung von Straßenbenutzungsgebühren

Sowohl für die Autobahnen als auch für den Stadtverkehr wird die Einführung von Straßenbenutzungsgebühren („road pricing") diskutiert. Die Spanne der möglichen Lösungen reicht von einfachen Vignetten bis hin zu vollständig automatisierten Verfahren, die eine strecken- und zeitabhängige Tarifierung gestatten.

Automatisierte Systeme zur Erhebung von Straßenbenutzungsgebühren können das Recht auf informationelle Selbstbestimmung der Straßenbenutzer beeinträchtigen. Zu befürchten ist insbesondere, daß mit derartigen Verfahren erhobene personenbezogene Daten zu Bewegungsprofilen verarbeitet werden.

Im Zusammenhang mit einem Feldversuch auf der Bundesautobahn A555 haben wir im Auftrag des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder Vorschläge für eine datenschutzgerechte Gestaltung des „road pricing" erarbeitet. Diese Vorschläge sollen auf einem vom Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern organisierten Workshop im Januar 1995 mit Vertretern der Wissenschaft, der Hersteller und des Bundesministeriums für Verkehr diskutiert werden.

Nur Verfahren mit geringstmöglichem Eingriff in das allgemeine Persönlichkeitsrecht sollten zum Einsatz kommen. Daraus resultieren die folgenden datenschutzrechtlichen Anforderungen:

Der Grundsatz der „datenfreien Fahrt" muß auch künftig gewährleistet sein. Je weniger personenbezogene Daten erhoben, verarbeitet oder genutzt werden, desto geringer ist auch die Gefahr einer mißbräuchlichen Datennutzung. Aus diesem Grund ist das Anonymitätskriterium die wichtigste Datenschutzanforderung. Jedenfalls sollten bei regelgerechter Straßenbenutzung keine personenbezogenen Daten entstehen.

Grundsätzlich bieten Verfahren, bei denen Gebühren im voraus entrichtet werden (Prepaid-Verfahren) bessere Voraussetzungen für die Wahrung der Anonymität als solche Systeme, bei denen zunächst Verkehrsdaten erhoben und dann den Benutzern in Rechnung gestellt bzw. von deren Konten abgebucht werden (Postpaid-Verfahren).

Soweit die Speicherung von Benutzerdaten gleichwohl erforderlich ist (z.B. für den Nachweis der Richtigkeit der Gebührenerhebung), sollten diese Daten dezentral beim Benutzer gespeichert werden. Die Erhebung von Benutzerdaten

durch „Erhebungsstellen" und deren Übermittlung an Konzentratoren oder zentrale Abrechnungseinheiten sollte unterbleiben.

Die Überwachung der Gebührenerhebung sollte so gestaltet werden, daß die Identität des Benutzers nur dann aufgedeckt wird, wenn ein begründeter Mißbrauchsverdacht besteht. Die Überwachung, ob ein Mißbrauch vorliegt, sollte grundsätzlich nur stichprobenweise und nicht vollständig erfolgen, da Systeme mit flächendeckender Mißbrauchskontrolle eine Infrastruktur voraussetzen, die für eine vollständige Erfassung „zweckentfremdet" werden könnte. Dabei könnte sich die Kontrolldichte an der Kontrollpraxis bezüglich der Einhaltung von Geschwindigkeitsbegrenzungen orientieren.

Sofern personenbezogene Daten erhoben werden, müssen sie vertraulich behandelt werden. Die unbefugte Kenntnisnahme durch Dritte ist durch technische und organisatorische Maßnahmen auszuschließen.

Es ist zu gewährleisten, daß die Daten jeweils den richtigen Benutzern zugeordnet werden und keine Über-, Unter- oder Doppelerfassung erfolgt. Der Abbuchungsimpuls darf nicht derart streuen, daß er etwa – z.B. beim Spurwechsel – andere Fahrzeuge erfaßt.

Alle sicherheitsrelevanten Informationen – hierzu gehören sowohl Authentifikationsdaten als auch benutzungsbezogene Angaben (zurückgelegte Strecke, Zeitpunkte, Tarifierung) – sind mit geeigneten Verfahren gegen Manipulationen zu schützen.

Das gesamte Verfahren muß für die Teilnehmer durchschaubar sein, d. h. die Benutzer müssen die realistische Chance haben, sowohl über den generellen Ablauf als auch über die Datenerhebung und -speicherung im Einzelfall Bescheid zu wissen.

Die Systemkomponenten sind so zu gestalten, daß die Datenschutz- und Datensicherungsfunktionen stabil sind und nicht einseitig durch den Systembetreiber oder durch Dritte zurückgenommen oder unterlaufen werden können.

Systeme, die eine generelle Videoüberwachung des fließenden Verkehrs voraussetzen, werden abgelehnt, weil sie sich bei nur geringen Modifikationen auf eine Vollkontrolle umstellen lassen.

16.3 Illegale Beschäftigung im Taxengewerbe

Im Zusammenhang mit der Änderung der Taxenordnung erfuhren wir von einem Prüfauftrag des Senats, ob Taxenunternehmen illegal Arbeitnehmer beschäftigten und wie dem begegnet werden könne. Im Gespräch war, im Zusammenwirken mit allen prüfberechtigten Verwaltungseinheiten die Kontrollen zu verstärken und Datenübermittlungen an die Bundesanstalt für Arbeit (BA) nicht nur über angestellte Taxifahrer, sondern auch über Taxiunternehmer vorzunehmen.

Der Taxifahrer ist unter anderem verpflichtet, seine Fahrerlaubnis zur Fahrgastbeförderung mitzuführen und zuständigen Personen zur Prüfung auszuhändigen; das gleiche gilt für die Genehmigungsurkunde des Taxis. Die Einhaltung dieser und weiterer taxenspezifischer Vorschriften wird durch einen Außendienst der Baubehörde überprüft.

Daneben muß der Taxiunternehmer nach den sozialrechtlichen Vorschriften jeden Beschäftigten der Einzugsstelle für den Gesamtsozialversicherungsbeitrag (Krankenkasse) melden. Die Einhaltung dieser Pflichten prüft die BA ; sie kann sich hierzu der Amtshilfe der Zollverwaltung sowie der Witschafts- und Ordnungsämter bedienen. Der Außendienst der Baubehörde gehört nicht zu den hierzu befugten Stellen.

Tatsächlich übermittelte die Baubehörde an die BA seit 1986 personenbezogene Daten von angestellten Taxifahrern , die bei Prüfungen der taxenspezifischen Verpflichungen erhoben worden waren.

Nach unserem Hinweis, daß weder die Taxenordnung noch § 150 a Abs. 2 Arbeitsförderungsgesetz solche regelmäßigen präventiven Übermittlungen rechtfertigen, hat die Baubehörde die bisherige Übermittlungspraxis eingestellt. Es besteht Einvernehmen, daß nach der geltenden Rechtslage Übermittlungen an die BA nur in Betracht kommen, wenn konkrete Anhaltspunkte z.B. für eine gewerberechtliche Unzuverlässigkeit bestehen, die durch Nachfrage überprüft werden müssen. Auf dieser Grundlage konnte von einer Beanstandung abgesehen werden.

17. Polizei

17.1 Entwurf eines Gesetzes über das Bundeskriminalamt

Während die meisten Landespolizeigesetze inzwischen Regelungen zur Datenverarbeitung der Polizei enthalten, steht nach wie vor eine bereichsspezifische Novellierung des Gesetzes über das Bundeskriminalamt (BKA-Gesetz) aus. Dieses Defizit wiegt deshalb besonders schwer, weil das BKA-Gesetz zwei Bereiche zu regeln hat. Zum einen sind dies die Kompetenzen der Kriminalpolizei des Bundes, die für die internationale Kriminalität auf den Gebieten Waffen-, Rauschgift- und Falschgeldhandel sowie zur Abwehr und Verfolgung von Straftaten gegen die Bundesorgane zuständig ist. Zum anderen wird im BKA-Gesetz die Datenverarbeitung im bundesweiten Informationssystem der Polizeien (INPOL-System) zu regeln sein. In diesem Zusammenhang hat das BKA-Gesetz ganz wesentliche Auswirkungen für die Datenverarbeitung der Länderpolizeien.

Nach jahrelanger Vorbereitung (siehe 9. TB, 4.12.2.1) wurde im Dezember 1993 ein Entwurf des Bundesministers des Innern vorgelegt, der allerdings erneut so unausgereift war, daß er nicht mehr zur Verabschiedung im Bundeskabinett gelangt ist und daher auch nicht parlamentarisch beraten wurde. Dieser

Entwurf machte jedoch bereits die Grundvorstellungen über zukünftige Regelungen zum INPOL-System deutlich. In unserer Stellungnahme haben wir insbesondere auf folgende Probleme hingewiesen:

— Zentralstellenfunktion des BKA

Wir haben deutlich gemacht, daß der Entwurf das Ziel verfolgte, dem BKA eine Fülle von zusätzlichen Befugnissen zu Lasten der Länder einzuräumen, insbesondere die polizeiliche Datenverarbeitung sehr weitgehend beim BKA zu zentralisieren. Es fiel auf, daß diese beabsichtigte Kompetenzverschiebung nicht an den polizeilichen Aufgaben der Strafverfolgung und Gefahrenabwehr anknüpfte. Vielmehr sollte diesen Aufgaben aus Sicht des BKA eine eigenständige sog. Zentralstellenfunktion hinzugefügt werden.

Die Zentralstelle nach Art. 87 GG unterstützt die jeweils zuständigen Polizeibehörden insbesondere dadurch, daß sie die Infrastruktur für die bundesweite Speicherung und Übermittlung relevanter Erkenntnisse zur Verfügung stellt. Die Teilnehmer des Informationssystems nutzen diese Erkenntnisse zur Erfüllung ihrer eigenen polizeilichen Aufgaben. In einem stellenübergreifenden Informationssystem muß die datenschutzrechtliche Verantwortlichkeit immer bei der Stelle liegen, die die Daten erhoben hat und für eigene Zwecke im Informationssystem speichert.

Nach der Konzeption des Entwurfs sollten die anliefernden Polizeibehörden für die von ihnen eingegebenen Daten zwar verantwortlich sein; das BKA sollte jedoch befugt werden, sämtliche Daten zu verändern, zu nutzen, zu ergänzen und zu übermitteln. Hierbei sollte es nicht an seine materiellen Aufgaben als Bundespolizeibehörde gebunden sein. Vielmehr sah der Entwurf vor, daß die hiervon weitestgehend losgelöste Zentralstellenfunktion das BKA ermächtigen sollte, sich über die Bindungen hinwegzusetzen, die für die verantwortlichen Stellen gelten.

Damit verkehrte der Entwurf die in Art. 87 GG vorgesehene Unterstützungsfunktion der Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen zu einer selbständigen Bundesaufgabe mit eigenen Eingriffsbefugnissen unabhängig von der materiellen Aufgabenzuweisung auf den Gebieten Strafverfolgung und Gefahrenabwehr.

— Rechte der Betroffenen und Datenschutzkontrolle

Der Entwurf enthielt ursprünglich eine Regelung, die vorsah, daß nur das BKA Auskunft an die Betroffenen erteilen sollte. Damit wäre im Unterschied zu bisher keine Auskunftserteilung durch Länderpolizeien über die von ihnen im INPOL-System gespeicherten Daten mehr möglich gewesen. Dies hätte im eklatanten Widerspruch zu deren eigener datenschutzrechtlicher Verantwortung für die Speicherungen gestanden. In den weiteren Beratun-

gen des Entwurfs wurde klargestellt, daß die Auskunftserteilung durch die Stelle, die die Daten eingegeben hat, unberührt bleibt.

Auch in Bezug auf die Datenschutzkontrolle gab es Unklarheiten. Zunächst wurde nur auf die Kontrollkompetenz des Bundesbeauftragten für den Datenschutz (BfD) nach § 24 Bundesdatenschutzgesetz (BDSG) verwiesen. Die Prüfungskompetenz des BfD für das gesamte beim BKA geführte INPOL-System ist unbestritten. Dies kann jedoch nicht bedeuten, daß keine Kontrollbefugnis der Landesbeauftragten für die von den jeweiligen Länderpolizeien eingegebenen Daten besteht, da dann eine massive Beeinträchtigung der Kontrollierbarkeit des gesamten INPOL-Systems eintreten würde. In den weiteren Beratungen wurde die Kontrollbefugnis der Landesbeauftragten klargestellt.

Es bleibt abzuwarten, ob in der neuen Legislaturperiode ein Entwurf für das BKA-Gesetz vorgelegt wird, der die Schwächen seiner Vorläufer vermeidet.

17.2 Entwurf eines Übereinkommens für ein Europäisches Polizeiamt (Europol)

Die Pläne, ein Europäisches Polizeiamt (Europol) einzurichten, stehen im Vordergrund der öffentlichen Diskussionen um die Zukunft der polizeilichen Aufgaben, insbesondere im Zusammenhang mit der Verfolgung der organisierten Kriminalität. Allerdings wird hierbei nicht immer deutlich, um was es bei Europol eigentlich geht.

Falsch ist jedenfalls die Vorstellung, in Zukunft würden Europol-Beamte bei internationalen Verbrechen eigene Ermittlungen durchführen, Täter verhaften und vor Gericht bringen. Die Aufgaben der Strafverfolgung und polizeilichen Gefahrenabwehr sollen auch nach Errichtung von Europol unverändert bei den zuständigen Polizeien der Mitgliedstaaten der Europäischen Union (EU) verbleiben. Das heißt, das Landeskriminalamt Hamburg (LKA) bleibt auch dann zuständig, wenn hiesige Kriminalität in andere EU-Staaten hineinreicht oder von dort herrührt.

Europol soll vielmehr die Zusammenarbeit zwischen den Polizeien der Mitgliedstaaten unterstützen, insbesondere ein europaweites Informationssystem der Polizeien zur Verfügung stellen. Damit ist klar, daß datenschutzrechtliche Fragen das zentrale Problem bei der Errichtung von Europol sind.

Auch aus datenschutzrechtlicher Sicht besteht kein Zweifel an der Notwendigkeit eines Austauschs der erforderlichen Informationen in einem zusammenwachsenden Europa. Diese Zusammenarbeit zwischen den Polizeien der Mitgliedstaaten der EU ist in einem völkerrechtlich verbindlichen Vertrag zwischen den Mitgliedstaaten zu regeln.

Wesentlich ist jedoch, daß im Rahmen dieser Zusammenarbeit die materielle Verantwortlichkeit der zuständigen Polizeibehörden gewahrt bleiben muß. Nur die Polizeibehörde, die personenbezogene Daten rechtmäßig erhoben hat sowie zu eigenen Zwecken speichert und nutzt, kann die Erforderlichkeit ihrer weiteren Verwendung im europäischen Zusammenhang beurteilen. Aufgrund ihrer Erkenntnisse und Unterlagen ist nur sie in der Lage, die Richtigkeit und Vollständigkeit der an andere europäische Polizeien übermittelten Daten zu gewährleisten.

Das Übereinkommen zur Errichtung eines europäischen Polizeiamtes (Europol-Übereinkommen) darf sich nicht über diesen Grundsatz der materiellen Verantwortlichkeit hinwegsetzen. Andernfalls würde eine eigenständige polizeiliche Aufgabe geschaffen, wozu weder der Bundesgesetzgeber noch die Europäische Union befugt ist. Art. 73 Nr. 10 GG verleiht dem Bund auch bei der internationalen Verbrechensbekämpfung nur die Gesetzgebungskompetenz für die Zusammenarbeit des Bundes und der Länder mit den ausländischen Behörden; die materiellen Zuständigkeiten werden hierbei vorausgesetzt. Artikel K.2 Abs. 2 des Vertrages über die Europäische Union stellt ausdrücklich fest, daß die Verantwortung der Mitgliedstaaten bei der Aufrechterhaltung der öffentlichen Ordnung und dem Schutz der inneren Sicherheit unberührt bleibt.

Für das Europol-Übereinkommen bedeutet dies, daß die Regelungen für den Aufbau eines gemeinsamen Informationssystems daran zu messen sind, ob sie die polizeilichen Aufgaben im europäischen Zusammenhang unterstützen oder eigenständige hiervon losgelöste Informationsstrukturen schaffen. Aus datenschutzrechtlicher Sicht sind daher folgende Anforderungen zu stellen:

Entscheidendes Kriterium für die Frage, welche Daten im Europol-Informationssystem gespeichert werden können, muß eine klare Beschreibung der Zielsetzung von Europol sein.

Von der Straftat, die zur Speicherung führt, müssen mehrere Mitgliedstaaten in einer Weise betroffen sein, die aufgrund des Umfangs, der Bedeutung und der Folgen ein gemeinsames Vorgehen der Mitgliedstaaten erfordern.

Alle im Informationssystem gespeicherten und im Rahmen von Europol übermittelten Daten dürfen nur zur Verfolgung und Verhütung dieser eindeutig zu beschreibenden Kriminalitätsformen verwendet werden.

Speicherungen im Informationssystem von Europol können nur durch die Stelle veranlaßt werden, die materiell für die zugrundeliegende Aufgabe der Strafverfolgung oder Gefahrenabwehr zuständig ist.

Der Verantwortlichkeit für die Eingaben in das Informationssystem müssen auch die weiteren Verarbeitungsschritte, insbesondere Berichtigungen und Löschungen folgen. Wenn die ursprünglich zuständige Behörde zu Berichti-

gungen oder Löschungen verpflichtet ist, muß sie diese direkt vornehmen oder verbindlich veranlassen können.

Eigene Datenbestände von Europol, die nicht unmittelbar von den zuständigen Polizeibehörden der Mitgliedstaaten gespeist werden, dürfen nicht entstehen.

Die Regelungen über die Rechte der Betroffenen – insbesondere auf Auskunft – und über den Rechtsweg müssen sich am Vorbild des Schengener Durchführungsübereinkommens orientieren:

Die Auskunftserteilung muß sich nach dem Recht des Mitgliedstaates richten, in dem der Auskunftsantrag gestellt wird. Klagen in Bezug auf die Datenverarbeitung im Informationssystem müssen vor den Gerichten der Mitgliedstaaten erhoben werden können. Nur wenn dies gewährleistet ist, kann zusätzlich eine Zuständigkeit von Europol selbst für Auskunftserteilungen und eine Zuständigkeit der Europäischen Gerichtsbarkeit für Klagen in Betracht kommen.

Die Datenschutzkontrolle des Informationssystems muß in erster Linie bei den Polizeibehörden ansetzen, von denen die im Rahmen von Europol verarbeiteten Informationen stammen.

Für die Bundesrepublik Deutschland bedeutet dies: Der Bundesbeauftragte und die Landesbeauftragten kontrollieren in ihrem jeweiligen Zuständigkeitsbereich die Datenanlieferungen für und Abrufe bei Europol. Hierfür müssen sie jeweils Zugang zu den entsprechenden Protokollen haben. Bei der Bildung der für Europol insgesamt zu schaffenden gemeinsamen Kontrollinstanz sind die Landesbeauftragten für den Datenschutz angemessen zu beteiligen.

Wir haben unsere Bedenken gegenüber den zuständigen hamburgischen Behörden geltend gemacht, damit sie in die Bundesratsberatungen einbezogen werden.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich in einer gemeinsamen Entschließung ebenfalls in diesem Sinne geäußert. Sofern keine Verbesserungen im Übereinkommenstext erreicht werden, soll die deutsche Seite wenigstens eine Klarstellung über die Verantwortung der Länder für die in ihrem Zuständigkeitsbereich erhobenen Daten zum Beispiel durch eine Protokollerklärung, treffen. Der Bundesbeauftragte für den Datenschutz hat diese Entschließung der Arbeitsgruppe Europol beim Rat der Europäischen Union mitgeteilt.

17.3 Projekt Computerunterstützte Vorgangsbearbeitung bei der Polizei (COMVOR)

1994 ist die erste Teilleistung des Verfahrens COMVOR in einer Pilotdienststelle eingeführt worden. Sie betrifft die rechnergestützte Erstellung einer großen Anzahl polizeilicher Formulare anhand von vorgefertigten Masken.

Allerdings hat sich gezeigt, daß die Gestaltung, insbesondere die Übersichtlichkeit der Masken, noch nicht den Anforderungen der Anwender entspricht. Ein weiteres erhebliches Problem stellte das Antwortzeitverhalten beim Ausdruck der Texte dar. Aus Sicht der Praxis dauerte es viel zu lange, bis ein Text nach Ausführung des Druckauftrags vorlag. Daher war eine umfassende Überarbeitung der ersten Teilleistung erforderlich. Neue datenschutzrechtliche Probleme sind damit nicht verbunden. Wir haben eine Überprüfung des bisherigen Verfahrensstandes zurückgestellt, bis diese Überarbeitung abgeschlossen ist.

17.4 Überprüfung der Erforderlichkeit polizeilicher Befugnisse und der Auswirkungen für die Rechte der Betroffenen

Im 11.TB (17.9) und 12. TB (17.7 bzw.19.8) waren jeweils Zahlenangaben über Einsätze besonderer Befugnisse zur verdeckten Datenerhebung nach dem Hamburgischen Gesetz über die Datenverarbeitung der Polizei (HmbPolDVG) und der Strafprozeßordnung veröffentlicht worden. In diesem Tätigkeitsbericht wird von dieser Veröffentlichung abgesehen.

Ein Grund hierfür ist, daß die veröffentlichten Zahlen kein vollständiges Bild über den tatsächlichen Umfang des Einsatzes dieser besonderen Erhebungsmethoden gaben, weil insbesondere die Staatsanwaltschaft bei dem Landgericht Hamburg selbst keine vollständige Kenntnis über die Einsatzzahlen hat. Sie stimmte auch der Veröffentlichung über Einsätze nach der StPO aus Sicherheitsgründen grundsätzlich nicht zu. Die damalige generelle Auskunftsverweigerung durch die Staatsanwaltschaft bei dem Oberlandesgericht Hamburg halte ich weiterhin für unzulässig (siehe Niederschrift über den Unterausschuß Datenschutz der Bürgerschaft vom 28. Oktober 1994). Die Polizei gab nur bei Einsätzen verdeckter Ermittler und V-Personen nach dem HmbPolDVG keine Zustimmung zu der Veröffentlichung.

Der wichtigere Grund für den jetzigen Verzicht auf die Veröffentlichung reiner Fallzahlen ist, daß inzwischen eine breitere Diskussion über die Notwendigkeit stattgefunden hat, das Wissen über die Erforderlichkeit und die Auswirkungen der polizeilichen Befugnisse zur Erhebung personenbezogener Daten auf eine bessere Grundlage zu stellen.

Angesichts der aktuellen Diskussion über die innere Sicherheit ist darauf hinzuweisen, daß seit Jahren die polizeilichen Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten insbesondere im technischen Bereich gesetzlich verankert und auch erweitert worden sind.

Zum Kreis der Betroffenen zählen dabei nicht nur Personen, gegen die Verdachtsgründe vorliegen, sondern auch nicht verdächtige Kontakt- und Begleitpersonen und sonstige Unbeteiligte, deren Schutz nach Auffassung der Datenschutzbeauftragten besonders wichtig ist.

In der aktuellen Auseinandersetzung über Maßnahmen zur Aufrechthaltung der inneren Sicherheit wird behauptet, daß diese staatlichen Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten notwendig und die damit verbundenen Eingriffe im überwiegenden Interesse der Allgemeinheit gerechtfertigt sind. Forderungen, noch weitergehende Eingriffe in die Grundrechte – insbesondere das Persönlichkeitsrecht (Art. 2 GG), das Fernmeldegeheimnis (Art. 10 GG) und die Unverletzlichkeit der Wohnung (Art. 13 GG) – zuzulassen, schließen sich an. Dagegen werden Bedenken vorgebracht, daß von den bestehenden und weiteren Eingriffsbefugnissen Gefährdungen für Grundrechte ausgehen könnten.

Auch auf ausdrückliche Nachfragen sind mir bisher keine Belege für die Annahme erbracht worden, datenschutzrechtliche Bestimmungen würden die wirksame Verfolgung oder Verhütung von Straftaten verhindern oder unvertretbar erschweren.

Aus meiner Sicht wäre es ein Gewinn, wenn sich die Diskussion über die Erforderlichkeit der bestehenden Instrumente zur polizeilichen Datenverarbeitung und deren Ausweitung auf Erkenntnisse stützen würde, die stärker als bisher gesichert sind. Das Bundesverfassungsgericht hat im Volkszählungsurteil – bezogen auf statistische Erhebungen – ausgeführt, daß der Gesetzgeber „ungewissen Auswirkungen eines Gesetzes dadurch Rechnung tragen muß, daß er die ihm zugänglichen Erkenntnisquellen ausschöpft, um die Auswirkungen so zuverlässig wie möglich abschätzen zu können; bei einer sich später zeigenden Fehlprognose ist er zur Korrektur verpflichtet. Der Gesetzgeber kann aufgrund veränderter Umstände zur Nachbesserung einer ursprünglich verfassungsgemäßen Regelung gehalten sein."

Vor diesem Hintergrund habe ich sowohl der Behörde für Inneres als auch in der Diskussion mit den anderen Datenschutzbeauftragten des Bundes und der Länder Vorschläge unterbreitet, um den derzeitigen Erkenntnisstand über die Erforderlichkeit polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten sowie ihre Auswirkungen auf die Rechte der Betroffenen zu verbessern.

17.4.1 Rechtstatsachensammlung

Gemeinsam mit den übrigen Datenschutzbeauftragten des Bundes und der Länder teile ich die von zuständigen Innenministern vertretene Auffassung, daß bloße Angaben über Einsatzzahlen der besonderen Befugnisse zur Datenerhebung nur einen begrenzten Aussagewert haben. Um Aufschluß über die tatsächliche Praxis, ihre Erforderlichkeit und Verhältnismäßigkeit zu bekommen, müssen unter Beteiligung der Datenschutzbeauftragten und der Wissenschaft, insbesondere der Kriminologie und des Polizeirechts, objektive und nachprüfbare Auswertungskriterien entwickelt werden.

Die Datenschutzbeauftragten begrüßen daher die Initiative für eine sogenannte Rechtstatsachensammlung, die Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen zusammenführen soll. Sie schlagen vor, in diese Rechtstatsachensammlung insbesondere Angaben über den Anlaß einer Datenerhebung mit besonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, den betroffenen Personenkreis sowie die Anzahl der ermittelten und verurteilten Personen einzubeziehen. Derartige Aufstellungen wären nicht nur für elektronische Überwachungsmethoden, sondern auch für Observationen, verdeckte Ermittler und V-Personen sowie Rasterfahndungen denkbar.

17.4.2 Überprüfung der Erforderlichkeit von Dateien

Das Hamburgische Gesetz über die Datenverarbeitung der Polizei (HmbPolDVG) wie die Dateienrichtlinien des Bundes und die meisten anderen Polizeigesetze verpflichten zur Überprüfung der Notwendigkeit, bestehende Dateien weiterzuführen oder zu ändern. Der Arbeitskreis II der Innenministerkonferenz hat 1990 beschlossen, über Effektivität und Effizienz der einzelnen INPOL-Anwendungen zu berichten. Hierbei soll u.a. auf die weitere Erforderlichkeit der Anwendungen, deren Nutzen, Schwachstellen und Mängel sowie Vorschläge zu deren Beseitigung oder Minimierung eingegangen werden.

Ich halte es für erforderlich, für diese Überprüfungen Kriterien zu entwickeln, die sich z.B. auf folgende Bereiche beziehen:

— Überprüfung der tatsächlichen Nutzung anhand der „Trefferfälle" insbesondere bei Anwendungen, die mit dem Zweck betrieben werden, polizeiliche Maßnahmen im Einzelfall zu ermöglichen (z.B. ist für die Arbeitsdatei „Landfriedensbruch" bereits vor Jahren von den Anwendern erwogen worden, Trefferfälle zumindest zahlenmäßig zu erfassen, um Aufschluß über die Effizienz des Meldedienstes zu erhalten).

— Überprüfung der Nutzbarkeit für unterschiedliche Zwecke (z.B. hat eine polizeiinterne Arbeitsgruppe im Jahr 1989 den möglichen Nutzen der Datei APIS anhand von Kriterien in den Bereichen Repression und Prävention definiert und auf dieser Grundlage Einzelfälle ausgewertet, 9.TB, 4.12.5.1).

— Überprüfung der Speicherungsvoraussetzungen insbesondere, wenn die Errichtungsanordnungen Bewertungen verlangen (vgl. unten 17.5).

— Überprüfung anhand des jeweiligen Kriminalitätsbereichs (z.B. hat eine Analyse der sog. „Rotlichtkriminalität" in Hamburg zum Verzicht auf die bisherige undifferenzierte Erfassung von Prostituierten und stattdessen zur Konkretisierung auf die relevanten Erscheinungsformen der Zuhälter- und Milieukriminalität geführt, 12. TB, 17.5).

17.4.3 Weiterer Fortgang der Diskussion

In einer Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sind die Grundlinien dieser Vorschläge vereinbart worden. Die Datenschutzbeauftragten gehen davon aus, daß sie bei den Überlegungen zur Rechtstatsachensammlung rechtzeitig beteiligt und die jeweiligen Materialien und Zwischenergebnisse mit ihnen erörtert werden. Innerhalb der Polizeien wird das Thema Rechtstatsachensammlung im Rahmen der AG Kripo diskutiert, allerdings sind noch keine Ergebnisse erzielt worden. Die Behörde für Inneres hat für 1995 angekündigt, die im PolDVG vorgesehene Dateienüberprüfung durchzuführen.

17.5 Arbeitsdatei PIOS „Innere Sicherheit" (APIS)

Im 12. TB (17.7) war geschildert worden, in welcher Form die Staatsschutzabteilung des Landeskriminalamtes (LKA) das Ersuchen der Bürgerschaft zum 10. TB umsetzen wollte. Danach sollten die Auswirkungen der in Schleswig-Holstein entwickelten ergänzenden Regelung für die Datei APIS durch ein Versuchsprogramm dokumentiert werden. Das LKA vergibt für die Fälle, die unter die Regelung aus Schleswig-Holstein fallen, also dort nicht gespeichert werden könnten, eine besondere Kennung. Im Oktober 1994 haben wir uns einen Eindruck von der bisherigen Verfahrensweise verschafft.

Von den seit April 1993 in APIS insgesamt erfaßten 937 Taten waren mit Stand vom 4. Oktober 1994 145 mit der besonderen Kennung versehen. Teilweise ist die Kennungsvergabe rückwirkend erfolgt. Bei insgesamt 328 Taten mit linksextremistischer Zuordnung wurden 24 Kennungen vergeben. Bei 411 Taten mit rechtsextremistischer Zuordnung wurden 114 Kennungen vergeben. Der Bereich der sogenannten fremdenfeindlichen Straftaten (198 Fälle) ist von dem Versuchsprogramm ausgenommen.

Aufgrund einiger Stichproben haben wir die Vergabe der besonderen Kennungen mit den zuständigen Mitarbeitern eingehend erörtert. Hierbei stellte sich heraus, daß in einer Reihe von Fällen, in denen auch nach der ergänzenden Regelung die APIS-Speicherung möglich ist, die Kennungen vergeben wurden. Hierbei würde also eine APIS-Speicherung unterbleiben, obwohl die ergänzende Regelung hierfür keine Veranlassung gibt.

Betroffen waren Fälle von Gewaltandrohung oder -anwendung gegen Personen (z.B. Bombendrohungen oder tätliche Angriffe auf Polizeibeamte), die nach der ergänzenden Regelung Indizien für hinreichende Schwere der Tat und überregionale Bedeutung darstellen, also eine APIS-Speicherung ermöglichen, auch wenn die extremistische Motivation nicht zweifelsfrei ist.

Ferner waren auch solche Fälle mit den Kennungen versehen, in denen die Straftaten zwar nur zu geringfügigen Sachbeschädigungen geführt hatten, die extremistische Motivation jedoch eindeutig feststellbar war; z.B. lagen Bekennerschreiben vor, mit denen sich die Täter selbst extremistischen Bestrebungen zuordneten. Offenbar legte die Staatsschutzabteilung die ergänzende Regelung so aus, daß geringfügige Sachbeschädigungen immer zur Anwendung der Regelung und damit zum Ausschluß aus APIS führen.

Eine Reihe von Fällen betraf die Verwendung von Kennzeichen nach § 86a StGB, also Hakenkreuzen und ähnlicher Nazisymbole. Die ergänzende Regelung schließt die Speicherung dieser Fälle nicht generell aus, vielmehr soll geprüft werden, ob es sich um eine unpolitische Einzeltat oder um eine Tat mit verfassungsfeindlicher Zielsetzung und Zusammenhängen zu rechtsextremistischen Organisationen handelt. Danach ist etwa zu unterscheiden, ob es sich um eine Hakenkreuzschmiererei an einer beliebigen Stelle handelt oder z.B. um den gewerbsmäßigen Vertrieb von Naziemblemen. Im ersteren Fall sind APIS-Speicherungen schon wegen der mangelnden Bedeutung der Information für Teilnehmer an dem Verbundsystem APIS in anderen Bundesländern wenig sinnvoll, im zweiten Fall liegt die extremistische Zielsetzung und deren überregionale Bedeutung auf der Hand.

Wir haben deutlich gemacht, daß der Sinn der ergänzenden Regelung nicht darin besteht, schematisch bestimmte Fallgruppen auszuschließen. Vielmehr haben wir vorgeschlagen, die versuchsweise Erprobung der ergänzenden Regelungen auf die Frage zu konzentrieren, ob ein Verzicht auf folgende Fälle möglich ist:

— Es gibt keine eindeutigen Anhaltspunkte für die extremistische Motivation;

— in diesen Fällen ohne eindeutige Anhaltspunkte liegt auch keine Androhung oder Ausübung von Gewalt gegen Personen vor oder der Sachschaden ist nicht höher als DM 1000;

— diese Fälle haben auch keine überörtliche Bedeutung.

Wenn die Regelung dagegen so ausgelegt wird, daß auch eindeutig extremistisch motivierte und schwere Fälle unter sie fallen, wird das von der Bürgerschaft gewünschte Versuchsprogramm ad absurdum geführt.

Die Behörde für Inneres hat hierzu mitgeteilt, daß eine grundsätzliche Änderung der Verfahrensweise bei der Vergabe der Kennungen zur Zeit nicht erfolgen soll. Die exakte Zuordnung soll vielmehr bei der gemeinsam mit uns im September 1995 beabsichtigten Auswertung angestrebt werden.

17.6 Automatisiertes Fingerabdruck-Identifizierungssystem (AFIS)

17.6.1 Speicherungen in AFIS

Im Dezember 1993 hat das Bundeskriminalamt (BKA) das automatisierte Fingerabdruck-Identifizierungssystem vollständig in Betrieb genommen. Früher waren Unterlagen über Fingerabdrücke aus erkennungsdienstlichen Behand-

lungen nur indirekt aufgrund einer Verformelung der wesentlichen Merkmale automatisiert recherchierbar. AFIS ermöglicht dagegen den unmittelbaren Vergleich von Fingerabdrücken aus Tatortspuren mit dem gespeicherten Referenzmaterial über Fingerabdrücke aufgrund von erkennungsdienstlichen Behandlungen.

Das wesentliche datenschutzrechtliche Problem an AFIS ist der Umfang des gespeicherten Referenzmaterials. Nach § 81b der Strafprozessordung (StPO) ist die Erhebung und Speicherung von Fingerabdrücken zum Zwecke des Erkennungsdienstes zulässig. Erkennungsdienstlich behandelt werden dürfen nach dieser Vorschrift nur Personen, gegen die als Beschuldigte ein strafrechtliches Ermittlungsverfahren durchgeführt worden ist und die aus polizeilicher Sicht auch in Zukunft als Straftäter in Betracht kommen können. Für diese Fälle ersetzt AFIS lediglich das herkömmliche System der Speicherung von Fingerabdrücken durch eine modernere Technik.

Ein Jahr vor der Einführung von AFIS für diese polizeilichen Zwecke wurde das System bereits zur Erfassung von erkennungsdienstlichen Unterlagen über Asylbewerber benutzt. Nach § 16 Asylverfahrensgesetz (AsylVfG) ist die erkennungsdienstliche Behandlung (ed-Behandlung) sämtlicher Asylbewerber vorgesehen, unabhängig davon, ob sie Straftaten begangen haben oder über gültige Ausweispapiere verfügen. Lediglich Minderjährige unter 14 Jahren und Inhaber von unbefristeten Aufenthaltsgenehmigungen sind ausgenommen. Die ed-Unterlagen über Asylbewerber werden von den jeweils örtlich zuständigen Außenstellen des Bundesamtes für die Anerkennung ausländischer Flüchtlinge erhoben und ebenso wie die von der Polizei erhobenen Unterlagen über Strafverdächtige beim Bundeskriminalamt gespeichert.

Der Einwand von Datenschutzbeauftragten des Bundes und der Länder, daß eine ed-Behandlung von Asylbewerbern nur dann verhältnismäßig sei, wenn die Betroffenen über keine Ausweispapiere verfügen, blieb unberücksichtigt.

17.6.2 Nutzung von AFIS durch die Polizei

Wir haben im Berichtszeitraum die Verfahrensweise der Polizei bei der Nutzung von AFIS geprüft und festgestellt, daß sie grundsätzlich datenschutzrechtlich bedenkenfrei ist.

Die an Tatorten gesicherten Fingerabdruckspuren werden in einer sogenannten Remotestation im Landeskriminalamt (LKA) von einer Kamera aufgenommen. Die anatomischen Merkmale werden automatisiert codiert, manuell nachbearbeitet und dann per Datenleitung zum BKA überspielt. Dort werden sie mit den gespeicherten Fingerabdrücken verglichen, wobei regional und gegenständlich differenzierte Recherchemöglichkeiten bestehen.

Schätzungsweise 80% der Recherchen des LKA werden im Bereich der aus Hamburg und dem Umland gespeicherten Fingerabdrücke durchgeführt. Darüberhinaus sind Recherchen im polizeilichen Gesamtbestand, im Bestand der Daten über Asylbewerber und im Gesamtbestand von AFIS (also Verdächtige und Asylbewerber) möglich.

Eine Recherche, die auch den Bestand nach AsylVfG umfassen soll, muß von der anfordernden Dienststelle schriftlich besonders begründet werden. Hierbei müssen bestimmte Tatsachen dafür vorliegen, daß die Spuren von einer Person stammen, die im Bestand nach AsylVfG erfaßt ist.

Als Ergebnis der Recherche unterbreitet AFIS ein „Angebot" von bis zu 99 ähnlichen Fingerabdruckmustern. Ob die Spuren tatsächlich mit den von AFIS angebotenen Fingerabdrücken übereinstimmen, wird dann anschließend anhand eines nicht-automatisierten Vergleichs zwischen der Spur und dem Original des Fingerabdruckblatts festgestellt.

Die eingelesenen Spuren enthalten keine Hinweise auf personenbezogene Daten. Auch die Rechercheergebnisse weisen nicht die Personalien derjenigen auf, von denen die Spuren stammen, sondern nur eine 12-stellige Nummer. Anhand dieser Nummer muß eine Abfrage in der INPOL-ED-Datei erfolgen, um die Personalien festzustellen.

17.6.3 Errichtungsanordnung für AFIS

Während diese Praxis der Polizei einwandfrei ist, muß bemängelt werden, daß für den Betrieb von AFIS die erforderliche Errichtungsanordnung mit wesentlichen Regelungen fehlt.

Aus unserer Sicht ist in der Errichtungsanordnung festzulegen, daß Zugriffe auf den Bestand der Asylbewerber nur unter den besonderen gesetzlichen Voraussetzungen nach § 16 Abs. 5 AsylVfG erfolgen. Ob diese Voraussetzungen im Einzelfall vorgelegen haben, läßt sich nachträglich nur anhand der jeweiligen Ermittlungsvorgänge feststellen. Daher ist eine besondere Protokollierung dieser Recherchen erforderlich. Dagegen halten wir die zur Zeit praktizierte Protokollierung sämtlicher Anfragen im Bestand, der nicht die Asylbewerberdaten umfaßt, für überflüssig. Aus diesen Protokollen läßt sich nicht mehr entnehmen, als daß die Mitarbeiter der Dienststelle, die über den AFIS-Anschluß verfügt, den AFIS-Datenbestand im Rahmen seiner Zweckbestimmung benutzt haben.

Dagegen hätte eine gesonderte Protokollierung von Recherchen im Asylbewerberbestand die Wirkung, daß die besonderen Voraussetzungen für Recherchen im Bestand nach AsylVfG in Erinnerung gerufen werden und somit Routinerecherchen in diesem Bestand unterbleiben. Da diese Protokollierung Auskunft über das Abrufverhalten der Landespolizei gibt, müssen die Landes-

beauftragten für den Datenschutz auf Anforderung zu Prüfzwecken Zugang zu diesen Protokollen haben. Dies ist bislang nicht eindeutig geregelt.

17.7 Probleme bei polizeilichen Datenübermittlungen

Bei Eingaben von Bürgern oder datenschutzrechtlichen Prüfungen stellen sich häufig Fragen, ob und inwieweit die Polizei personenbezogene Daten an andere Stellen übermitteln darf. Im folgenden werden daher beispielhaft einige dieser Problemfälle dargestellt.

17.7.1 Übermittlungen aus polizeilichen Dateien ohne aktuelle Feststellungen

Im 12. TB (16.1) war bereits ein Fall geschildert worden, in dem die Polizei der Führerscheinstelle Mitteilung über einen acht Jahre zurückliegenden Vorgang im Zusammenhang mit Drogenkonsum gemacht hatte. 1994 betraf eine Eingabe die polizeiliche Mitteilung an ein Wirtschafts- und Ordnungsamt über Jahre zurückliegende Ermittlungsverfahren aus Anlaß der Erteilung einer Gewerbeerlaubnis.

Grundlage für die Übermittlung war jeweils eine Speicherung über die Petenten im polizeilichen Auskunftssystem POLAS; aktuelle polizeiliche Feststellungen lagen den Mitteilungen nicht zugrunde. In beiden Fällen waren über die Petenten weder im Bundeszentralregister noch im Verkehrs- oder Gewerberegister Eintragungen vorhanden. Die Übermittlung an die Führerscheinstelle erfolgte spontan durch einen Polizeibeamten, die Mitteilung an das Wirtschafts- und Ordnungsamt beruhte auf einer entsprechenden Nachfrage.

Wir haben dagegen geltend gemacht, daß Speicherungen im polizeilichen Auskunftssystem oder anderen polizeilichen Dateien besonders tief in die Rechte der Betroffenen eingreifen. Gemäß § 16 Abs. 2 Satz 3 und 4 des hamburgischen Gesetzes über die Datenverarbeitung der Polizei (HmbPolDVG) sind sie nicht abhängig von rechtskräftigen Verurteilungen; vielmehr reicht ein polizeilicher Verdacht aus, der im weiteren Ermittlungsverfahren nicht ausgeräumt worden ist. POLAS und andere polizeilichen Dateien dienen grundsätzlich nur der Gewinnung von Erkenntnissen durch die Polizei zur Strafverfolgung und vorbeugenden Bekämpfung von Straftaten, nicht jedoch als Informationsquelle für andere Stellen, die nicht diesen gesetzlichen Auftrag haben. Die weitreichenden polizeilichen Speicherungsbefugnisse sind nur dann verhältnismäßig, wenn die Dateieintragungen auf ihren ursprünglichen Zweck und die in ausdrücklichen gesetzlichen Vorschriften normierten Verwendungsmöglichkeiten begrenzt bleiben.

§ 20 Abs. 1 Satz 3 HmbPolDVG läßt die Übermittlung personenbezogener Daten zu einem anderen Zweck als dem der Speicherung nur zu, wenn die Daten auf andere Weise nicht rechtzeitig oder nur mit unverhältnismäßigem

Aufwand erlangt werden können und die Übermittlung zur Abwehr einer unmittelbar bevorstehenden Gefahr erforderlich ist. Entscheidend ist das Kriterium der unmittelbar bevorstehenden – also konkreten – Gefahr. Die Verfahren zur Überprüfung der Eignung zum Führen eines Fahrzeugs und das Verfahren zur Überprüfung der gewerberechtlichen Zuverlässigkeit betreffen jedoch lediglich abstrakte Gefahren für die Sicherheit im Straßenverkehr oder bei der Ausübung von Gewerben.

Nur wenn in besonderen Rechtsvorschriften im Sinne von § 20 Abs. 4 HmbPolDVG auch die Heranziehung von polizeilichen Erkenntnissen vorgesehen ist, kann auf Speicherungen in POLAS zurückgegriffen werden. Dies ist z.B. bei förmlichen Sicherheitsüberprüfungen der Fall (vgl. § 12 Abs. 1 Nr. 3 und Abs. 2 Sicherheitsüberprüfungsgesetz des Bundes).

Für den Fall der Gewerbeerlaubnis gestattet die Gewerbeordnung in § 11, daß Anfragen an die Polizei nach laufenden Verfahren gerichtet werden. Hiermit soll vermieden werden, daß in Unkenntnis eines schwebenden Strafermittlungsverfahrens eine Gewerbeerlaubnis erteilt wird, die nach einer Verurteilung sofort wieder entzogen werden müßte. Bereits vor Inkrafttreten dieser Regelung in der Gewerbeordnung beschränkten die einschlägigen Verwaltungsvorschriften entsprechende Anfragen bei der Polizei auf laufende Verfahren in besonderen Einzelfällen.

Im Falle des Petenten bezogen sich die von der Polizei an das Wirtschafts- und Ordnungsamt mitgeteilten Erkenntnisse aus POLAS aber ausschließlich auf längst abgeschlossene Ermittlungen. Bei der Erteilung der Gewerbeerlaubnis konnten sie demnach gar nicht mehr berücksichtigt werden.

Derartige Übermittlungen über Speicherungen in POLAS, die sich auf zurückliegende Ermittlungen beziehen, unterlaufen die Tilgungsfristen des Bundeszentralregistergesetzes, wenn diese kürzer sind als die Speicherungsdauer in POLAS. Dies ist oftmals der Fall, da keine rechtlichen Abhängigkeiten bestehen.

17.7.2 Übermittlungen aus Anlaß aktueller polizeilicher Feststellungen

Ganz anders zu beurteilen sind Übermittlungen der Polizei, die nicht auf Dateispeicherungen beruhen, sondern die sie anläßlich aktueller eigener Datenerhebungen vornimmt. Ein Beispiel hierfür ist die polizeiliche Feststellung, daß jemand unter Drogeneinfluß am Straßenverkehr teilnimmt. Zweck der Datenerhebung über den unter Drogen stehenden Autofahrer ist in diesem Zusammenhang nicht die vorbeugende Bekämpfung von Straftaten, sondern die Gewährleistung der Verkehrssicherheit. Daher entspricht der Erhebungszweck dem der Übermittlung an die Führerscheinstelle. Beide Male soll die Verkehrssicherheit gewährleistet werden: durch den Polizeibeamten vor Ort, indem er den Betroffenen an der Weiterfahrt hindert, durch die Übermittlung an die Führerscheinstelle, damit sie die Eignung zum Führen eines Kraftfahrzeugs fest-

stellt. Die Feststellungen sind aktuell und beruhen nicht auf Vorratsspeicherungen für zukünftige Zwecke. Daher ist die Übermittlung gemäß § 20 Abs. 1 Satz 1 Nr. 4 HmbPOlDVG ohne weitere Einschränkungen zulässig.

Andere nicht seltene Fälle sind Übermittlungen an das Sozialamt wegen des Verdachts auf Sozialhilfebetrug. Wenn die Polizei z.B. im Rahmen von Ermittlungen zur Strafverfolgung feststellt, daß jemand unberechtigt Sozialhilfe bezieht, der über erhebliche andere Einkünfte verfügt, kann sie dies dem Sozialamt mitteilen. Es fehlen zwar immer noch bereichsspezifische Rechtsgrundlagen für Übermittlungen von Daten, die anläßlich der Strafverfolgung erhoben worden sind. Es besteht jedoch Übereinstimmung darüber, daß jedenfalls der Geschädigte von Straftaten, die sich gegen ihn richten, informiert werden kann. Im Falle des Sozialhilfebetrugs ist die öffentliche Hand geschädigt; Empfänger der Übermittlung ist das zuständige Sozialamt.

Voraussetzung ist allerdings, daß tatsächlich ein Ermittlungsverfahren wegen Sozialhilfebetrugs eingeleitet wird, weil hinreichende aktuelle Tatsachen für diesen Verdacht vorliegen. Ist dies nicht der Fall und bestehen nur entsprechende Vermutungen, kommt auch keine Übermittlung an andere Stellen in Betracht.

17.7.3 Übermittlungen an Private

Nicht selten beschweren sich Bürger darüber, daß eine andere Person, mit der sie einen Streit austragen, Informationen von der Polizei bekommen habe. Maßgebliches Kriterium für die Zulässigkeit derartiger Übermittlungen an Private ist in aller Regel die Frage, ob die andere Person ein rechtliches Interesse an dieser Information hatte.

Rechtliche Interessen bestehen dann, wenn der Empfänger auf die Daten zur Durchsetzung eigener Rechtsansprüche angewiesen ist. Ist dies der Fall, ist die Übermittlung durch die Polizei an die Privatperson zulässig (§ 21 Satz 1 Nr.3 HmbPolDVG), sofern die Daten keinen zusätzlichen Zweckbindungen unterliegen, wie dies z.B. für Dateispeicherungen der Fall ist (§ 21 Satz 2 HmbPolDVG).

Allerdings ist auch hier Zurückhaltung geboten. Häufig liegt die Schwierigkeit darin, daß die Polizei das Vorliegen derartiger rechtlicher Interessen nicht verbindlich feststellen kann. Entscheidend ist, ob der Polizeibeamte, der die Information weitergibt, aufgrund seinen eigenen aktuellen Feststellungen zu dem Ergebnis kommt, daß der Datenempfänger die Information zur Durchsetzung seiner Ansprüche benötigt. Bloße unüberprüfte Behauptungen, man sei geschädigt worden, reichen dagegen nicht.

Durch eigene zeitnahe polizeiliche Feststellungen müssen insbesondere auch die Daten, die weitergegeben werden, gesichert sein. Niemandem ist mit einer ungeprüften Information gedient, die sich nachher als falsch herausstellt.

Wesentlich ist auch, daß die Information einen Sachverhalt betrifft, für den die Polizei selbst zuständig ist. Liegt die Auskunft dagegen im Zuständigkeitsbereich einer anderen Behörde, kann sie nicht von der Polizei gegeben werden (z.B. Adreßauskünfte, die nur von der Meldebehörde erteilt werden).

17.8 Parlamentarischer Untersuchungsausschuß „Hamburger Polizei"

Wie bereits beim Parlamentarischen Untersuchungsausschuß (PUA) „Städtische Wohnungen" (siehe 12. TB, 12.7) ist auch beim PUA „Hamburger Polizei" umstritten, in welchem Umfang und unter welchen Voraussetzungen personenbezogene Akten vom Senat an den PUA weitergegeben werden können.

Wir haben in ausführlich begründeten Stellungnahmen gegenüber den beteiligten Behörden die Forderung erhoben, daß eine personenbezogene Aktenvorlage nur dann erfolgt, wenn zureichende Anhaltspunkte dafür vorliegen, daß Polizeibeamte tatsächlich Übergriffe begangen haben. Der Senat hat dagegen entschieden, alle Strafermittlungs- und Beschwerdeakten vorzulegen, allerdings unter den Bedingung, daß die personenbezogenen Daten grundsätzlich nur vertraulich behandelt werden. Gegen diese Bedingung hat sich der PUA gewandt, der selbst entscheiden will, welche Vorkehrungen zum Schutz des Persönlichkeitsrechts er trifft. Der Streit war bei Redaktionsschluß noch nicht ausgeräumt.

Jedenfalls hat diese Auseinandersetzung erneut deutlich gemacht, daß eine gesetzliche Regelung zum Ausgleich der Persönlichkeitsrechte der Betroffenen mit den Rechten des Parlaments überfällig ist (12. TB, 1.5.2).

18. Verfassungsschutz

18.1 Entwurf eines Hamburgischen Verfassungsschutzgesetzes

18.1.1 Beratung in der Bürgerschaft

Die parlamentarische Beratung des bereits im 12. TB (18.1) vorgestellten Entwurfes eines Hamburgischen Verfassungsschutzgesetzes erfolgte u. a. durch eine Anhörung von Sachverständigen im Innenausschuß der Bürgerschaft.

Dabei hat der Entwurf Kritik sowohl aus der Sicht der als Gutachter berufenen Amtsleiter von Verfassungsschutzbehörden als auch bei Wissenschaftlern gefunden, jeweils aus unterschiedlichen Gründen. Bewertet man die Gutachten, so zeigt sich nach Auffassung des Hamburgischen Datenschutzbeauftragten, daß mit dem vorliegenden Entwurf ein vertretbarer Mittelweg zwischen den für die Aufgabenerledigung erforderlichen Befugnissen einerseits und dem Schutz des Bürgers vor unangemessenen Eingriffen des Staates vor allem in sein Grundrecht auf informationelle Selbstbestimmung gefunden wurde.

Die wichtigsten Kritikpunkte bei der Anhörung waren die Beschränkung des Gewaltbegriffs auf die physische Gewalt, die Schutzvorschriften zugunsten von Minderjährigen und die nur beschränkt zulässige Übermittlung von Informationen des Landesamtes für Verfassungsschutz an die Polizei.

Der Begriff der „Gewalt" hat durch die Rechtsprechung zum Straftatbestand der Nötigung eine Ausdehnung erfahren, die für die Zwecke des Verfassungsschutzes ungeeignet ist. Gewalt ist danach nicht nur die physische, sondern auch die psychisch vermittelte. Deshalb können z.B. passive Sitzblockaden Gewalt im Sinne der Nötigung darstellen.

Der Begriff der Gewalt wird an verschiedenen Stellen im Entwurf des Hamburgischen Verfassungsschutzgesetzes zur Konkretisierung des Verhältnismäßigkeitsgrundsatzes als Voraussetzung für besonders intensive Eingriffe verwendet. Die beschränkende Wirkung im Sinne eines verhältnismäßigen Vorgehens kann aber nur dann erreicht werden, wenn die klar erkennbare physische Gewalt, nicht aber eine diffuse psychisch vermittelte Gewalt Eingriffsvoraussetzung ist. Von daher muß an der einschränkenden Definition des Gewaltbegriffs im Entwurf des Hamburgischen Verfassungschutzgesetzes festgehalten werden.

18.1.2 Einbeziehung des Verfassungsschutzes in die Beobachtung der organisierten Kriminalität

Ein wichtiger Punkt in der Diskussion um das neue Hamburgische Verfassungsschutzgesetz ist die Frage, ob der Verfassungsschutz befugt werden soll, nachrichtendienstliche Mittel zur Beobachtung organisierter Kriminalität einzusetzen.

Der Entwurf enthält keine derartigen Regelungen; auch in anderen Bundesländern sind entsprechende gesetzliche Vorschläge abgelehnt worden. Lediglich das Land Bayern hat in sein Verfassungsschutzgesetz derartige Vorschriften aufgenommen.

Die Diskussion hierüber hält allerdings an. Der Präsident des Bundesamtes für Verfassungsschutz hat die Forderung, die nachrichtendienstlichen Befugnisse auch auf die Kriminalitätsbekämpfung auszudehnen, u.a. in der Anhörung der Bürgerschaft zum Hamburgischen Verfassungsschutzgesetz vertreten. Zu dieser Vermischung von nachrichtendienstlichen und polizeilichen Befugnissen liegen dagegen ablehnende Stellungnahmen des Bundesministers des Innern und des Präsidenten des Bundeskriminalamtes vor. Auch die Leiter des Landesamtes für Verfassungsschutz und des Landeskriminalamtes in Hamburg haben sich eindeutig gegen diese Vorstellungen gewandt.

Aus datenschutzrechtlicher Sicht sind diese Überlegungen aus folgenden Gründen abzulehnen:

Datenerhebungen zum Zwecke der Strafverfolgung und zu Zwecken des Verfassungsschutzes verfolgen grundsätzlich unterschiedliche Ziele. Die Ausgestaltung der jeweiligen Verfahren ist daher nicht vergleichbar.

Die Datenerhebung zur Strafverfolgung ist prinzipiell offen, nur in Ausnahmefällen verdeckt. Strafverfolgung ist an das Legalitätsprinzip gebunden und unterliegt in allen Fällen der Kontrolle durch die Staatsanwaltschaft, nach Anklageerhebung durch das Gericht. Spätestens vor dem Abschluß der Ermittlungen durch die Staatsanwaltschaft wird der Beschuldigte von den über ihn erhobenen Informationen in Kenntnis gesetzt. Die weitreichenden Befugnisse zur Erhebung und weiteren Verwendung personenbezogener Daten zur Strafverfolgung werden vor allem durch die strikte Bindung an die Tatbestände des materiellen Strafrechts begrenzt.

Datenerhebung durch den Verfassungsschutz mit nachrichtendienstlichen Mitteln dient ausschließlich dem Schutz der freiheitlichen demokratischen Grundordnung sowie des Bestandes und der Sicherheit des Bundes und der Länder. Sie erfolgt in aller Regel verdeckt. Für den Verfassungsschutz gilt kein Legalitätsprinzip; er unterliegt nicht der staatsanwaltschaftlichen Verfahrensherrschaft. In aller Regel wird die Offenlegung von Erhebungsvorgängen mit den Argumenten Quellenschutz und Ausforschungsgefahr verwehrt. Damit wird nicht zuletzt auch die gerichtliche Nachprüfbarkeit erheblich eingeschränkt. Die weitreichenden Befugnisse und die Beschränkungen der rechtsstaatlichen Kontrolle sind nur dann hinnehmbar, wenn der Einsatz der Befugnisse an die besonderen Voraussetzungen der gegen die freiheitliche demokratische Grundordnung gerichteten, sicherheitsgefährdenden und gewalttätigen Bestrebungen gebunden bleibt.

Das Trennungsgebot zwischen Verfassungsschutz und Polizei ist die Konsequenz aus den historischen Erfahrungen mit der „Geheimen Staatspolizei" und hat vor dem Hintergrund der Erfahrungen mit der „Staatssicherheit" der DDR seine Aktualität behalten. Daher muß die Verwendung von Informationen, die mit Befugnissen des Verfassungsschutzes erhoben worden sind, zu Zwecken der Strafverfolgung auf eng begrenzte Ausnahmen, die mit der Aufgabenstellung des Verfassungsschutzes in unmittelbarem Zusammenhang stehen, beschränkt bleiben. Dies sind herkömmlich die sogenannten Staatsschutzdelikte (§§ 74a, 120 Gerichtsverfassungsgesetz).

Eine Erweiterung auf Delikte etwa im Zusammenhang mit der organisierten Kriminalität würde nicht nur die unterschiedlichen Aufgaben der Strafverfolgung und des Verfassungsschutzes vermischen, sondern auch die für die jeweiligen Tätigkeiten bestehenden Grenzen aufheben. Wenn nicht mehr klar abgrenzbar ist, bei welchen Voraussetzungen (Verdacht auf Verstoß gegen Straftatbestand oder Anhaltspunkte für verfassungsschutzrelevante Bestrebungen) die jeweilige Tätigkeit einsetzt, verlieren auch die spezifischen ver-

fahrensmäßigen und datenschutzrechtlichen Schutzvorkehrungen ihre Wirkung.

18.1.3 Datenübermittlungen des Verfassungsschutzes an die Strafverfolgungsbehörden

In diesem Zusammenhang ist auch der Änderungsvorschlag zu erwähnen, der in den bürgerschaftlichen Beratungen zum Hamburgischen Verfassungsschutzgesetz gestellt worden ist. Durch Änderung von § 14 Abs. 2 des Gesetzentwurfs soll das Landesamt für Verfassungsschutz künftig personenbezogene Daten auch dann an die Staatsanwaltschaft und die Polizei übermitteln dürfen, wenn jemand eine in § 100 a Nrn. 3 und 4 Strafprozeßordnung genannte Straftat plant, begeht oder begangen hat.

In der Begründung zu dem Änderungsvorschlag heißt es, daß dem Landesamt auch die Möglichkeit eingeräumt werden sollte, seine Erkenntnisse zur Abwehr von erheblichen Gefahren für Leib und Leben von Personen oder für hohe Sachwerte sowie zur Verfolgung anderer besonders schwerer Straftaten an die Strafverfolgungsbehörden zu übermitteln. Als Beispiele werden insbesondere die Delikte aus dem Rauschgift- bzw. Drogen- und dem Waffenhandel erwähnt.

Nach dem Wortlaut des Änderungsvorschlags und der Begründung soll diese Übermittlungsmöglichkeit für das Landesamt unabhängig davon bestehen, ob bei den personenbezogenen Daten irgendein Zusammenhang mit Verfassungsschutzangelegenheiten vorhanden ist. Es könnte sich demnach auch um reine Zufallsfunde des Landesamts handeln, die bisher nicht weitergegeben werden konnten.

Die amtliche Begründung zum Senatsentwurf besagt dazu zutreffend, daß sich das Landesamt bei der Weitergabe „auf die Daten beschränken muß, die zur Verfolgung oder Verhinderung von Staatsschutzdelikten erforderlich sind."

Die Datenschutzbeauftragten des Bundes und der Länder haben im September 1994 einstimmig mit Besorgnis Entwicklungen festgestellt, die die klare Trennungslinie zwischen Nachrichtendiensten und Polizeibehörden weiter zu verwischen drohen. Sie haben gefordert, daß für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung das Trennungsgebot strikt beachtet wird.

Bedenklich wäre eine derart weitgehende Übermittlung durch das Landesamt insbesondere dann, wenn es seine Kenntnisse durch Einsatz nachrichtendienstlicher Mittel erhalten hat. Soweit die Kenntnisse auf Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses beruhen, dürfen sie kraft vorrangiger bundesgesetzlicher Regelung nach § 7 des Gesetzes zu Artikel 10 Grundgesetz (G 10) ohnehin nur dann weitergegeben werden, wenn es sich um eine der in § 2 dieses Gesetzes genannten Handlungen oder aber um eine in § 138 Strafgesetzbuch genannte schwere Straftat handelt.

Damit wird zugleich die verfassungs- und datenschutzkonforme Lösung zur Frage der zulässigen Übermittlungen an die Strafverfolgungsbehörden aufgezeigt. Nicht nur im Falle des G 10, sondern in allen Fällen wäre die Übermittlungsbefugnis des Landesamtes auf den Katalog der Straftaten nach § 138 Strafgesetzbuch zu beschränken, der in seiner aktualisierten Form bereits eine Vielzahl schwerer Delikte umfaßt.

Ich habe diese datenschutzrechtlichen Bedenken dem bürgerschaftlichen Innenausschuß zur Kenntnis gegeben. Der Ausschuß hat den Gesetzentwurf erst nach dem Redaktionsschluß für diesen TB weiter beraten.

18.2 Sicherheitsüberprüfungsgesetz

Bei einer Sicherheitsüberprüfung wird nicht nur anhand der Karteien von Polizei und Verfassungsschutz festgestellt, ob z.B. bei einem Mitarbeiter ein Sicherheitsrisiko vorliegen könnte. Vielmehr wird in Abhängigkeit von der Sensibilität der zu übertragenden Aufgabe auch das private Umfeld des Mitarbeiters ausgeforscht. Derartig intensive Eingriffe in das Grundrecht auf informationelle Selbstbestimmung bedürfen einer bereichsspezifischen Rechtsgrundlage.

Die Sicherheitsüberprüfung durch Bundesbehörden ist zwischenzeitlich durch ein Gesetz geregelt worden. Für die Sicherheitsüberprüfungen bei Stellen in Hamburg fehlt bisher ein solches Gesetz; es liegt nicht einmal ein Entwurf vor.

18.3 Querschnittsprüfung des Landesamtes für Verfassungsschutz mit Referatsarbeitskartei (RAK)

Bei dem Landesamt für Verfassungsschutz wurde 1994 eine Querschnittsprüfung durchgeführt. Ziel dieser Prüfung war es, das Zusammenwirken der verschiedenen Teile des Landesamtes für Verfassungsschutz und die Einbeziehung der elektronischen Datenverarbeitung datenschutzrechtlich zu prüfen.

Hierzu wurden verschiedene Arbeitsplätze geprüft, die sich mit der Beschaffung, der Auswertung sowie der Speicherung und Aufbewahrung von Informationen befassen. Die Arbeitsplätze wurden überwiegend unangemeldet aufgesucht und die dateiförmige und manuelle Verarbeitung von personenbezogenen Daten überprüft.

Dabei wurden angesichts der Vielzahl von Dateien zunächst systematisch alle in den jeweiligen EDV – Verzeichnissen enthaltenen Dateien kursorisch geprüft. Ergaben sich hierbei Anhaltspunkte für datenschutzrechtlich zweifelhafte Vorgehensweisen, wurden Stichproben gezogen und die der jeweiligen Speicherung zugrundeliegenden Informationen eingesehen. Bestätigten die Stichproben datenschutzrechtlich zweifelhafte Vorgehensweisen, wurde die Stichprobe bis zur vollständigen Revision der Dateiinhalte ausgeweitet. Die an den Arbeitsplätzen vorhandenen Akten und Karteien wurden in die Prüfung mit einbezogen, einschließlich der Registratur.

Aus der Vielzahl von Einzelfeststellungen wurden dann für bestimmte Abläufe typische Fälle im Prüfbericht dargestellt und einer Bewertung unterzogen. Der Prüfbericht enthält eine Reihe von Forderungen, die hier aus Geheimhaltungsgründen nicht aufgelistet werden können; zum Teil soll die Thematik im bürgerschaftlichen Kontrollausschuß für den Verfassungsschutz weiter erörtert werden. Ausgewählte Fragestellungen ergeben sich aus den folgenden Darstellungen.

Mit der Einführung des Automationsprojektes RAK und des neuen Bürokommunikationssystems befindet sich das Landesamt in einer schwierigen Umstellungsphase. Fast alle Informationen, die nunmehr in der RAK auf EDV erfaßt sind, wurden vorher in einer personenbezogenen Handkartei festgehalten, die nicht weiter differenzierbar ist. Demgegenüber sind die Informationen jetzt in kürzester Frist mit einer personen- und sachbezogenen Volltextrecherche suchfähig.

Mit dem neuen EDV-Projekt und zugleich der Anwendung des Hamburgischen Verfassungsschutzgesetzentwurfs (18.1) sind wesentlich weitergehende datenschutzrechtliche Anforderungen als bisher zu erfüllen. Jede personenbezogene Speicherung in der RAK oder in Indizes (siehe 18.3.4) hat sich an den Voraussetzungen der §§ 7 ff. des Gesetzentwurfs zu orientieren.

Differenzen hat es vor allem über die Aussagefähigkeit des jeweils ersten Erkenntnistextes gegeben, der bei dem bisherigen System über eine Person festgestellt wurde. Die datenschutzrechtlichen Risiken bestanden bereits bei der Handkartei, wenn auch mit begrenzten Auswirkungen. Bei einer automatisierten Datei mit der erwähnten Suchfähigkeit müssen aber auf jeden Fall eindeutige und einheitliche Kriterien für diesen ersten Erkenntnistext bestehen.

Mit dem Landesamt besteht Einvernehmen, daß der erste Erkenntnistext eine klare inhaltliche Begründung für die Speicherung beinhalten muß, die eine rechtliche Subsumtion des Sachverhaltes eindeutig erkennbar werden läßt. Darüber hinaus muß der Sachverhalt, der der Speicherung zugrunde liegt, aus den Akten ersichtlich sein.

Bei den Beratungen zum Entwurf des Hamburgischen Verfassungsschutzgesetzes im bürgerschaftlichen Innenausschuß habe ich in diesem Sinne erklärt, daß für die Speicherung in automatisierten Dateien eine klare Standardisierung mit vorgegebenen Formulierungen über die Zuordnung zu den einzelnen Kategorien notwendig ist, die von der Amtsleitung etwa in Form einer Dienstvorschrift festzulegen ist. Dies gilt für jede Erstspeicherung, aber auch als Grundlage für jede Wiederholungsprüfung, um eindeutig feststellen zu können, in welche rechtliche Kategorie die gespeicherte Person einzuordnen ist. Wegen der unterschiedlichen rechtlichen Voraussetzungen und Folgen ist dies z.B. wichtig für die Unterscheidung zwischen Personen, die selbst zu einer verfassungsschutzrelevanten Bestrebung gehören, und anderen Personen wie z.B. Begleit- und Kontaktpersonen.

Datenschutzrechtlich bedenklich ist insbesondere der Umstand, daß der interne Datenschutzbeauftragte, der Systemabfragen z.B. für die Erteilung von Auskünften an Bürger durchführt, aufgrund technischer Gegebenheiten nicht sicher sagen kann, ob eine Person gespeichert ist oder nicht.

18.3.1 Stand des Automationsprojektes RAK

Die im 11. TB (18.3) sowie im 12. TB (18.3.2) dargestellten Probleme hinsichtlich der Sicherheitskomponenten wurden Anfang 1994 durch den Einsatz zusätzlicher Sicherheitssoftware sowohl auf Seiten der PC als auch des Servers gelöst. Dazu wurde an verschiedenen Programmkomponenten eine Neuprogrammierung vorgenommen und dabei eine Reihe von datenschutzrechtlichen Anforderungen, aber auch Änderungen in den Anforderungen durch die Anwender, einbezogen.

Bei der Querschnittsprüfung wurden verschiedene Mängel festgestellt, die in einer neuen Version, die gegen Ende 1994 installiert werden soll, z. T. beseitigt werden sollen. Eine spätere technische Prüfung wird zeigen, ob die Anforderungen des Hamburgischen Datenschutzbeauftragten – über die inhaltlich mit dem Landesamt für Verfassungsschutz keine Differenzen bestehen – als erfüllt angesehen werden können.

Die derzeitige Softwareausstattung des Landesamtes verbindet die Möglichkeiten der (traditionellen) feldorientierten Suche auf der Basis einer Datenbank mit der Möglichkeit der Volltextrecherche über alle Dokumente des Landesamtes hinweg. Diese überragenden Suchmöglichkeiten haben datenschutzrechtlich eine Reihe von Konsequenzen; die wesentlichen sind in den Ziffern 18.3.3, 18.3.4 und 18.3.6 dargestellt.

18.3.2 Speicherung personenbezogener Daten

Das datenschutzrechtlich völlig unzureichende, derzeit gültige Hamburgische Verfassungsschutzgesetz enthält im wesentlichen – was die Voraussetzungen für die Speicherung von personenbezogenen Daten betrifft – nur Generalklauseln. Damit dieses Gesetz unter Berücksichtigung des ablaufenden Übergangsbonus zur Anwendung kommen kann, muß es verfassungskonform ausgelegt werden. Zwischen dem Hamburgischen Datenschutzbeauftragten und dem Landesamt für Verfassungsschutz wurde der Entwurf eines Hamburgischen Verfassungsschutzgesetzes vom 20.April 1993 (Bürgerschaftsdrucksache 14/3940) als eine verfassungskonforme Konkretisierung der Generalklauseln bewertet und als Prüfungsmaßstab übereinstimmend zugrundegelegt.

Im Zusammenhang mit der Prüfung wurde auch die Frage erörtert, wie das Landesamt für Verfassungsschutz bei der Speicherung von Familienangehöri-

gen verfährt. Das Landesamt geht davon aus, daß Familienangehörige bei der Beobachtung terroristischer Aktivitäten eine begleitende Rolle spielen können, aber nicht müssen. Deshalb würde das familiäre Umfeld dieser Personen nicht automatisch in die Beobachtung des Amtes miteinbezogen. Familienangehörige werden dann gespeichert, wenn sie Träger von Bestrebungen nach § 4 Abs. 1 des Gesetzentwurfs sind oder zur Bewertung gewalttätiger Bestrebungen oder geheimdienstlicher Tätigkeiten nach § 9 Abs. 1 Satz 1 Nr. 2 des Gesetzentwurfs in Betracht kommen.

Außerdem wurde die Frage erörtert, welche Anforderungen das Landesamt für Verfassungsschutz an die Speicherung von Personen stellt, die lediglich einen beruflichen Kontakt zu gespeicherten Personen haben. Das Landesamt hat darauf hingewiesen, daß keine Speicherung allein aufgrund der beruflichen Tätigkeit erfolge. Maßgeblich sind vielmehr die Erkenntnisse und der dahinter liegende Sachverhalt im Rahmen der Beobachtung von verfassungsschutzrelevanten Bestrebungen. Es gelten dieselben Maßstäbe, die hinsichtlich der Familienangehörigen wiedergegeben wurden.

Schwierigkeiten bei der Speicherung von Unorganisierten beruhen nach unserem Eindruck darauf, daß die vorhandene Verkartungsanweisung keinen für alle Mitarbeiter nachvollziehbaren Kriterienkatalog dafür enthält, wann eine Person verfassungsschutzrelevante Ziele in diesem Bereich verfolgt und wann nicht. Je nach Sachbearbeiter und Bereich existieren unterschiedliche Kriterien, die insgesamt keinen stimmigen Eindruck zu erwecken vermochten. Nach Angaben des Landesamtes muß der Sachbearbeiter den jeweiligen Gesamtsachverhalt würdigen und danach über die Speicherung entscheiden. Nach Auffassung des Hamburgischen Datenschutzbeauftragten ist hier jedoch eine Überarbeitung und Präzision der Dienstanweisung erforderlich und möglich.

Weiterhin wurde eine Reihe von Fällen – teilweise Erstspeicherungen aus jüngster Zeit – festgestellt, in denen Personen mit Formulierungen eingespeichert worden waren, die keinerlei Anhaltspunkte für verfassungsschutzrelevantes Verhalten enthielten. Die verbreitete Arbeitsweise, sich bei der Speicherung die Zuordnung zu einer der gesetzlich vorbestimmten Kategorien für die jeweilige Person zunächst noch offen zu halten, ist nicht zulässig. Die vorgeschriebene Verfahrensweise, die eine klare Zuordnung bei Ersteinspeicherung sicherstellen soll, wurde teilweise nicht beachtet.

In weiteren Fällen wurde festgestellt, daß der zu einer Person gespeicherte Text zwar verfassungsschutzrelevante Inhalte aufwies, die sich aber aus den zugrundeliegenden Vorgängen nicht oder nicht so entnehmen ließen. Auch konnte das Landesamt für Verfassungsschutz in Einzelfällen nicht angeben, woher eine entsprechende Information stammte, und insoweit nur Vermutungen äußern. Teilweise konnte die Herkunft der Information nachträglich rekonstruiert werden, teilweise jedoch nicht.

18.3.3 Volltextrecherche und Drittpersonen

Für die Beantwortung der Frage, wann eine Person im EDV-System des Landesamtes für Verfassungsschutz gespeichert ist, müssen die überragenden Suchmöglichkeiten des Systems berücksichtigt werden.

Jeder Mitarbeiter in der Auswertung des Landesamtes für Verfassungsschutz ist in der Lage, nach jedem Begriff – sei es ein Ort oder auch ein Name – sowohl in der Datenbank als auch in jedem Textdokument zu suchen, soweit er die dazu erforderlichen Zugriffsrechte hat. Damit ist jede Person, die im EDV – System z.B. auch in der Textverarbeitung gespeichert ist, als suchfähig gespeichert zu bewerten.

Diese Abfragemöglichkeit bedeutet, daß z.B. eine Person, bei der beobachtete Personen regelmäßig einkaufen – wie zum Beispiel ein Bäcker – aufgrund der Möglichkeiten des Systems namentlich suchfähig würde, während die Bäckerei eigentlich nur als Objekt feststellbar sein soll. Die personenbezogene Speicherung wäre aber unabhängig davon möglich, ob diese Person in irgendeiner Weise verfassungsschutzrelevant tätig wird.

Nach längerer Diskussion hat das Landesamt für Verfassungsschutz die Forderung des Hamburgischen Datenschutzbeauftragten akzeptiert, daß jede Person, die mit Volltextrecherche suchfähig gespeichert ist, selbst die gesetzlichen Voraussetzungen für eine Speicherung erfüllen muß, also verfassungsschutzrelevant tätig geworden sein muß. Dies gilt nicht, soweit der administrative Bereich des Landesamtes, z.B. hinsichtlich Verwaltungsdateien mit Personenangaben von Mitarbeitern, berührt ist.

Als „ Drittperson" werden nur diejenigen Personen bezeichnet, die zwar suchfähig z. B. in Texten oder Indizes gespeichert sind, jedoch in der RAK (zunächst) keinen eigenen Datensatz haben. Bei diesen Personen ist zu prüfen, ob sie die gesetzlichen Voraussetzungen für eine Speicherung erfüllen oder nicht. Erfüllt eine Drittperson die gesetzlichen Voraussetzungen, ist über sie ein eigener Datensatz anzulegen; anderenfalls ist sie zu löschen.

Zur Zeit ist aber noch eine Vielzahl von Personen suchfähig gespeichert, die keinen eigenen Datensatz haben. Diese werden auch nicht in den Zahlen berücksichtigt, die das Landesamt für Verfassungsschutz über die bei ihm gespeicherten Personen veröffentlicht. Die veröffentlichten Zahlenangaben betreffen nur die in der RAK enthaltenen Datensätze.

Das Landesamt für Verfassungsschutz hat auf die Forderung des Hamburgischen Datenschutzbeauftragten hin veranlaßt, daß alle bisher im System suchfähig gespeicherten Namen daraufhin geprüft werden, ob sie einen eigenen Datensatz haben. Die Personen erhalten dann nach den oben erwähnten Kriterien ggf. einen eigenen Datensatz; anderenfalls werden die Namen gelöscht.

Die Bereinigung der Datenbestände wird – die bisherige Vorgehensweise hochgerechnet – noch ca. 2 Jahre andauern.

18.3.4 Verhältnis Index – RAK

Das Landesamt für Verfassungsschutz hatte traditionell neben der an Personen orientierten RAK noch an Organisationen oder Ereignissen orientierte Indizes. Dort wurden – überwiegend entlang der Zeitachse – die Erkenntnisse des Amtes zu Organisationen oder Ereignissen fortgeschrieben. Diese beiden Formen der Aufbereitung von Erkenntnissen wurden unverändert auf dem neuen EDV – System abgebildet.

Die neuen Suchmöglichkeiten führen nun dazu, daß sich durch eine geschickte Abfragestrategie aus der personenorientierten RAK organisationsbezogene Erkenntnisse gewinnen lassen und umgekehrt. Hinsichtlich der personbezogenen Daten bedeutet dies, daß eine Person, die im Index erwähnt ist, suchfähig gespeichert ist und damit auch in der RAK mit einem eigenen Datensatz gespeichert sein müßte (Parallelität der Speicherungen, Drittperson). Dies ist nach den Ergebnissen der Prüfung häufig noch nicht der Fall. Der Hamburgische Datenschutzbeauftragte hat das Landesamt aufgefordert, die Parallelität der Speicherungen sicherzustellen.

18.3.5 Übermittlung von Daten an andere Dienste

Bei der Querschnittsprüfung wurde u.a. auch die Übermittlungspraxis an andere Dienste einer Überprüfung unterzogen.

Entsprechend den gesetzlichen Bestimmungen hat das Landesamt für Verfassungsschutz z.B. an das Bundesamt für Verfassungsschutz die für die Aufgabenerfüllung erforderlichen Daten zu übermitteln. Bei der Prüfung wurde festgestellt, daß z.B. bei der Übersendung von Berichten mit personenbezogenen Angaben über verschiedene Personen häufig keine Prüfung der Erforderlichkeit mit einer gegebenfalls notwendigen Teilanonymisierung erfolgt. Vielmehr wird schon dann, wenn eine einzige (Teil-) Information des Berichtes von Interesse für einen anderen Dienst ist, der gesamte Bericht übersandt . Hier wurde das Landesamt aufgefordert, Vorkehrungen dafür zu treffen, daß nicht erforderliche personenbezogene Daten auch nicht übermittelt werden.

Demgegenüber vertritt das Landesamt die Auffassung, daß es seine Informationen umfassend im inhaltlichen und personellen Kontext jeweils an das Bundesamt für Verfassungsschutz bzw. die anderen Landesämter für Verfassungsschutz zu übermitteln hat. Erst die Auswertung von Informationen mit dem Gesamtsachverhalt aus dem Gesamtkontext ermögliche eine sachgerechte und wirklichkeitsnahe Betrachtung, die auch den Belangen von Betroffenen gerecht werde. Eine teilweise Übermittlung der Informationen würde nicht der Gemeinschaftsaufgabe Verfassungsschutz von Bund und Ländern

entsprechen. Die Prüfung der Erforderlichkeit unter Berücksichtigung der Pflicht zur Zusammenarbeit führe zur umfassenden Informationsmitteilung gemäß dem gesetzlichen Auftrag für den Verfassungsschutz.

Diese grundsätzliche Frage, ob die datenschutzrechtliche Prüfung der Erforderlichkeit wegen der Besonderheiten der Verfassungsschutzaufgabe bei der Übermittlung an andere Verfassungsschutzämter praktisch entfällt, bedarf weiterer Klärung. Dabei ist es durchaus vorstellbar, daß Gesamtsachverhalte weitergegeben werden und dabei über die Personen, die für das andere Verfassungsschutzamt nicht relevant sind, nur anonymisiert berichtet wird.

Bisher gibt es jedenfalls kein anderes Fachgebiet, bei dem aus der Besonderheit der Sachaufgabe heraus eine ausnahmslos personenbezogene Übermittlung anerkannt ist.

18.3.6 Protokollierung von Abfragen

Ein weiteres Problem besteht in der Protokollierung der Abfragen, die Mitarbeiter des Landesamtes für Verfassungsschutz im EDV – System durchführen. Zwar wurde aufgrund der Forderungen des Hamburgischen Datenschutzbeauftragten ein mehrstufiges Protokollsystem installiert. Allerdings wurde festgestellt, daß die Protokollierung zum Teil nur vom System selbst vergebene Dateinamen verwendet.

Aus diesem Dateinamen läßt sich der vom Benutzer vergebene Dateiname nur so lange ersehen, wie eine eindeutige Zuordnung eines Systemnamens zu einem Benutzernamen existiert. Werden Dateinamen gelöscht, ist eine solche Zuordnung nicht mehr möglich; die Protokollierung geht dann ins Leere und kann ihren Zweck nicht mehr erfüllen.

Hier ist die Protokollierung ohne Personenbezug so auszugestalten, daß der jeweilige Zugriff auf Dateien nachvollziehbar bleibt. Die Vorstellung des Landesamtes, nach der Löschung der Datei keine personenbezogenen Daten mehr in den Protokolldateien erscheinen zu lassen, wird von uns geteilt.

18.4 Fernmeldeaufklärung des Bundesnachrichtendienstes

Die Diskussion über die Einbeziehung von Nachrichtendiensten in die Verfolgung von Straftaten insbesondere im Bereich der organisierten Kriminalität betrifft nicht allein die Erweiterung von Befugnissen des Verfassungsschutzes (siehe oben 18.1.2). Kurz vor Ende der letzten Legislaturperiode des Deutschen Bundestages ist das Verbrechensbekämpfungsgesetz verabschiedet worden. Neben anderen problematischen Neuerungen (siehe unten 19.1.1) sieht es eine Erweiterung der Befugnisse des Bundesnachrichtendienstes (BND) zur Verbrechensbekämpfung vor. Der BND wird im Zuständigkeitsbereich der Länder nicht tätig; dennoch ist eine Auseinandersetzung mit dieser Neuregelung auch aus Landessicht erforderlich, weil sie die Problematik der

Einbeziehung von Nachrichtendiensten in die Strafverfolgung deutlich macht und weil sich die Neuregelung auf die Strafverfolgungsbehörden der Länder auswirkt.

Gemeinsam mit anderen Landesbeauftragten für den Datenschutz haben wir starke Bedenken gegen die Erweiterung der Befugnisse des BND geltend gemacht.

Der BND hat die gesetzliche Aufgabe, Erkenntnisse über das Ausland zu sammeln, die von außen- und sicherheitspolitischer Bedeutung sind (§ 1 Abs. 2 BND-Gesetz). Der Begriff der außen- und sicherheitspolitischen Bedeutung ist bereits in der Vergangenheit im Zusammenhang mit den Befugnissen des BND nach § 3 des Gesetzes zu Artikel 10 Grundgesetz (G 10) erweiternd ausgelegt worden. Von außen- und sicherheitspolitischer Bedeutung sollen nicht nur die in § 3 G 10 bislang ausdrücklich erwähnte militärische Bedrohung, sondern auch andere Aktivitäten sein, wenn sie für die Sicherheit und den Bestand der Bundesrepublik Deutschland als Ganzes eine ernste Gefahr darstellen können.

Bei der vom BND zur Abwehr der Gefahr eines bewaffneten Angriffs bisher praktizierten Fernmeldeaufklärung nach dem G 10 ist aus datenschutzrechtlicher Sicht von zentraler Bedeutung, daß keine Begrenzung auf bestimmte Personengruppen erfolgt. Vielmehr werden – anders als bei zielgerichteten Maßnahmen der technischen Überwachung zur Strafverfolgung – in der Art einer Rasterfahndung ohne Vorliegen eines Anfangsverdachts unvermeidlich in großer Zahl Unbeteiligte in Abhörmaßnahmen mit einbezogen.

Damit wird in großem Umfang in das Fernmeldegeheimnis eingegriffen, das nicht nur durch Art. 10 GG, sondern auch international durch Art. 8 der Europäischen Menschenrechtskonvention und Art. 17 des Internationalen Paktes über bürgerliche Rechte besonders geschützt ist.

Die Neuregelungen des Verbrechensbekämpfungsgesetzes führen nunmehr zu einer Erweiterung dieser Befugnisse nach dem G 10 insbesondere auf die Einfuhr von Drogen, die internationale Geldfälschung und damit zusammenhängende Geldwäsche, obwohl die Vergleichbarkeit der hierdurch hervorgerufenen Gefährdungen mit der Gefahr eines militärischen Angriffs zweifelhaft ist.

Damit wirkt der BND – ohne ausdrückliche Änderung seiner Aufgaben – faktisch auch bei der Verbrechensbekämpfung mit, indem er die von ihm erhobenen personenbezogenen Daten an Strafverfolgungsbehörden übermitteln darf.

Der Gesetzgeber hat diese Bedenken nicht berücksichtigt. Er hat die geforderte Klarstellung unterlassen, daß nur Zufallserkenntnisse über die in § 3 G 10 neu genannten Straftatbestände an die für die Verfolgung zuständigen Behörden übermittelt werden dürfen. Auch ein Richtervorbehalt für die Weitergabe der Erkenntnisse ist nicht vorgesehen.

Wir haben den Bundesbeauftragten für den Datenschutz unterstützt, der verstärkte datenschutzrechtliche Kontrollen im G 10-Bereich gefordert hat. Bisher ist es jedoch bei der Einschränkung der Kontrollkompetenz des Bundesbeauftragten geblieben, so daß die Forderung in der neuen Legislaturperode bestehen bleibt.

Das gesamte Verfahren der Fernmeldeaufklärung muß transparenter ablaufen. Daher ist eine wirksame Öffentlichkeitsunterrichtung anzustreben.

19. Justiz

19.1 Rechtsgrundlagen für die Datenverarbeitung im Strafverfahren

19.1.1 Zentrales staatsanwaltschaftliches Verfahrensregister

Die öffentliche Diskussion um das Verbrechensbekämpfungsgesetz hat sich im wesentlichen auf die Erweiterung der Befugnisse des Bundesnachrichtendienstes bei der internationalen Fernmeldeaufklärung konzentriert (vgl. 18.4).

Wenig öffentliche Beachtung hat dagegen eine weitere Neuregelung durch das Verbrechensbekämpfungsgesetz erfahren: Am 1. Dezember 1994 sind die Vorschriften im Achten Buch der Strafprozeßordnung (§§ 473 bis 477) in Kraft getreten. Danach wird beim Bundeszentralregister in Berlin ein zentrales staatsanwaltschaftlichen Verfahrensregister geführt. Es wird Personendaten sämtlicher Beschuldigter in allen Strafverfahren mit Angaben zur zuständigen Staatsanwaltschaft, zu Tatzeiten und Tatvorwürfen, zur Einleitung des Strafverfahrens sowie der Verfahrenserledigung bei der Staatsanwaltschaft oder bei Gericht enthalten.

Dies bedeutet, daß im Unterschied zu den bisherigen nur örtlich oder regional betriebenen staatsanwaltschaftlichen Verfahrensdateien alle Personen, gegen die ein Strafverfahren gleich welcher Art geführt wurde, an einer zentralen Stelle erfaßt werden. Alle Staatsanwaltschaften werden zu Direktabrufen im automatisierten Verfahren berechtigt. Auskünfte ohne Online-Berechtigung erhalten daneben die Polizeien zur Strafverfolgung und die Nachrichtendienste.

Wir haben im Gesetzgebungsverfahren massive Bedenken gegen die Einführung dieses Registers vorgebracht und darauf hingewiesen, daß der hiermit verbundene Eingriff in die Rechte der Betroffenen in keinem Verhältnis zum Interesse an einer wirksamen Strafverfolgung steht.

Es ist insbesondere nicht erkennbar, welche zwingenden Erfordernisse für eine zentralisierte Speicherung sämtlicher Daten über Strafermittlungsverfahren sprechen. Dies gilt insbesondere für unbegründete Strafanzeigen, für Fahrlässigkeitsdelikte und für Straftaten ohne überörtliche Bedeutung. Verdachtsfälle von Gewicht und überörtlicher Bedeutung speichert die Polizei im bundesweiten polizeilichen Informationssystem (INPOL). Diese Informationen stehen

somit zur Strafverfolgung neben den im Bundes- bzw. Verkehrszentralregister erfaßten rechtskräftigen Entscheidungen und Verurteilungen zur Verfügung.

Abgesehen von diesen grundsätzlichen Einwänden sind einzelne vorgesehene Vorschriften unakzeptabel:

Es ist vorgesehen, daß die Daten auch nach Einstellung eines Verfahrens ohne Restverdacht oder Freispruch noch zwei Jahre weiter gespeichert werden. Wenn durch rechtskräftigen Freispruch der Verbrauch der Strafklage eingetreten ist oder die Staatsanwaltschaft entscheidet, daß der ursprünglich Beschuldigte nicht als Täter in Betracht kommt, oder sein Verhalten gar nicht strafbar war, kann es keine überwiegenden Gründe geben, die eine jahrelange bundesweite Weiterspeicherung rechtfertigen. Ein überwiegendes Interesse der Allgemeinheit an der zentralen Erfassung derartiger Fälle ist schlechthin nicht erkennbar.

Hinzu kommt, daß jede weitere Speicherung die Löschung aufschieben soll. Jeder willkürliche Anzeigenerstatter hat es damit in der Hand, die grundlose, dauernde und bundesweit verfügbare Speicherung jeder denkbaren Person zu bewirken.

Diese Bedenken sind von der Justizbehörde nicht berücksichtigt worden, die im Gesetzgebungsverfahren keine Einwände gegen diese Regelungen vorgebracht hat. Dies ist auch deshalb unverständlich, weil die Staatsanwaltschaft Hamburg derzeit keinesfalls in der Lage ist, die gesetzlichen Pflichten, die sich aus diesen Regelungen ergeben, zu erfüllen:

Der Datensatz für das zentrale staatsanwaltschaftliche Verfahrensregister sieht mehr Einzelangaben vor, als zur Zeit in der Zentralkartei der Staatsanwaltschaft Hamburg gespeichert werden (Tatzeiten, Tatvorwürfe mit näherer Bezeichnung; Verfahrensverlauf bei Staatsanwaltschaft und Gericht). Der Staatsanwaltschaft fehlt also nach dem derzeitigen Sachstand eine wesentliche Grundlage, um ihre Übermittlungen an das Register vornehmen zu können. Die Daten des zentralen Registers sind laufend zu aktualisieren (§ 474 Abs. 3; § 476 Abs. 1 StPO), wofür die zuständige Staatsanwaltschaft die Verantwortung trägt. Die Staatsanwaltschaft Hamburg ist jedoch zur Zeit nicht einmal in der Lage, die Aktualisierungen in ihrer eigenen Zentralkartei vorzunehmen (siehe 19.2.2)

Wenn demnächst beim Bundeszentralregister die technischen Voraussetzungen für das zentrale staatsanwaltschaftliche Verfahrensregister geschaffen werden und der Echtbetrieb beginnt, gerät die Staatsanwaltschaft Hamburg in Bezug auf das zentrale Verfahrensregister sofort in eine gesetzwidrige Situation, wenn nicht zuvor die bei der Zentralkartei Hamburg bestehenden Mängel bereinigt werden. Die dann eintretende massenhafte Verletzung von Rechten der Betroffenen wäre ebenso wenig hinnehmbar, wie jetzt bei der eigenen Zentralkartei.

19.1.2 Entwurf für ein Strafverfahrensänderungsgesetz 1994

Nicht allein die Einführung des zentralen staatsanwaltschaftlichen Verfahrensregisters ruft Gefahren für die Wahrung des Grundrechts auf Datenschutz im Strafverfahren hervor, sondern auch gesetzgeberische Vorschläge zur Regelung des Umgangs mit personenbezogenen Daten im Strafverfahren.

Seit Jahren ist eine gesetzliche Grundlage für die Verarbeitung personenbezogener Daten im Strafverfahren, die den Geboten der Normenklarheit und Verhältnismäßigkeit entspricht, überfällig (vgl. 8.TB, 3.10.1). Der Entwurf des Bundes für ein Strafverfahrensänderungsgesetz (StVÄG) ist seit 1990 nicht über das Referentenstadium hinausgelangt. In dieser Situation haben die Länder Bayern, Hessen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland und Thüringen im Bundesrat den Entwurf eines Strafverfahrensänderungsgesetzes (StVÄG 1994) eingebracht, der auch vom Bundesrat beschlossen worden ist.

Dieser Gesetzentwurf stellt den Tiefstand aller bisherigen Versuche dar, bereichsspezifische Grundlagen für die Datenverarbeitung im Strafverfahren zu schaffen.

Wir haben gegenüber der Justizbehörde mehrfach deutlich gemacht, daß der Entwurf den vom Bundesverfassungsgericht vor mehr als 10 Jahren im Volkszählungsurteil aufgestellten Maßstäben der Verhältnismäßigkeit und Normenklarheit, an denen sich alle gesetzesförmigen Eingriffe in das Grundrecht auf Datenschutz zu messen haben, in keiner Hinsicht gerecht wird.

Der Entwurf fällt weit hinter den Standard der allgemeinen Datenschutzgesetze und sogar der Polizeigesetze der Länder zurück. Er dient erkennbar nur dem Ziel, bestehende EDV-Systeme einzelner Bundesländer und überkommene Arbeitsweisen der Justiz formal abzusichern.

Den gesamten Gesetzentwurf prägt der Gedanke: Der Schutz der Persönlichkeitsrechte der am Strafverfahren Beteiligten ist aufwendig und störend, so daß er auf ein Minimum beschränkt werden soll.

Wird der Entwurf unverändert Gesetz, müssen Verdächtige ebenso wie Verbrechensopfer, Tatzeugen und Unbeteiligte damit rechnen, daß Daten über ihre Person aus Strafakten nicht nur an andere Rechtspflegeorgane, sondern an viele andere Behörden weitergegeben werden können. Es wird verkannt, daß die Aufgabenstellung einer anderen Behörde nicht pauschal die Auskunft aus und insbesondere nicht die Einsicht in Strafverfahrensakten rechtfertigen kann. Strafverfahrensakten haben Inhalte, die nur aufgrund der besonderen Befugnisse der Strafverfolgungsbehörden z.B. unter Zeugenzwang erhoben werden dürfen. Diese Erhebungsbefugnisse stehen anderen Aktenauskunft oder -einsicht begehrenden Behörden jedoch nicht zu.

So sind wir z.B. durch eine Eingabe darauf aufmerksam gemacht worden, daß die Staatsanwaltschaft vollständige Strafakten unverschlossen an die Landes-

hauptkasse übersandt hat, obwohl es allein um Nachfragen zum Eintreiben einer Forderung ging, für die der gesamte Akteninhalt gar keine Bedeutung hatte. Die Staatsanwaltschaft hat uns mitgeteilt, daß diese Praxis abgestellt werde und eine entsprechende Dienstanweisung ergangen sei.

Derartige Dienstanweisungen wären verzichtbar, wenn klare gesetzliche Regelungen bestünden. Diese müßten Aktenauskünfte und -übersendungen davon abhängig machen, ob die ersuchende Behörde die Akteninhalte auch aufgrund eigener Befugnisse erfahren könnte. Wenn dies nicht der Fall ist, kann auch erhöhter Aufwand kein Kriterium sein, das die Akteneinsicht rechtfertigt.

Aktenauskünfte und insbesondere Einsichtnahmen durch Private oder deren Anwälte sollen nach dem Entwurf lediglich von einem berechtigten Interesse abhängen. Das würde bedeuten, daß Anwälte zur Verfolgung von irgendwelchen wirtschaftlichen oder z.B. auch publizistischen Interessen ihrer Mandanten undifferenziert sämtliche Inhalte von Strafverfahren – auch wenn ihre Mandanten daran völlig unbeteiligt sind – erfahren dürfen. Dies wäre unverhältnismäßig, weil die mit Zwang oder aufgrund besonderer Befugnisse erhobenen Daten besonders zu schützen sind und nicht mit irgendwelchen nicht ausdrücklich rechtlich verbürgten Interessen Dritter auf eine Stufe gestellt werden können.

Maßgeblich für die Gewährung eines Rechts auf Akteinsicht können nur rechtliche Interessen sein. Daher müssen die Personen, die Auskünfte oder Akteneinsicht begehren, zur Verfolgung von Rechtsansprüchen auf den Akteninhalt angewiesen sein.

Da sich die rechtlichen Interessen selten mit dem gesamten Akteninhalt decken werden, kann der Aufwand kein Kriterium für den Verzicht auf eine differenzierte Herangehensweise sein. Nur soweit die jeweiligen rechtlichen Interessen reichen, kann Einsicht gewährt werden. In jedem Fall ist zu prüfen, ob nicht einzelne Auskünfte ausreichen.

Der Gesetzentwurf sieht auch vor, daß Angaben in Justizdateien abweichend vom allgemeinen Datenschutzrecht nur nach dem Zufallsprinzip aus Anlaß einer Einzelfallbearbeitung gelöscht werden sollen. Wie dies in der Praxis aussähe, wird deutlich, wenn man die Verfahrensweise der Staatsanwaltschaft bei der Zentralkartei betrachtet (siehe unten 19.2.2).

Unsere gemeinsam mit anderen Datenschutzbeauftragten des Bundes und der Länder erhobene Forderung, dem StVÄG 1994 im Bundesrat nicht zuzustimmen und den Entwurf noch einmal gründlich zu überarbeiten, blieb unberücksichtigt. Der Bundesrat hat die Einbringung des Gesetzentwurfs im Bundestag beschlossen.

Die „Qualität" des Entwurfs wird bereits in der Wahl der Paragraphen deutlich: Wenige Wochen, nachdem der Bundesrat durch die Verabschiedung des Verbrechensbekämpfungsgesetzes ein neues Achtes Buch der Strafprozeßordnung eingeführt hat, das in §§ 473 ff. Regelungen für das zentrale staatsanwaltschaftliche Verfahrensregister enthält (siehe oben 19.1.1), hat derselbe Bundesrat in seinem Gesetzesantrag für das StVÄG 1994 ebenfalls ein neues Achtes Buch der StPO vorgesehen, das in §§ 473 ff. StPO ganz andere Regelungen über staatsanwaltschaftliche Akten enthalten soll.

Was der Bundestag daraus macht, bleibt abzuwarten.

19.2 Staatsanwaltschaft

19.2.1 Automation bei der Staatsanwaltschaft

Die Justizbehörde plant, die Staatsanwaltschaft weitgehend zu vernetzen, um für die Geschäftstellen und die Staatsanwälte ein gemeinsames Verfahren zur Vorgangsverwaltung und -bearbeitung einzurichten. Die bisherige – technisch abgängige – Zentralkartei der Staatsanwaltschaft soll in dieses Verfahren integriert werden. Wegen des insoweit bestehenden Zeitdrucks soll die Zentralkartei als erste auf das neue Verfahren umgestellt werden.

Auch aus datenschutzrechtlicher Sicht besteht kein Zweifel an der Erforderlichkeit, die völlig unzulängliche Zentralkartei zu ersetzen (siehe unten 19.2.2). Es ist ein Verfahren zu entwickeln, daß die Unterstützung der Tätigkeit der Staatsanwaltschaft gewährleistet und datenschutzrechtlichen Anforderungen genügt.

Für das Projekt wurde ein für die Tätigkeit der Geschäftstellen der Finanzgerichte entwickeltes Programm „GEORG" („Geschäftsstellenorganisiation bei den Finanzgerichten") ausgewählt, welches an die Tätigkeit der Staatsanwaltschaft angepaßt werden soll. Diese Entscheidung ist getroffen worden, ohne daß wir beteiligt worden sind. Wir haben deutlich gemacht, daß eine derartige Verfahrensweise in einem Großprojekt nicht mit den Bestimmungen über die rechtzeitige Beteiligung des Hamburgischen Datenschutzbeauftragten in Einklang zu bringen ist.

Es waren auch erhebliche Zweifel angebracht, ob die Entscheidung für die Übernahme des Verfahrens „GEORG" auf einer hinreichend gesicherten Grundlage getroffen worden ist. Ein Pflichtenheft über die gewünschte Ausgestaltung des Verfahrens liegt uns nicht vor. Die Überlegungen zur Konzeption enthalten ausschließlich Absichtserklärungen. Auf die Gründe für die Gesamtautomation in der dargestellten Form ging der Projektbericht nicht ein; welche Alternativen erwogen wurden und warum die Entscheidung für dieses System getroffen wurde, ergibt sich aus dem Projektbericht nicht. Diese Bestandteile wären aber notwendig gewesen, um das Vorhaben datenschutzrechtlich beurteilen zu können.

Bei der Präsentation des Programms „GEORG" – in der Konfiguration, wie sie für das Finanzgericht entwickelt worden war – stellte sich heraus, daß es die Ar-

beitsabläufe der Staatsanwaltschaft im wesentlichen nicht abbildet und datenschutzrechtliche Erfordernisse, z. B. im Bereich der Protokollierung, nicht erfüllt werden.

Bei der Entscheidung des Senats über die Beantragung von Haushaltsmitteln für dieses Projekt wurde zugesichert, daß die datenschutzrechtlichen Anforderungen erfüllt werden. Seitdem sind keine Fortschritte bei der umfassenden Automation der Staatsanwaltschaft festzustellen.

19.2.2 Zustand der Zentralkartei der Staatsanwaltschaft

Der Zustand der Zentralkartei der Staatsanwaltschaft ist datenschutzrechtlich besorgniserregend. In der Zentralkartei werden die Aktenzeichen und die Personalien bekannter Beschuldigter (1993 über 130.000), Ermittlungsverfahren gegen unbekannte Beschuldigte (1993 über 200.000) sowie Einsprüche gegen Bußgeldbescheide bei Ordnungswidrigkeiten (1993 über 7.700) jeweils mit Kurzangaben zum Vorwurf erfaßt. Die Zentralkartei dient der Information für die Staatsanwaltschaft selbst, welche Verfahrensakten vorliegen, aber auch der Auskunftserteilung an andere Stellen.

Zur Aufarbeitung der im 12. TB (19.4) geäußerten Kritik an der Erteilung von Auskünften an andere Stellen sind binnen einer Arbeitswoche im Februar 1994 die telefonischen Anfragen der Polizei protokolliert worden. Die Auswertung der Protokolle hat ergeben, daß die Polizeibeamten im wesentlichen nach staatsanwaltschaftlichen Aktenzeichen von Vorgängen gefragt haben, die sie selbst der Staatsanwaltschaft übersandt hatten. Hiergegen ist grundsätzlich aus datenschutzrechtlicher Sicht nichts einzuwenden.

Die Polizei hat allerdings angemerkt, daß auf telefonische Nachfragen weitgehend verzichtet werden könnte, wenn die Rücklaufzettel mit den Aktenzeichen binnen 3 bis 4 Tagen eintreffen würden und nicht erst nach 4 bis 6 Wochen. Damit wurde nur eines der Probleme im Zusammenhang mit der Zentralkartei deutlich.

Viel besorgniserregender als der Rückstand bei der Mitteilung von Aktenzeichen sind die Rückstände bei den Verfahrensergebnissen. Wenn der zuständige Staatsanwalt ein Ermittlungsverfahren selbst durch Einstellung abschließt oder von einer gerichtlichen Entscheidung erfährt, füllt er einen sogenannten „gelben Zettel" aus, in dem das Verfahrensergebnis eingetragen wird. Dieser „gelbe Zettel" wird zunächst an die Zentralkartei weitergeleitet, damit dort das Verfahrensergebnis eingetragen wird. Anschließend soll er an die Polizei weitergeleitet werden.

Nur so kann die Polizei ihrer gesetzlichen Verpflichtung nachkommen, eigene Speicherungen entsprechend dem Ausgang des Ermittlungsverfahrens zu überprüfen. Hiervon hängen Speicherungsfristen ab, da bei Einstellung wegen geringer Schuld oder Verurteilung zu geringen Geldstrafen nur eine verkürzte

Laufzeit von Speicherungen in Kriminalakten und im polizeilichen Auskunftssystem in Betracht kommt (vgl. 10. TB, 16.3.1). Wichtiger ist noch die gesetzliche Verpflichtung zur Löschung von polizeilichen Speicherungen, wenn der dem Verfahren zugrundliegende Verdacht entfällt (§ 16 Abs. 2 Satz 4 des hamburgischen Gesetzes über die Datenverarbeitung der Polizei).

Bei der Zentralkartei kommt es jedoch zu einem ganz erheblichen Rückstand bei der Abarbeitung der „gelben Zettel". Während wir im 12. TB, 19.4 noch über 20.000 unerledigte Vorgänge berichteten, wuchs der Rückstand im Laufe des Jahres 1994 rapide an. Er kann nur noch kistenweise erfasst werden. Er betrug Mitte September 66 Kisten, was einen Rückstand von etwa 40.000 Vorgängen bedeutet, Ende Oktober 81 Kisten mit schätzungsweise 50.000 „gelben Zetteln". Infolgedessen besteht in 50.000 Fällen die Gefahr, daß entlastende Verfahrensergebnisse nicht durch Fortschreibungen bei der Zentralkartei und Berichtigungen oder Löschungen bei der Polizei umgesetzt werden.

Wir haben daher unverzüglich Maßnahmen zur Beseitigung der Rückstände gefordert. Die Staatsanwaltschaft hat unser Schreiben vom 24. Oktober 1994 an die Justizbehörde weitergegeben, ohne in der Sache Stellung zu nehmen. Sie hatte der Justizbehörde bereits wiederholt über die Probleme bei der Zentralkartei berichtet.

Bei den bürgerschaftlichen Ausschußberatungen zum 12. TB am 28. Oktober 1994 hat sich ergeben, daß offenbar mit einer baldigen Behebung dieses Mangels nicht zu rechnen ist. Ich habe der Justizbehörde inzwischen eine förmliche Beanstandung gemäß § 25 HmbDSG angekündigt, falls die Behebung der Mängel nicht unverzüglich sichergestellt wird. Ohne eine umgehende personelle Verstärkung und geeignete organisatorische Maßnahmen wird es nicht gelingen können, diesen erheblichen Datenschutzmangel in einem realistischen Zeitraum zu beseitigen.

Unakzeptabel ist auch, daß die Staatsanwaltschaft es ablehnt, in Einzelfällen die Erforderlichkeit von Speicherungen in der Zentralkartei zu überprüfen. Die Speicherungsdauer richtet sich entsprechend der Aufgabenstellung der Zentralkartei nach den Aufbewahrungsvorschriften für die zugrundeliegenden Akten. Daher ist die Überprüfung der Frist immer möglich, solange Akten vorliegen. Wenn keine Akten mehr vorliegen, sind die Daten in der Zentralkartei zu löschen.

19.2.3 Speicherungen über Mitteilungen nach dem Geldwäschegesetz

Nach § 11 Geldwäschegesetz (GwG) haben Finanzinstitute und Spielbanken diejenigen Tatsachen, die darauf schließen lassen, daß die Finanztransaktion einer strafbaren Geldwäsche dient, unverzüglich der zuständigen Strafverfolgungsbehörde anzuzeigen.

Die Staatsanwaltschaft nimmt über sämtliche derartige Mitteilungen dateimäßige Speicherungen vor. Es werden Daten über die meldende Bank, den

Auftraggeber und Empfänger der Transaktion sowie staatsanwaltschaftliche Aktenzeichen in einer Registerdatei erfaßt. Hierüber sind wir im Dezember 1993 in Kenntnis gesetzt worden.

Erst bei einer Erörterung im Juli 1994 haben wir jedoch erfahren, daß eine weitere Datenbank eingerichtet worden ist, in der darüberhinaus auch Angaben zu den einzelnen Verdachtsgründen und insbesondere auch zu sonstigen Personen, wie z.B. Kontobevollmächtigten, erfaßt werden.

Nach den Erläuterungen der Staatsanwaltschaft reicht die Registerdatei nicht aus, um hinreichende Verdachtsgründe bei weiteren eingehenden Mitteilungen zu erhalten. Daher habe man sich entschlossen, die zweite Datei einzurichten. Die Datei ist datensatzübergreifend durch Eingabe von Suchbegriffen oder anhand von Suchlisten frei recherchierbar. Im Juli waren ca. 70 Sachverhalte erfaßt; etwa die gleiche Anzahl war noch nachzutragen. Man rechnete damit, daß wöchentlich ca. 4 bis 5 Meldungen neu eingehen.

In keinem Fall war jedoch ein förmliches Ermittlungsverfahren wegen des Verdachts auf Geldwäsche oder eines zugrundeliegenden Delikts (z.B. Drogenhandel) eingetragen.

Wir haben erhebliche Bedenken gegen die Führung dieser Datei bei der Staatsanwaltschaft geltend gemacht.

Nach der Dateistruktur, ihrer Auswertbarkeit und der geschilderten Zielsetzung handelt es sich um ein Instrument zur Erkennung von Zusammenhängen und die Sammlung eines Datenvorrats mit dem Zweck der Verdachtsschöpfung für zukünftige Fälle. Sie ist somit nicht dem Bereich der Strafverfolgung nach der Strafprozeßordnung, sondern dem der vorbeugenden Bekämpfung von Straftaten zuzuordnen.

Vorbeugende Bekämpfung von Straftaten ist jedoch nicht Aufgabe der Staatsanwaltschaft, sondern nach § 1 Abs. 1 Satz 2 Nr. 1 des Gesetzes über die Datenverarbeitung der Polizei (HmbPolDVG) Aufgabe der Polizei. Nach diesem Gesetz ist die Polizei befugt, Daten über Personen zu speichern, gegen die ein strafrechtliches Ermittlungsverfahren eingeleitet wurde. Hierbei muß sie jedoch immer den Verfahrensausgang berücksichtigen: bestätigt sich der Verdacht nicht, müssen die Daten gelöscht werden (§ 16 Abs. 2 PolDVG). Danach richtet sich die Staatsanwaltschaft für ihre Datei nicht, sondern sie speichert alle Fälle, obwohl sie selbst keinen hinreichenden Anfangsverdacht annimmt.

Die polizeiliche Speicherung von Personen, gegen die kein strafrechtliches Ermittlungsverfahren eingeleitet wird (hier im Regelfall die Auftraggeber und Empfänger der Transaktionen) und sog. Kontakt- und Begleitpersonen (hier die sog. „weiteren Personen") ist nur unter besonderen Voraussetzungen möglich. Hierzu gehört insbesondere, daß tatsächliche Anhaltspunkte für die künftige Begehung von Straftaten von erheblicher Bedeutung vorliegen müssen und

verkürzte Prüf- und Löschfristen zu beachten sind (§§ 6 Nr. 6 und 7, § 14 Abs. 1, § 16 Abs. 3 HmbPolDVG).

Die bei der Staatsanwaltschaft geführte Datei hält diese Vorgaben nicht ein. Über Speicherungsfristen hatte man sich bislang noch keine Gedanken gemacht; es gab auch keinerlei technische Vorkehrungen, um die Einhaltung derartiger Fristen zu gewährleisten.

Die Datei setzt sich damit nach unserer Auffassung sowohl über die gesetzliche Aufgabenzuweisung als auch über die gesetzlichen Begrenzungen der Speicherbefugnisse hinweg.

Die Vertreter der Staatsanwaltschaft haben dem entgegengehalten, daß sie durch das neue Geldwäschegesetz eine zusätzliche Aufgabe erhalten hätten. Sie seien ohne die Speicherungen in der Datei nicht in der Lage, diese Aufgabe zu erfüllen. Erkenntnisse, die zur Begründung eines Tatverdachts auf strafbare Geldwäsche nach § 261 Strafgesetzbuch (StGB) dienlich seien, würden ohne die Datei verloren gehen. Die Führung der Datei bei der Staatsanwaltschaft entspreche daher dem Willen des Gesetzgebers. Die bei der Polizei geführten Dateien reichten nicht aus, da sie sich lediglich auf Fälle im Zusammenhang mit organisierter Kriminalität bezögen und somit nur einen Teilbereich der nach dem Geldwäschegesetz und § 261 StGB relevanten Fälle abdecken würden.

Wir haben demgegenüber darauf hingewiesen, daß sich dem Wortlaut und dem Zweck des Geldwäschegesetzes weder normenklar noch aufgrund einer Generalklausel eine eigenständige Ermittlungs- und Speicherungskompetenz der Staatsanwaltschaft entnehmen läßt. Vielmehr setzt das Gesetz die bestehenden Befugnisse nach der Strafprozeßordnung einerseits und dem Polizeirecht andererseits voraus und läßt sie unberührt. Die Neuerung des Gesetzes besteht darin, daß aufgrund der Anzeigepflicht Informationen flächendeckend in erheblich weiterem Umfang als bei „normalen" Strafanzeigen üblich eingehen. Daher bedarf es einer Eingrenzung der speicherungsfähigen Sachverhalte, die das Polizeirecht durch die Kriterien tatsächliche Anhaltspunkte für bevorstehende Straftaten von erheblicher Bedeutung und die Prüf- und Löschfristen vorsieht.

Das zusätzliche Kriterium des Bezugs zur organisierten Kriminalität (OK-Relevanz) gilt ausschließlich für Speicherungen in der bundesweit betriebenen Arbeitsdatei PIOS „Organisierte Kriminalität" (APOK) nach Maßgabe der Errichtungsanordnung (vgl. 12. TB,17.3.1). Speicherungen im Bereich des Landeskriminalamtes können unabhängig von der OK-Relevanz nach Maßgabe des HmbPolDVG vorgenommen werden.

Eine Annäherung der entgegengesetzten Positionen war bisher nicht zu erzielen. Es wurde vereinbart, weitere Erfahrungen einzubeziehen, insbesondere, ob die zusätzlichen in der Datei vorgesehenen Angaben die erwartete Unter-

stützung bei der Bearbeitung von Mitteilungen nach dem GwG leisten. Hierfür sollen bei der Staatsanwaltschaft geeignete Vorkehrungen zur Auswertung von Trefferfällen, der Erkennung von Zusammenhängen etc. getroffen werden. Diese Auswertung war bei Redaktionsschluß dieses Berichts noch nicht abgeschlossen.

19.3 Gnadenwesen

Bereits im 12. TB (19.5) war darauf hingewiesen worden, daß die Vorschrift des § 2 Abs. 5 Hamburgisches Datenschutzgesetz (HmbDSG), der die Anwendung des HmbDSG auf das Gnadenwesen ausschließt, mit dem Grundrecht auf informationelle Selbstbestimmung unvereinbar ist. Bei der Vorbereitung von Gnadenentscheidungen werden eine Vielzahl sensibler personenbezogener Daten erhoben, ohne daß insoweit eine Rechtsgrundlage existiert.

Mein Vorschlag, diese Einschränkung zu streichen, wurde von der Justizbehörde nicht in den Entwurf zur Novellierung des HmbDSG übernommen.

Eine Reihe von Datenschutzgesetzen anderer Bundesländer und auch das BDSG kennen diese Einschränkung des Anwendungsbereiches nicht.

Im Saarland wurde am 16. März 1994 ein Gesetz über das Gnadenwesen verabschiedet, welches auch die datenschutzrechtlichen Fragestellungen im wesentlichen löst.

Eine Regelung entweder im HmbDSG oder aber in einem eigenständigen Gnadengesetz sollte 1995 angestrebt werden.

20. Strafvollzug

20.1 Aufarbeitung des Berichtes der Querschnittsprüfung von Justizvollzugsanstalten

Im Berichtszeitraum wurde zu dem 1993 erstellten (vgl. 12.TB, 20.2), ca. 200 Seiten umfassenden Prüfungsbericht des Hamburgischen Datenschutzbeauftragten durch die Justizbehörde (Strafvollzugsamt) Stellung genommen. In einer Reihe von Fällen wurden die im Prüfbericht unterbreiteten Vorschläge des Hamburgischen Datenschutzbeauftragten von der Justizbehörde übernommen. Eine Reihe von Problempunkten, von denen die wichtigsten im folgenden dargestellt werden, sind noch nicht abschließend bearbeitet. Insgesamt lässt sich aber festhalten, daß deutliche Fortschritte zur Verbesserung des Datenschutzes bei den schwierigen Rahmenbedingungen in den Strafanstalten auf den Weg gebracht wurden.

20.2 Einsicht in die Gefangenenpersonalakte

Über jeden Gefangenen wird eine Gefangenenpersonalakte angelegt, die alle Vorgänge enthält, die während der Strafzeit anfallen. Neben dem Urteil, in dem

sich auch Ausführungen z. B. zu psychiatrischen Auffälligkeiten befinden können, werden alle Anträge des Gefangenen sowie Beurteilungen über ihn, aber auch besondere Vorkommnisse in die Akte aufgenommen. In diese Akte hat der Strafgefangene bisher keine Akteneinsicht.

Die Bediensteten der Strafanstalt haben hingegen zu dieser Akte einen unbeschränkten Zugang, ohne daß dies nachzuvollziehen ist oder eine Prüfung der Erforderlichkeit erfolgt.

Im Prüfungsbericht (vgl.12.TB,20.2) wurde durch den Hamburgischen Datenschutzbeauftragten eine Änderung dieser Praxis gefordert, sowohl hinsichtlich der Bediensteten als auch hinsichtlich des Gefangenen selbst. Den datenschutzrechtlichen Grundsatz, daß Zugang zu personenbezogenen Daten für Bedienstete nur insoweit eingeräumt werden darf, wie es die jeweilige Aufgabe erfordert, hatte die Justizbehörde für die Gefangenenpersonalakte bereits erkannt.

Die Justizbehörde hat hinsichtlich der Einsicht in die Akten durch die Bediensteten vorgesehen, daß jede Akteneinsicht durch sogenannte „Lesekarten" protokolliert wird. Jede Einsichtnahme eines Bediensteten soll auf dieser Karte eingetragen werden. Die Einführung dieser Maßnahme ist insoweit zu begrüßen, als nunmehr wenigstens die Möglichkeit geschaffen wird, nachzuvollziehen, wer in die Akte eingesehen hat. Diese Maßnahme reicht aber nicht aus.

Der Hamburgische Datenschutzbeauftragte hatte darüber hinaus gefordert, daß die Gefangenenpersonalakte zumindest in zwei Teile aufgeteilt werden sollte. Ein Teil sollte sensible, die Intimsphäre des Gefangenen betreffende Informationen enthalten (Urteil, Lebenslauf pp). In diesen Teil sollten nur diejenigen Bediensteten Einsicht erhalten, die diese Informationen für ihre Aufgabenstellung im Rahmen des Behandlungsvollzuges benötigen. Ein zweiter Teil sollte die weniger sensiblen Daten enthalten, die für die „Verwaltung" des Strafgefangenen erforderlich sind. Das Strafvollzugsamt hat diesen Vorschlag abgelehnt, da dies rechtlich nicht geboten und verwaltungsökonomisch nicht zu vertreten sei. Dies überzeugt den Hamburgischen Datenschutzbeauftragten nicht. Die Diskussion wird zu diesem Punkt fortgesetzt.

Hinsichtlich der Forderung des Datenschutzbeauftragten, einen funktional differenzierten Zugriff auf die Akte bzw. auf Teile der Akte entsprechend dem arbeitsteilig strukturierten Anstaltsbetrieb zu schaffen, hat das Strafvollzugsamt angekündigt, eine neue Allgemeine Verwaltungsvorschrift zum Umgang mit der Gefangenenpersonalakte zu erlassen. Ob und inwieweit diese die nach Auffassung des Datenschutzbeauftragten erforderlichen Differenzierungen enthält, bleibt abzuwarten.

Gewisse Fortschritte sind auch bei dem Problemkreis der Akteneinsicht des Strafgefangenen in seine Gefangenenpersonalakte festzustellen. Im 12. TB

(20.3) war dargestellt worden, daß dem Strafgefangenen ein Anspruch auf Auskunft bzw. Akteneinsicht zusteht. Da das Strafvollzugsgesetz keine Vorschriften über die Akteneinsicht enthält, gelten die Vorschriften des Hamburgischen Datenschutzgesetzes mit seinem Recht auf Auskunft. In der Praxis des Strafvollzuges wurde dem Strafgefangenen ein Anspruch auf Auskunft bzw. Akteneinsicht bisher nicht eingeräumt.

Das Strafvollzugsamt hat in seiner Stellungnahme zum Prüfbericht vorgeschlagen, dem Strafgefangenen einen Anspruch auf Auskunft auf die in seiner Gefangenenpersonalakte zu seiner Person gespeicherten Daten einzuräumen. Dieser Anspruch soll u. a. allerdings nur dann bestehen, wenn der Gefangene sein Auskunftsinteresse darlegt. Ein solches Erfordernis findet in den Bestimmungen des Hamburgischen Datenschutzgesetzes über die Erteilung einer Auskunft keine Stütze. Von daher ist insoweit der Diskussionsprozess mit der Justizbehörde noch nicht abgeschlossen.

Hinsichtlich der weitergehenden Akteneinsicht durch den Strafgefangenen oder seinen Bevollmächtigten erkennt die Justizbehörde einen Anspruch auf Einsicht in die Gefangenenpersonalakte an. Dieser soll allerdings auf die Teile beschränkt werden, der objektive Befunde und Berichte enthält, nicht aber auf solche, die subjektive Notizen, persönliche Eindrücke und Wertungen betreffen. Auch diese Einschränkungen sind nach Auffassung des Hamburgischen Datenschutzbeauftragten nicht mit den gesetzlichen Bestimmungen in Einklang zu bringen; eine weitere Diskussion ist erforderlich. Anzuerkennen ist lediglich die von der Justizbehörde vorgeschlagene Einschränkung, eine Akteneinsicht dann zu versagen, wenn die Anstaltssicherheit hiervon berührt wird. Dies enspricht den Verweigerungsgründen, die durch das Hamburgische Datenschutzgesetz anerkannt werden.

20.3 Postkontrolle

Zur Postkontrolle (vgl. 12.TB, 20.1; 11.TB, 20; 10. TB, 20.2) bleibt die Justizbehörde bei ihrer Ausgangsposition, daß in bestimmten Anstalten eine generelle Postkontrolle zulässig sei. Wir vertreten dagegen unverändert die Auffassung, daß § 29 Abs. 3 des Strafvollzugsgesetzes eine Einzelfallbetrachtung verlangt, ob die Postkontrolle aus Gründen der Behandlung oder der Sicherheit oder Ordnung der Anstalt erforderlich ist.

Inzwischen hat die Justizbehörde mitgeteilt, daß im Einzelfall davon abgesehen wird, Briefe inhaltlich zu kontrollieren, wenn keine konkreten Anhaltspunkte für das Vorliegen einer Gefährdung erkennbar sind und aus den genannten Gründen nach § 29 Abs. 3 Strafvollzugsgesetz keine Überwachung geboten erscheint. Damit nähert sich die Praxis der Postkontrolle im Strafvollzug unserer Forderung nach einer Einzelfallbetrachtung an.

21. Gesundheitswesen

21.1 Rechtsgrundlagen

Das seit Jahren angemahnte Gesetz über den öffentlichen Gesundheitsdienst, das als bereichsspezifische Rechtsgrundlage insbesondere für die bezirklichen Gesundheitsämter benötigt wird, wurde auch 1994 nicht erlassen. Inzwischen existiert jedoch ein Bericht des Projekts „Reform des öffentlichen Gesundheitsdienstes" und ein erster Rohentwurf für das Gesetz. Derzeit werden in bezirksübergreifenden Arbeitsgruppen die festzulegenden Aufgaben des öffentlichen Gesundheitsdienstes erörtert. Vom Ergebnis sind auch die Datenschutzregelungen abhängig. Ob – wie im Juli 1994 angekündigt – die Behördenabstimmung des Gesetzentwurfs noch bis zum Ende des Jahres 1994 erfolgt, bleibt abzuwarten.

Den Entwurf eines Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (HmbPsychKG) leitete der Senat Anfang September 1994 der Bürgerschaft zu. In der Behördenabstimmung hatten wir zu den umfangreichen Datenschutzregelungen ausführlich Stellung genommen und wesentliche Verbesserungen erreichen können.

Zum Problem wurde dagegen die Neufassung der Berufsordnung der Hamburger Ärzte. Sie bedarf als Satzung der Selbstverwaltungskörperschaft Ärztekammer der Genehmigung der Behörde für Arbeit, Gesundheit und Soziales als Aufsichtsbehörde. Datenschutzrechtlich bedenklich erschien die Regelung des Praxis-Verkaufs. Der Bundesgerichtshof (BGH) hatte entschieden, daß die Übergabe der Patientenkartei einer Praxis vom Veräußerer an den Käufer nur mit Einwilligung der Patienten zulässig ist (vgl. 11. TB, 21.10). Die von der Kammer verabschiedete Berufsordnung sieht lediglich vor, der Arzt habe dafür Sorge zu tragen, „daß seine ärztlichen Aufzeichnungen und Untersuchungsbefunde nach Aufgabe der Praxis in gehörige Obhut gegeben werden". Es fehlt der für ein rechtmäßiges Verhalten der Ärzte wichtige Hinweis auf die notwendige Einwilligung der Patienten. Auch die Justizbehörde hielt die beschlossene Regelung deswegen nicht für genehmigungsfähig. Die Kammer bestätigte gleichwohl die beschlossene Berufsordnung noch einmal in ihrer Versammlung im September 1994. Die Behörde für Arbeit, Gesundheit und Soziales plant, diesem Teil der Berufsordnung nun die aufsichtsbehördliche Genehmigung zu versagen, und erwägt eine Aufsichtsverfügung zur Durchsetzung des BGH-Urteils.

21.2 Projekt Qualitätssicherung in der Chirurgie (Quasic)

Was lange währt, wird endlich gut. Nach den kritischen Berichten in den letzten Jahren (11.TB, 21.5.1; 12.TB, 21.3) hat sich das Projekt Quasic teilweise inzwischen zu einem datenschutzrechtlichen „Vorzeige-Projekt" weiterentwickelt:

Dem Allgemeinen Krankenhaus Barmbek gelang in Abstimmung mit uns erstmals eine befriedigende technisch-organisatorische Lösung für § 14 des Hamburgischen Krankenhausgesetzes (HmbKHG). Dieser fordert, daß bei EDV-Anlagen mit „Direktabruf" von Patientendaten dieser Direktabruf zu sperren ist, sobald die Behandlung des Patienten in dem Krankenhaus abgeschlossen ist. Zugleich muß jedoch gewährleistet bleiben, daß ein Zugriff auf die Patientendaten wieder möglich wird, wenn der Patient später einmal erneut in demselben Krankenhaus behandelt wird.

Das Quasic-Konzept sieht dazu zunächst die getrennte Speicherung von Patienten-Identifikations-Daten einerseits und medizinischen Therapiedaten andererseits in verschiedenen Dateien vor. Über eine Bezugsnummer werden die Daten während der Behandlungzeit verknüpft. Nach Abschluß einer Behandlung wird die Verknüpfbarkeit aufgehoben, so daß die medizinischen Daten grundsätzlich nur noch ohne Patientenbezug genutzt werden können – etwa für Forschung und Qualitätssicherung. Damit ist dem § 14 HmbKHG Rechnung getragen.

Um bei einer späteren Wiederaufnahme desselben Patienten die früheren Behandlungsdaten verfügbar zu machen, wird ausschließlich Ärzten eine besondere Zugriffsfunktion eingeräumt, die die Verknüpfbarkeit von Patienten-Identifikations-Daten und Behandlungsdaten wieder ermöglicht. Diese Funktion gibt keinen Zugriff auf Verwaltungsdaten, bezieht sich nur auf aktuell aufgenommene Patienten, gilt nur für die Dauer der aktuellen Behandlung und löst vor allem eine eigene automatische Protokollierung aus. Damit ist ein mißbräuchliches Nutzen patientenbezogener medizinischer Daten außerhalb einer Behandlung weitgehend ausgeschlossen.

Diese technisch-organisatorische Lösung haben wir den für den Datenschutz Verantwortlichen in den staatlichen Krankenhäusern bei einem gemeinsamen Treffen ausdrücklich empfohlen.

21.3 Überregionale Forschungsprojekte

Die Mehrheit der Forschungsprojekte, die wir datenschutzrechtlich zu bewerten hatten, zeichnete sich durch einen hamburgübergreifenden Datenfluß aus. Dies erforderte zum einen die Festlegung der örtlichen Zuständigkeit je nach dem Ort der einzelnen Datenverarbeitungsphasen und zum anderen eine Abstimmung mit den Datenschutzbeauftragten der ebenfalls betroffenen Länder.

So konnten wir der Weitergabe von anonymisierten Leichenschauscheinen aus Hamburger Gesundheitsämtern an das Deutsche Krebsforschungszentrum Heidelberg für die epidemiologische Studie „Mortalität in Gießereien" zustimmen. Die für den Datenempfänger zuständige baden-württembergische Datenschutzbeauftragte hatte das Verfahren ebenfalls gebilligt.

Das überregionale Forschungsprojekt „Systemische Haemophilus influenzae Erkrankungen nach Einführung der Schutzimpfung in Deutschland bei Kindern unter 10 Jahren" wurde uns bereits mit Stellungnahmen von drei Landesdatenschutzbeauftragten vorgestellt. In Hamburg ging es vor allem um eine Übermittlung von Meldedaten an die Universität Düsseldorf. Nach § 31 Abs.1 des Hamburgischen Meldegesetzes war sie zulässig.

Anläßlich der multizentrischen Studie „Qualitätssicherung in der Krankenhaushygiene" fand zwischen den Datenschutzbeauftragten des Bundes und der Länder eine aufwendige Abstimmung im Arbeitskreis Wissenschaft statt. Grund war, daß die Forschungsklauseln in den Krankenhausgesetzen bzw. – soweit nicht vorhanden – in den Datenschutzgesetzen der Länder unterschiedlich gefaßt sind. Diesen Nachteil für ein überregionales Forschungsprojekt versuchten die Datenschutzbeauftragten durch eine Vereinheitlichung ihrer Stellungnahmen auszugleichen. Hauptgegenstand dieser Bemühungen war die Verständigung über Notwendigkeit und Form der Patienten-Einwilligung.

Ein Hamburger Institut für Gesundheitsforschung meldete im Berichtszeitraum gleich drei überregionale Forschungsprojekte zur datenschutzrechtlichen Stellungnahme: eine Studie zur möglichen fruchtbarkeitsmindernden und fruchtschädigenden Wirkung eines Lösungsmittels, eine Elternbefragung in der Umgebung einer Sonderabfall-Verbrennungsanlage und eine Gesundheitsfolgen-Untersuchung zum Störfall bei einem Chemieunternehmen.

Obwohl die eigentliche Datenerhebung jeweils in anderen Bundesländern erfolgte, hatten wir als für den Sitz des Instituts zuständige Aufsichtsbehörde insbesondere folgendes zu prüfen: Ist durch das Muster-Anschreiben des Instituts die Freiwilligkeit der Teilnahme an der Studie und eine ausreichende Information über die Datenverarbeitung sichergestellt ? Ist die Einwilligungserklärung angemessen formuliert ? Ist die Sicherheit der Datenverarbeitung in Hamburg gewährleistet ? Die von uns angeregten Verbesserungsvorschläge wurden aufgegriffen und umgesetzt. In Abstimmung mit uns äußerte sich bei der Störfall-Studie auch der Hessische Datenschutzbeauftragte zur Einwilligungserklärung der Studienteilnehmer.

Zusammenfassend bewertet erscheint im Bereich der überregionalen Forschung sowohl die datenschutzrechtliche Situation als auch die praktische Aufsichtstätigkeit der Datenschutzinstanzen unbefriedigend: Nicht immer ist die grenzüberschreitende Datenverarbeitung von Anfang an deutlich; Forschungsinstitute können einzelne Datenschutzbeauftragte mit früheren Stellungnahmen anderer zu Zugeständnissen drängen; die föderale Rechtsstruktur erzwingt zuweilen gegensätzliche Stellungnahmen der Datenschutzbeauftragten zu der gleichen Forschungsarbeit; schließlich ist auch eine Einigkeit unter den betroffenen Datenschutzbeauftragten angesichts vielfach notwendiger Auslegungs- und Abwägungsprozesse nicht selbstverständlich.

Möglicherweise könnte hier die interne Festlegung eines „federführenden" Datenschutzbeauftragten für ein überregionales (öffentliches) Forschungsprojekt hilfreich sein. Dieser kann zwar nicht unterschiedliche Rechtssituationen und formale Zuständigkeiten überwinden. Er könnte aber Vorklärungen erreichen und für das Forschungsinstitut als Ansprechpartner während der Prüfungen zur Verfügung stehen.

21.4 Prüfung des Allgemeinen Krankenhauses St. Georg

21.4.1 Prüfungsgegenstand

Im Februar und März 1994 führten wir eine datenschutzrechtliche Querschnittsprüfung im AK St.Georg durch. Schwerpunkte der Untersuchung waren

— die Organisation des Datenschutzes,

— die Patientenaufnahme,

— die Patientendatenverwaltung in einem Stationszimmer (Chirurgische Station),

— die HIV-Ambulanz,

— die Datenverarbeitung im Onkologischen Schwerpunkt,

— das Krankengeschichtenarchiv,

— Formulare mit Patientendaten.

Diese Prüfungsgegenstände ermöglichten keine „flächendeckende" Kontrolle, sondern beschränkten sich auf datenschutzrechtliche Kernbereiche und Einzelfälle, die von Patient/innen oder Mitarbeiter/innen an uns herangetragen wurden.

Die Leitung des Krankenhauses und auch das angeprochene ärztliche und Pflegepersonal unterstützten uns durch eine konstruktive Zusammenarbeit.

21.4.2 Interne Organisation des Datenschutzes

Die von der Geschäftsführung des Landesbetriebs Krankenhäuser 1993 beschlossenen Empfehlungen zum Datenschutz setzte das AK St. Georg für den IuK-Bereich in eine eigene Dienstanweisung um. Hinsichtlich der Krankenakten-Verwaltung seien die Empfehlungen „verbindliche Handlungsgrundlage".

Die personelle Verantwortung für den Datenschutz im AK St.Georg wurde einem Arzt und einem Verwaltungsbeamten übertragen. Auch der Leiter der IuK-Abteilung habe Datenschutzaufgaben zu erfüllen. Eine diese Aufgaben umschreibende Einsetzungverfügung existiert für keine Person; auf unsere Anregung wurden jedoch die Stellenbeschreibungen entsprechend ergänzt.

Das Hauptproblem der Datenschutz-Organisation im AK St.Georg liegt darin, daß die genannten Personen in keiner Weise von ihren sonstigen Aufgaben entlastet wurden. Für eine – ggf. teilweise – Freistellung zur Übernahme von Datenschutzaufgaben gebe es keine Kostenübernahme durch die Krankenversicherung. Wir haben der Leitung des AK St. Georg deutlich gemacht, daß angesichts der Sensibilität der Patienten- und Mitarbeiterdaten, der Größe des Krankenhauses und des Umfangs der Datenverarbeitung die von § 10 HmbDSG geforderte Sicherstellung des Datenschutzes so nicht zu gewährleisten ist.

21.4.3 Patientenaufnahme

Die Patientenaufnahme im AK St.Georg erfolgt in einem großen Raum an mehreren Bildschirmarbeitsplätzen. Auf unsere Anregung wird durch eine Umgruppierung von Stühlen und Bildschirmen versucht, bei zeitgleichen Aufnahmen mehrerer Patienten ein Mithören sensibler persönlicher Daten Dritter zu verhindern.

Die Patientenaufnahme wird technisch unterstützt durch das System IDIK, das jedoch demnächst durch ein moderneres Verfahren ersetzt werden soll. Die Aufnahmemaske enthält Daten, die für die Behandlung notwendig sind, und andere, die der Patient ggf. freiwillig angibt. Während bei der Konfessions-Angabe bereits ein Freiwilligkeits-Hinweis auf der Bildschirmmaske erscheint, haben wir dies auch für die Angaben zu Angehörigen, zum Arbeitgeber (außer bei Arbeitsunfällen) und zum Hausarzt gefordert.

Zur Heranziehung früherer Unterlagen wurde der Patient bisher lediglich gefragt, ob er schon einmal im AK St.Georg war. Nach unserem Hinweis auf die Datenschutz-Empfehlungen des Landesbetriebes soll der Patient in Zukunft ausdrücklich um seine schriftliche Einwilligung in die Beiziehung bereits bestehender Krankenakten gebeten werden.

21.4.4 Datensicherheit

In verschiedenen Bereichen mußten wir eine unzureichende Datensicherheit feststellen:

— In einer chirurgischen Station, die wir trotz Ankündigung unbemerkt betraten, lag patientenbezogene Post offen in Körben unmittelbar neben der Flurtür.

— Die Räume, in denen die HIV-Ambulanz mit ihren hochsensiblen Datenbeständen untergebracht ist, sind weitgehend ungesichert. Die großen Fenster zur Straße bzw. zu einem Innenhof sind nur einfachverglast und haben z.T. renovierungsbedürftige Rahmen.

— In der endoskopischen Abteilung, in der wir uns – von Mitarbeiter/innen lange unbemerkt – umsahen, fanden wir die Patientenakten in offenen Papp-Kartons unter einer Liege. Auf dieser Liege warten Patienten auch zeitweise allein auf die weitere Behandlung.

— Im Onkologischen Schwerpunkt hatte auch eine abteilungsfremde Mitarbeiterin ihren Arbeitsplatz und damit Zugang zu sensibelsten Unterlagen. Dasselbe gilt nach wie vor für den Betriebsärztlichen Dienst. Im Flur des Onkologischen Schwerpunktes befinden sich zwei ältere Aktenrollschränke aus Holz, in denen Arztbriefe über Tumor-Patienten seit 1985 aufbewahrt werden. Die Abteilung sei mangels Personalkapazität nicht in der Lage, Datenerfassung und Plausibilitätskontrollen so zu verstärken, daß auf die alten Unterlagen verzichtet werden könnte.

Auf unsere Forderung, diese Mißstände abzustellen, leitete das Krankenhaus verschiedene Verbesserungen ein. Inwieweit diese Bemühungen tatsächlich eine ausreichende Datensicherheit erreichen, bleibt einer Nachschau vorbehalten.

21.4.5 Krankengeschichtenarchiv

Das Krankengeschichtenarchiv der Frauenklinik Finkenau, die Teil des AK St.Georg ist, war bei unserer Prüfung ohne Zugangssicherung. Ohne die Aufmerksamkeit einer Mitarbeiterin zu erregen, betraten wir den Regalraum und durchblätterten ungestört einige Patientinnen-Akten. In Zukunft wird nach Angaben des Krankenhauses die Flurtür verschlossen gehalten.

Auch die Türen zum Archiv des AK St.Georg waren unverschlossen. Inzwischen macht bei jeder Tür-Öffnung eine Klingel auf Besucher aufmerksam. Unmittelbar neben der Eingangstür fanden wir Computer-Ausdrucke mit den Patienten-Stammdaten seit 1979. Auf unseren Hinweis wurden sie inzwischen vernichtet.

Bei der Durchsicht einiger zufällig herausgegriffenen Krankenakten fiel uns auf, daß die Akte einer verstorbenen Tumor-Patientin zwar einen Sektionsbericht enthielt, aber keinen Hinweis auf eine Benachrichtigung bzw. Einwilligung von Angehörigen. Auf dem Blatt „Krankengeschichte" fehlten die Angaben zu „bei Todesfällen: Sind Angehörige verständigt?" und „Krebsfragebogen ausgestellt: ja/nein". Das AK St. Georg nahm unsere Darstellung zum Anlaß für einen entsprechenden Hinweis des Ärztlichen Direktors an das Kollegium der Ärzte.

21.4.6 Weiteres Verfahren

In einem Schreiben vom Juli 1994 begrüßten wir die bereits getroffenen Maßnahmen zur Verbesserung des Datenschutzes im AK St.Georg und wiesen auf folgende offenen Punkte hin:

— Als Folge aus unserem Prüfbericht plant das AK St.Georg die Neufassung einzelner Formulare. Diese sollten mit der Geschäftsführung des Landesbetriebs einerseits und mit uns andererseits abgestimmt werden (vgl. 21.10).

— Die Planung des neuen EDV-Systems für die Patientenaufnahme bedarf ebenfalls der Beteiligung des Hamburgischen Datenschutzbeauftragten. Obwohl dieses System das System IDIK schon 1995 ersetzen soll, liegen uns bisher keine näheren Konzept-Beschreibungen vor.

— Die räumliche „Entflechtung" des Onkologischen Schwerpunktes und des betriebsärztlichen Dienstes halten wir angesichts der gemachten Erfahrungen für dringend.

— Im übrigen bedarf es für einige der in Angriff genommenen Maßnahmen – insbesondere der Datensicherheit – der Nachschau bzw. Nachfrage, ob ihre Umsetzung inzwischen abgeschlossen werden konnte.

21.5 Prüfung des Allgemeinen Krankenhauses Eilbek

Während bei der Prüfung des Allgemeinen Krankenhauses (AK) St. Georg datenschutzrechtliche Aspekte im Vordergrund standen, bezog sich die Prüfung des AK Eilbek schwerpunktmäßig auf die automatisierte Datenverarbeitung, insbesondere auf das krankenhausweit im Einsatz befindliche Textverarbeitungssystem PRISMA, auf das zur Pflegeunterstützung eingesetzte Verfahren PULS sowie auf das Netzwerk insgesamt. Eine Prüfung des Netzwerks ist nicht zuletzt deshalb von grundsätzlicher Bedeutung, weil im Vergleich zu anderen Krankenhäusern des Landesbetriebs die einzelnen Kliniken des AK Eilbek fast alle miteinander vernetzt sind.

Da im Netz des AK Eilbek sensible medizinische Daten verarbeitet werden, wurden sowohl an die Sicherheit des Netzes als auch an die Sicherheit der geprüften Verfahren sehr hohe Anforderungen gestellt. Begrüßenswerterweise hat das AK Eilbek unsere Vorschläge zur Verbesserung der Datensicherheit konstruktiv aufgegriffen und umgesetzt.

21.5.1 Netzwerk

Das Netz ist weitgehend vor Mißbrauch durch klinikfremde Personen gesichert: Rechner und Verteilerschränke sind in speziell hierfür vorgesehenen Rechnerräumen untergebracht, die über eine Alarmanlage sowie über Panzerglas-Fenster verfügen. Glasfaserkabel, die zwischen den einzelnen Gebäuden verlegt sind, verhindern ein einfaches und unbemerktes Aufschalten auf das Übertragungsmedium und damit ein Abhören der übertragenen Daten.

Dennoch kann nicht verhindert werden, daß Klinikmitarbeiter – ausreichendes technisches Wissen und spezielle Hardware und Software vorausgesetzt – sensible personenbezogene Daten, die über das Netz übertragen werden, mit-

lesen und auf externe Datenträger kopieren. Diese Sicherheitslücke resultiert aus der Tatsache, daß neben den Subnetzen für die Bereiche Geschäftsführung des Landesbetriebs Krankenhäuser, Technik, Zentralinstitut und IuK-Abteilung nur ein großes logisches Kliniknetz existiert, in dem sämtliche übertragenen Daten netzweit verfügbar sind. In älteren lokalen Netzen, in denen keine filternden Sternkoppler eingesetzt werden, sind sämtliche Netzdaten sogar direkt am PC-Arbeitsplatz vorhanden (vgl. 12.TB, 3.3.1).

Erschwerend kommt hinzu, daß die fünf Subnetze über selbstlernende Netzkoppler miteinander verbunden sind, so daß noch nicht einmal eine Trennung der Subnetze untereinander ausreichend sichergestellt werden kann: Falls Benutzer aus verschiedenen Subnetzen miteinander kommunizieren bzw. Daten untereinander austauschen wollen, wird – unabhängig von der Rechtmäßigkeit einer solchen Übermittlung – in jedem Fall die Verbindung zwischen den beiden Netzteilnehmern hergestellt.

Zur Verbesserung der Netzsicherheit hat sich das AK Eilbek bereiterklärt, die Anzahl der Subnetze durch Einsatz weiterer Netzkoppler zu erhöhen. In den Kliniken, in denen keine filternden Sternkoppler im Einsatz sind, werden zusätzliche Filterfunktionen auf Netzwerkebene implementiert. Statt selbstlernender Netzkoppler sollen konfigurierbare Geräte verwendet werden, in denen die Adressen der jeweils zulässigen Verbindungen fest eingetragen sind.

21.5.2 Textverarbeitungssystem PRISMA

Zur Erstellung medizinischer Texte (Berichte, Protokolle und Arztbriefe) wird in den einzelnen Kliniken des AK Eilbek das System PRISMA eingesetzt. In der Regel verfügt jede Sekretariatskraft über einen eigenen PC-Arbeitsplatz, in einigen Sekretariaten teilen sich jedoch mehrere Schreibkräfte ein Gerät. Die Texte werden auf einem zentralen UNIX-Rechner gespeichert und über NFS (Network File System) dem PC lokal zur Verfügung gestellt.

Die Anmeldung am System erfolgt in zwei Schritten: Zunächst authentisiert sich der Benutzer gegenüber NFS durch Eingabe eines Paßworts, anschließend gegenüber der auf dem PC zusätzlich installierten Sicherheitssoftware. Da die für den NFS-Zugriff verwendete UNIX-Benutzerkennung im PC fest gespeichert ist, müssen sämtliche Benutzer eines Geräts ein gemeinsames UNIX-Paßwort benutzen. Innerhalb der Umgebung der Sicherheitssoftware besitzt jeder Benutzer allerdings eine eigene Kennung und folglich auch ein eigenes Paßwort. Die einzelnen Abteilungen werden dadurch voneinander abgeschottet, daß nach dem Systemstart mittels NFS dem Benutzer nur solche Verzeichnisse bereitgestellt werden, die für die jeweilige Abteilung bestimmt sind. Für den abteilungsübergreifenden Textaustausch existiert ein gemeinsam genutztes Verzeichnis.

Diese Art der Zugriffskontrolle ist datensicherungstechnisch unzureichend: Einerseits ist der Boot-Schutz der Personalcomputer wenig wirkungsvoll. Zwar wird das Booten per Diskette durch die Sicherheitssoftware unterbunden, allerdings kann dieser Schutz durch Ausbau einer Steckverbindung leicht umgangen werden. Andererseits haben alle PRISMA-Benutzer unnötigerweise lesenden und schreibenden Zugriff auf sämtliche PRISMA-Texte des UNIX-File-Servers. Eine Abschottung der einzelnen Benutzer oder Abteilungen gegeneinander findet auf UNIX-Ebene nicht statt. Falls es daher gelingt, den wenig wirkungsvollen Boot-Schutz auf PC-Ebene zu umgehen und die Start-Prozedur zu manipulieren, kann auf sämtliche PRISMA-Texte zugegriffen werden.

Darüber hinaus wird beim Bereitstellen von Verzeichnissen nicht zwischen mehreren Benutzern eines Geräts unterschieden, so daß noch nicht einmal die Startprozedur verändert werden muß, um auf Texte anderer Benutzer des PC zugreifen zu können. Hinzu kommt, daß der Paßwortschutz in wesentlichen Punkten vernachlässigt worden ist und nicht der geltenden Paßwortrichtlinie entsprach.

Das Datensicherheitsrisiko wird dadurch verstärkt, daß weder auf PC- noch auf Server-Ebene protokolliert wurde, welcher Benutzer auf welche Daten zugegriffen hat. Dieses Risiko betrifft insbesondere die Systemverwaltung: Da diese nicht nach dem Vier-Augen-Prinzip abgewickelt wird, standen den umfassenden Zugriffsmöglichkeiten des Systemadministrators keine effektiven Kontrollinstrumente gegenüber.

Zur Verbesserung der Datensicherheit hat das AK Eilbek zusätzliche Maßnahmen vorgesehen. Der Boot-Schutz soll durch Ausbau der Diskettenlaufwerke erhöht werden. Auch sollen die durch das eingesetzte Sicherheitsprodukt zur Verfügung stehenden Funktionen gemäß der Paßwort-Richtlinie genutzt werden: Paßwörter sind demnach nur 35 Tage gültig, ihre Mindestlänge beträgt 6 Zeichen. PC-seitig soll die Protokollfunktion des Sicherheitssystems aktiviert werden.

Augenblicklich nicht leistbar ist es nach Einschätzung des AK Eilbek, die UNIX-Verzeichnisse benutzerbezogen bereitzustellen. Zwar könnte eine benutzerbezogene Bereitstellung von Verzeichnissen durch das PC-Sicherheitssystem unterstützt werden. Eine solche dezentrale Lösung würde jedoch sehr hohen Administrationsaufwand bedeuten. Da das AK Eilbek ohnehin beabsichtigt, nicht zuletzt aufgrund datensicherungstechnischer Defizite den UNIX-Server durch einen Novell-Server zu ersetzen, ist eine Umstellung auf benutzerspezifische Lösungen erst mit der geplanten Anschaffung eines Novell-Netzes vorgesehen.

21.5.3 Pflegedienstsystem PULS

Das Verfahren PULS dient der Unterstützung des Pflegedienstes und dokumentiert patientenbezogen sämtliche durchgeführten Pflegetätigkeiten. Dies gilt auch für bereits entlassene Patienten.

Die Zugriffskontrollen von PULS sind insgesamt als ausreichend zu bezeichnen: Sämtliche personenbezogenen Daten werden auf einem UNIX-Server gespeichert, dezentral sind Personalcomputer ohne Diskettenlaufwerk im Einsatz. PC-seitig wird die Zugriffskontrolle durch eine über das BIOS gesteuerte Paßwortabfrage realisiert. Host-seitig werden dagegen die Zugriffsrechte auf Datenbankebene verwaltet. Die PC sind zudem so konfiguriert, daß sämtliche Schnittstellen gesperrt sind. Der Betriebssystemzugriff des Benutzers wird dadurch verhindert, daß nach dem Anschalten sofort das Anwendungsprogramm aufgerufen wird und dieses nicht verlassen werden kann. Auf Anwendungsebene findet eine weitere Paßwortabfrage statt. Die PC sind zusätzlich gegen Diebstahl gesichert.

Problematisch sind vielmehr die weitgreifenden Rechte des Systemverwalters. Das AK Eilbek hat sich allerdings bereiterklärt, die Systemverwaltung soweit wie möglich menügesteuert unter einer nicht-privilegierten Kennung abzuwikkeln. Um die verbleibenden Systemverwaltertätigkeiten kontrollieren zu können, werden privilegierte Superuser-Tätigkeiten demnächst entweder nach dem Vier-Augen-Prinzip ausgeführt oder revisionssicher protokolliert.

Unterstützt werden die technischen Sicherheitsmaßnahmen durch eine Dienstanweisung, die den Umgang mit Daten entlassener Patienten näher regeln soll. Statt – wie es bisher der Fall war – personenbezogene Daten entlassener Patienten lediglich in einer seperaten Datei zu speichern, werden die Daten entlassener Patienten demnächst vollständig gelöscht, wenn sie nicht mehr zur Unterstützung des Pflegedienstes benötigt werden.

Ebenfalls gelöst ist das Problem, daß die für die Schulung und Weiterentwicklung des PULS-Verfahrens zuständigen Mitarbeiter der IuK-Abteilung Zugriffsrechte auf Echtdaten besaßen. Da dies für die Erledigung ihrer Aufgaben nicht erforderlich ist, wurde für die Projektleitung inzwischen ein eigenes Testsystem eingerichtet.

21.6 Prüfung des Gesundheitsamtes Hamburg-Nord

Im 4. TB (4.13.2) hatten wir über die Schlußfolgerungen aus einer aufwendigen Querschnittsprüfung in einem Bezirksgesundheitsamt 1984 berichtet. Im Juli 1994 führten wir eine datenschutzrechtliche Prüfung im Gesundheitsamt Hamburg-Nord durch – nicht zuletzt, um die seinerzeit getroffenen Vereinbarungen und Maßnahmen nach 10 Jahren zu überprüfen.

Schwerpunkte der Untersuchung waren die Bereiche

— Ärztliche Suchkartei,

— Seuchenbekämpfung,

— amtsärztliche Gutachten,

— jugendpsychiatrischer Dienst und

— schulärztlicher Dienst.

Im Berichtszeitraum wurde mit dem Gesundheitsamt zunächst unsere Sachverhaltsdarstellung abgestimmt. Die datenschutzrechtliche Bewertung – ggf. mit Forderungen nach Verbesserungsmaßnahmen – konnte bis zum Redaktionsschluß dieses Tätigkeitsberichts nicht abgeschlossen werden. Folgende Sachverhalte sind für uns von Bedeutung:

— Die ärztliche Suchkartei enthält ca. 20.000 Karteikarten mit dem Namen und dem Geburtsdatum der Person, die Kontakt mit dem Gesundheitsamt hatte. Zur internen Zuordnung späterer Anfragen, Aufträge usw. enthalten die Karten daneben das Zeichen der tätig gewordenen Abteilung und – bei der Abteilung für amtsärztliche Gutachten – das Aktenzeichen. Zwecksetzung, Aufbewahrungsfristen und Datensicherheit der Suchkartei bedürfen der datenschutzrechtlichen Beurteilung.

— Amtsärztliche Gutachten werden für die unterschiedlichsten Zwecke gefertigt; die meisten der jährlich ca. 1500 Anfragen erhält das Gesundheitsamt vom Sozialamt. Datenschutzrechtlich relevant ist hier die Verwendung vorformulierter Einwilligungserklärungen und der Umfang der vom Gesundheitsamt an die anfragenden Stellen zu übermittelnden Daten. Ein besonderes Problem bildet die Feststellung und ggf. Offenbarung einer Nichteignung zum Führen von Kraftfahrzeugen.

— Der jugendpsychiatrische Dienst erhält in seinen (freiwilligen) Beratungsgesprächen besonders sensible Daten. Ob und ggf. wie die von den Jugendlichen bzw. deren Eltern erwartete Vertraulichkeit auch gegenüber den Kontroll- und Aufsichtsbefugnissen der Vorgesetzten und gegenüber den Anforderungen eines wirtschaftlichen Schreibdienstes gewahrt werden kann, war Gegenstand der im Gesundheitsamt geführten Gespräche. Wir beabsichtigen, hierzu praktische Hinweise zu geben.

— Beim schulärztlichen Dienst haben wir uns die Datenerhebung nach dem einheitlichen Dokumentationsbogen sowie die Kommunikation zwischen Schularzt, Eltern und behandelndem Arzt erläutern lassen.

21.7 Fernwartung der Patientenüberwachungsanlage im Universitätskrankenhaus Eppendorf (UKE)

Mit einiger Verzögerung ist im Frühjahr 1994 eine hochmoderne Patientenüberwachungsanlage auf der Intensivstation der Anästhesiologie im UKE in Betrieb genommen worden. Die Anlage besteht aus einem sogenannten hämodynamischen Monitoring, das aktuelle EKG-, Blutdruck- und andere überwachungsbedürftige physiologische Patientenwerte permanent erfaßt. Dazu

gehört ein Dokumentationssystem, das sämtliche auf der Intensivstation anfallenden diagnostischen und therapeutischen Daten archiviert.

Aufgrund der lebenswichtigen Rolle des Verfahrens bei der medizinischen Versorgung der Patienten wurden an die Verfügbarkeit des Systems sehr hohe Anforderungen gestellt. So wird das Kernstück der Anlage von zwei UNIX-Rechnern gebildet, von denen jeder allein den Betrieb der Anlage bei Ausfall des anderen Rechners aufrechterhalten kann. Beide Rechner sind mit einem Notstromaggregat ausgestattet, das auch bei Stromausfall eine unterbrechungsfreie Stromversorgung der Rechner garantiert. Um auch gegen einen Ausfall des Netzes gesichert zu sein, sind sämtliche Netzkomponenten in doppelter Ausführung vorhanden.

Aus datenschutzrechtlicher Sicht ist das Verfahren der Anästhesiologie von besonderer Bedeutung, weil das gesamte System – sowohl Software als auch Hardware – nicht im UKE gewartet wird, sondern vollständig per Standleitung aus San Diego in Kalifornien. Auf der ferngewarteten Anlage werden sehr sensible medizinische Daten gespeichert, die nicht nur aufgrund datenschutzrechtlicher Regelungen vor unberechtigtem Zugriff zu schützen sind. Ihre unbefugte Offenbarung ist außerdem bei einem Verstoß gegen die ärztliche Schweigepflicht nach § 203 StGB strafbar. Daher sind an die technische Sicherheit und an den Betrieb des Verfahrens sehr hohe Anforderungen zu stellen, zumal in den USA keine mit deutschen Regelungen vergleichbaren Datenschutzgesetze existieren.

Mit dem Ziel, sowohl eine hohe Verfügbarkeit als auch einen hohen Datensicherheitsstandard bei der Patientenüberwachungsanlage umzusetzen, wurden bereits im September 1992 einvernehmlich mit dem UKE zahlreiche Maßnahmen vereinbart. So sollten sämtliche über Namen und Geburtsdatum hinausgehenden personenbezogenen Daten auf einem separaten, vom UKE gewarteten PC gespeichert werden, um den Zugriff auf Patientendaten im Rahmen der Fernwartung von vornherein einzuschränken. Sämtliche Fernwartungsaktivitäten sollten zudem manipulationssicher protokolliert werden. Da die Protokollierung kurzfristig nicht realisierbar war, sollte der Datenverkehr mit San Diego zumindest online per Monitor überwacht werden können (vgl. 11.TB, 3.3).

Leider mußten wir jedoch bei einem Besuch vor Ort im April 1994 feststellen, daß von den vereinbarten Maßnahmen kaum etwas umgesetzt war. Fernwartungsaktivitäten wurden weder protokolliert, noch konnten sie bei Bedarf auf einem Monitor mitverfolgt werden. Das UKE hat im Anschluß an unseren Besuch zumindest die verabredete Protokollierung installiert. Die Auswertung der Protokollierung, etwa die Suche nach einem möglicherweise unbefugten Kopierbefehl zu Mißbrauchszwecken, ist jedoch nur mit einem großen technischen Aufwand möglich. Das UKE will die erforderliche Programmierung für eine derartige Auswertung aber erst bei einem konkreten Verdacht vornehmen.

Problematisch ist vor allem die Tatsache, daß das UKE die Kontrolle des Systems praktisch vollständig dem Hersteller in San Diego überläßt. Zwar gibt es im UKE mehrere Ansprechpartner mit speziellen Systemkenntnissen. Dennoch muß selbst bei kleineren Systemänderungen, wie beispielsweise dem Verändern von Anwendungsparametern, permanent der Hersteller in San Diego hinzugezogen werden. Hierdurch wird das Risiko unnötig erhöht, daß personenbezogene Daten unbefugt in die USA übermittelt werden.

Wir hatten das UKE daher aufgefordert, sich vom Hersteller privilegierte Zugriffsrechte geben zu lassen und einen Teil der Systemwartung selbst durchzuführen. Sollte der Hersteller die Übertragung privilegierter Rechte auf das UKE aus urheberrechtlichen oder wettbewerbsrechtlichen Gründen nicht akzeptieren, käme es auch in Betracht, die örtliche Systempflege durch einen inländischen Beauftragten durchzuführen.

Unter diesen Voraussetzungen könnten wir es akzeptieren, wenn zur Beseitigung komplexer Systemfehler der Hersteller in San Diego weiterhin jederzeit auf das System zugreifen darf. Um auch in zeitkritischen Fehlersituationen die Patientenversorgung nicht zu gefährden, muß die Fernwartung ausnahmsweise nicht – wie wir sonst immer fordern (vgl. 11.TB, 3.3) – ausdrücklich durch Techniker des UKE freigegeben werden.

Allerdings sollte der Systemzugriff per Fernwartung abgestuft erfolgen: In der Regel soll die Anlage nur mit nicht-privilegierten Rechten ferngewartet werden. Erst wenn diese nicht ausreichen, darf der Fernwartungstechniker auf den privilegierten Superuser-Status wechseln. Der abgestufte Zugriff gehört zu den anerkannten Grundregeln des Datenschutzes, um Mißbrauchsmöglichkeiten von vornherein einzuschränken.

Das UKE hatte diese Forderungen insoweit akzeptiert, als der Systemzugriff per Fernwartung abgestuft erfolgen sollte. Dies hat der Hersteller jedoch abgelehnt. Das UKE hat sich im Einvernehmen mit dem Hersteller auch bereit erklärt, den privilegierten Systemzugriff zur Überwachung der Fernwartung wahrzunehmen, der sich allerdings auf eine Leseberechtigung („View only") beschränkt. Das UKE lehnt es jedoch weiterhin ab, Wartungsarbeiten künftig selbst durchzuführen. Auch der Hersteller sieht sich nur in der Lage, ausschließlich lesenden Zugriff auf alle Dateien und Prozeßzustände zu gewähren. Zu einer partiellen Übernahme der Systemverwaltung durch das UKE führt diese Maßnahme mithin nicht.

Durch die dargestellten Maßnahmen kann einem Datenmißbrauch durch Fernwartungstechniker des Herstellers nicht ausreichend vorgebeugt werden. So wäre es z.B. in keiner Weise zu verhindern (möglicherweise noch nicht einmal zu entdecken), daß ein Techniker vom Aufenthalt eines Prominenten in der Intensivstation des UKE, von seiner Krankheit und Behandlung Kenntnis erlangt

und diese Kenntnis an interessierte Dritte weitergibt und entsprechende Systemaktivitätäten verschleiert.

Aus diesem Grunde habe ich mich entschlossen, das Verfahren bei dem Präsidenten der Universität nach § 25 HmbDSG formell zu beanstanden.

21.8 Übermittlung von Patientendaten an Krankenkassen

Im Berichtszeitraum hatten wir wieder einige Eingaben zu beantworten, die sich gegen die Anforderung von Patientenunterlagen durch die gesetzliche Krankenkasse wandten (21.8.2). In einem anderen Fall ging es um die Übermittlung von Daten für die Behandlung einer Versicherungsangestellten an ihren Arbeitgeber (21.8.3).

21.8.1 Übermittlung durch die Kassenärztliche Vereinigung

Bei den Vorbereitungen zu unserem Leitfaden „Datenschutz in der Arztpraxis" stießen wir auf die Praxis der Kassenärztlichen Vereinigung Hamburg, den Krankenkassen mit der Abrechnung auch die einzelnen Behandlungsscheine zu übermitteln. Wir halten dies für einen Verstoß gegen § 295 Abs.2 Sozialgesetzbuch V (SGB V). Diese Vorschrift läßt eine Angabe über die abgerechneten Leistungen nur „fallbezogen, nicht versichertenbezogen" zu.

Als Grundlage für den Datenaustausch zwischen Kassenärztlicher Vereinigung und Kassen sieht das SGB V eine Vereinbarung zwischen den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung vor. Zu einem entsprechenden Entwurf auf Bundesebene nahm der Bundesbeauftragte für den Datenschutz Stellung. Im Rahmen des Arbeitskreises „Gesundheit und Soziales" der Datenschenschutzbeauftragten beteiligen wir uns an den weiterführenden Erörterungen, um für die auf Landesebene erfolgende Datenübermittlung eine datenschutzgerechte Praxis zu gewährleisten.

21.8.2 Übermittlung durch Ärzte und Krankenhäuser

Einzelne Ärzte fragten uns, ob sie der Bitte von Krankenkassen um Befunde oder Entlassungsberichte von Patienten nachkommen dürfen.

Nach § 295 SGB V haben Vertragsärzte bei der Abrechnung ihrer Leistungen zwar Diagnosen mitzuteilen, Befunde jedoch nur bei einer zahnärztlichen Behandlung. Wir begrüßten es deswegen, daß die Kassenärztliche Vereinigung Hamburg (KVH) in ihrem Rundschreiben 1/94 alle Vertragsärzte bat, „künftig auf die Angabe des Befundes auf allen einschlägigen Vordrucken zu verzichten." Auf unsere Rückfrage bestätigte die KVH, daß dies auch für die Arbeitsunfähigkeitsbescheinigung gilt, die direkt an die Kassen übersandt wird.

Krankenhausärzte wehrten sich zu Recht gegen die pauschale Abforderung von Entlassungsberichten durch die Krankenkassen. In § 301 SGB V ist abschließend aufgezählt, welche Daten die Krankenhäuser an die Kassen weiterzugeben haben. Dazu gehören zwar die Aufnahme- und Entlassungsdiagnose und Angaben über durchgeführte Rehabilitationsmaßnahmen, nicht jedoch die Entlassungsberichte. Diese sind in erster Linie für nachbehandelnde Ärzte bestimmt und gehen in ihrem inhaltlichen Umfang weit über das hinaus, was die Kassen für ihre Abrechnungszwecke benötigen.

Auch über die Hausärzte darf selbstverständlich nicht verlangt werden, was die Krankenhäuser direkt nicht zu übermitteln haben.

In Einzelfällen hat die Krankenkasse jedoch den Medizinischen Dienst zu beauftragen, gutachtlich Stellung zu nehmen zu „Voraussetzung, Art und Umfang der Leistung" und z.B. bei Arbeitsunfähigkeit, § 275 SGB V. Hierzu hat die Kasse dem Medizinischen Dienst die dafür erforderlichen – bei ihr vorhandenen – Unterlagen vorzulegen, aber keine neuen beim Arzt anzufordern. Ob eine Prüfung durch den Medizinischen Dienst geboten ist, ergibt sich häufig jedoch erst durch weitere Unterlagen.

Mit der AOK Hamburg haben wir deswegen für diese Fälle ein Musterschreiben entwickelt, in dem die Versicherten gebeten werden, in eine zeitweise Überlassung von bestimmten Patientenunterlagen durch den Arzt einzuwilligen. In diesem Schreiben werden Anlaß, Zweck und Verfahren der Prüfung beschrieben und als Folge einer Verweigerung der Schweigepflichtentbindung die direkte Anforderung durch den Medizinischen Dienst benannt. Da diese zusätzlichen Unterlagen nicht bei der Kasse, sondern ggf. beim Medizinischen Dienst verbleiben, gehen wir davon aus, daß hiermit ein tragfähiger Kompromiß zwischen dem informationellen Selbstbestimmungsrecht des Patienten und den praktischen Erfordernissen der Krankenkasse gefunden wurde.

21.8.3 Übermittlung bei Krankenkassen-Mitarbeitern

Eine Angestellte einer Krankenversicherung machte uns auf folgendes Problem aufmerksam: Als sie zur Behandlung in ein Krankenhaus aufgenommen wurde, habe sie diesem mitgeteilt, daß ihre Versicherung zugleich ihr Arbeitgeber sei und daß die Abrechnung deswegen über eine spezielle Geschäftsstelle abgewickelt werden solle. Dies wurde zugesagt, aber aufgrund von Urlaubsvertretungen nicht eingehalten: Der Arbeitgeber erfuhr von der Diagnose und der durchgeführten Heilbehandlung seiner Mitarbeiterin.

Um solche Fehlleistungen in Zukunft zu vermeiden, vereinbarten wir mit dem betroffenen Krankenhaus eine Änderung im EDV-System. Während für die Krankenversicherung bisher nur die eine Hauptgeschäftsstelle im System eingetragen und somit automatisch bei jeder Korrespondenz mit dieser Versicherung angeschrieben wurde, wird bei der Aufnahme von Versicherungs-Beschäftigten nun die dafür zuständige Geschäftsstelle in den Datensatz der aufzunehmenden Patientin selbst aufgenommen.

21.9 Qualitätssicherung bei Röntgenaufnahmen

Röntgenaufnahmen unterliegen einerseits einer technischen Prüfung ohne Patientenbezug nach § 16 Röntgenverordnung (RöntgVO) und zum anderen der patientenbezogenen medizinischen Qualitätskontrolle nach §§ 136 f. Sozialgesetzbuch V (SGB V). Die technische Prüfung führt nach § 16 Abs.3 RöntgVO eine „Ärztliche Stelle" durch; die medizinische Kontrolle obliegt bei Vertragsärzten der Radiologiekommission der Kassenärztlichen Vereinigung, bei Krankenhäusern der Krankenkasse.

In Hamburg schlossen die Behörde für Arbeit, Jugend und Soziales, die Ärztekammer und die Kassenärztliche Vereinigung 1988 einen Vertrag, durch den einer gemeinsamen „Ärztlichen Stelle" sowohl die technische als auch die medizinische Prüfung aller Röntgenaufnahmen übertragen wurde.

Die Praxis sieht anders aus: Die Ärztliche Stelle besteht neben dem Plenum aus Prüfgremien, in die Ärztekammer und Kassenärztliche Vereinigung Sachverständige im Verhältnis 2:1 bzw. 1:2 entsenden – je nachdem, ob Röntgenaufnahmen von Krankenhäusern oder von Vertragsärzten zu prüfen sind. Diese Gremien nehmen nur die technische Prüfung vor, fordern aber neben den nach § 16 RöntgVO notwendigen Unterlagen auch den zur Röntgenaufnahme gehörenden patientenbezogenen Befund von den Ärzten ab.

Während eine medizinische Qualitätskontrolle der Aufnahmen von Krankenhausärzten nicht stattfindet, werden die Aufnahmen von Vertragsärzten durch die Ärztliche Stelle an die Radiologiekommission der Kassenärztlichen Vereinigung zur Fachprüfung weitergegeben. Zwischen den verschiedenen Prüfgremien besteht weitgehende Personalidentität.

Die datenschutzrechtliche Prüfung und die jahrelange Auseinandersetzung mit den betroffenen Institutionen führte im Juni 1994 zu einem gemeinsamen Gespräch und einem Kompromißvorschlag durch uns:

Die Personalidentität der Prüfgremien hielten wir wegen der notwendigen Fachqualifikation für weitgehend unvermeidbar. Wegen der notwendigen Zuordnung der Aufnahmen nahmen wir auch für die technische Prüfung hin, daß jede Röntgenaufnahme selbst im sog. Skribor den Namen des Patienten trägt. Die Befunde sind jedoch nur von Vertragsärzten, nicht von Krankenhäusern abzufordern, weil eine medizinische Prüfung hier gar nicht erfolgt. Da aber die technische Prüfung auch bei Aufnahmen von Vertragsärzten nach § 16 RöntgVO ohne Befunde auskommen muß, regten wir eine Umkehrung des Weitergabeverfahrens an: Nicht die Ärztliche Stelle, sondern die Radiologiekommission soll von den Vertragsärzten die Unterlagen für beide Prüfungen abfordern, nach der medizinischen Prüfung aber nur die Aufnahmen selbst – ohne Befunde – zur technischen Prüfung an die Ärztliche Stelle weitergeben. Dem Vertragsarzt wird dieses Verfahren mitgeteilt. Widerspricht er ihm, gibt die Radiologiekommission nur den Namen des Arztes an die Ärztliche Stelle weiter, die ihrerseits die Röntgenaufnahme für die technische Prüfung abfordern kann.

Die Ärztekammer Hamburg und die Kassenärztliche Vereinigung Hamburg teilen unsere Rechtsauffassung nicht, ohne daß sie sich mit den Bedenken auseinandersetzen. Die Kassenärztliche Vereinigung ist gleichwohl bereit, den beschriebenen Kompromißvorschlag „für zukünftige Verfahren (zu) berücksichtigen". Die an dem Gespräch beteiligten Vertreter/innen der Behörde für Arbeit, Gesundheit und Soziales haben auf unser Schreiben vom Juli 1994 bislang nicht reagiert. Ihnen hatten wir insbesondere eine Überprüfung des Vertrages über die Ärztliche Stelle von 1988 nahegelegt.

21.10 Formulare des Landesbetriebes Krankenhäuser

Ein Ergebnis der datenschutzrechtlichen Prüfung des Allgemeinen Krankenhauses (AK) Altona 1985 war, daß der Landesbetrieb Krankenhäuser (LBK) auf einige Daten der Patientenerfassungsbelege verzichtete bzw. sie der freiwilligen Angabe überließ (6.TB, 4.16.1.4). Bei der Prüfung des AK St.Georg (oben 21.4) wurden wir auf verschiedene Erfassungs-Formulare aufmerksam, die dem seinerzeit gefundenen Konsens nur zum Teil entsprachen. Da es sich auch um zentrale Vordrucke des Landesbetriebs handelte, suchten wir mit der Geschäftsführung des LBK eine Klärung.

In einem gemeinsamen Gespräch am 1. August 1994 wurde folgendes vereinbart:

— In den Behandlungsvertrag wird entsprechend den Datenschutzempfehlungen des LBK nunmehr eine Klausel aufgenommen, in der der Patient sich mit der Heranziehung alter Krankenunterlagen einverstanden erklärt bzw. diese ablehnt. Ferner wird der mißverständliche Begriff „sozialer Status" durch „Familienstand" ersetzt. Diese Angabe ist nach der Rechtsprechung erforderlich, um die Behandlungskosten nötigenfalls beim mitverpflichteten Ehegatten des Patienten geltend machen zu können.

— Die LBK-Geschäftsführung weist die Krankenhäuser ferner auf folgendes hin: In den Durchschriften des Notfallberichtes für die Kassenärztliche Vereinigung und die Krankenhausverwaltung sind die Felder „Vorgeschichte", „Befund" und „Röntgenbefund" unkenntlich zu machen. Angaben zu „Arbeitgeber / Beruf" sollen in allen Formularen mit dem Zusatz „nur bei Arbeits- und Wegeunfällen" versehen werden. Die Angabe „Datum und Ort des Grenzübertritts" ist in allen Formularen zu streichen. Die LBK-Geschäftsführung hat die Krankenhäuser mit Schreiben vom 9. und 19. August 1994 entsprechend unterrichtet.

Nicht erreicht werden konnte ein Verzicht auf die Daten „Geburtsname" und „Staatsangehörigkeit" der Patienten. Die Krankenhäuser sehen sich durch entsprechende Forderungen der Krankenkassen veranlaßt, diese Angaben zu er-

fassen und weiterzugeben. Die Krankenkassen benötigen den Geburtsnamen zur Zuordnung früherer Vorgänge. Die Staatsangehörigkeit sei zuweilen Merkmal für besondere staatliche Unterstützungsmaßnahmen, die der Zahlungspflicht der Krankenkassen vorgehen.

21.11 „Schwarze Arzt-Listen" einer Patientenberatungsstelle

1993 hatte uns eine Patientenberatungsstelle gebeten, sie bei der Einrichtung einer EDV-gestützten Dokumentation ihrer Arbeit zu beraten. Es sollten auch Ärzte, über die sich besonders viele Patienten beschweren, ermittelt werden können. Wir gaben Hinweise und Formulierungshilfen für die Einwilligungserklärung der Patienten und das Unterrichtungsschreiben an die Ärzte, über die im System eine Beschwerde gespeichert ist.

Nach mehreren Medienberichten über „schwarze Listen" der Patientenberatungsstelle wandte sich im April 1994 die Ärztekammer Hamburg an uns, um auf den Vorgang aufmerksam zu machen. Außerdem teilte sie uns mit, daß sie die Beratungsstelle mehrfach erfolglos um die Namen der angegriffenen Ärzte gebeten habe.

Mit der Patientenberatungsstelle wurden darauf hin noch einmal Einzelheiten der Datenverarbeitung geklärt: Um zu vermeiden, daß unbedeutende und ungeklärte Behauptungen automatisiert gespeichert und abrufbar sind, werden Beschwerden, die keiner weiteren Bearbeitung bedürfen, überhaupt nicht erfaßt. Bei gravierenderen Beschwerden, die eine Aufklärung erfordern, werden die Personalien der beschwerdeführenden Person und des genannten Arztes sowie der vorgetragene Sachverhalt gespeichert.

Über die Beschwerde und, wenn die beschwerdeführende Person zustimmt, deren Personalien wird der betroffene Arzt schriftlich unterrichtet und auf sein Auskunftsrecht hingewiesen. Die Beratungsstelle bittet ihn ggf. um Stellungnahme und um Übersendung der Patientenunterlagen in Kopie.

Die beschwerdeführende Person hat aber auch das Recht, die Übermittlung ihres Namens an den angegriffenen Arzt abzulehnen. Dies ergibt sich aus § 33 Abs.2 Nr.3 Bundesdatenschutzgesetz, der eine Pflicht zur Benachrichtigung insoweit ausschließt, als die Daten „wegen des überwiegenden rechtlichen Interesses eines Dritten geheimgehalten werden müssen". Sowohl das Interesse der beschwerdeführenden Person, Mißstände auch ohne Angst vor persönlichen Gegenangriffen (z.B. Strafanzeigen wegen Verleumdung oder Beleidigung) vorbringen zu können, als auch das Interesse der Beratungsstelle an Informationen, die ohne Einhaltung der Vertraulichkeit ausblieben , rechtfertigen eine Benachrichtigung ohne den Namen der beschwerdeführenden Person.

Will der Patient anonym bleiben und ist eine Klärung der Beschwerde wegen des dazu notwendigen patientenbezogenen Rückgriffs auf die konkrete Behandlung nicht möglich, werden alle Daten nach spätestens 3 Monaten gelöscht. Unaufgeklärte Sachverhalte und einseitige Behauptungen bleiben also nicht im System gespeichert.

Zum Wunsch der Ärztekammer, die Namen der kritisierten Ärzte für eigene Ermittlungen zu erfahren, erklärte die Beratungsstelle, dies sei erst nach einer (Vor-)Klärung des Vorwurfs sinnvoll. Wir sahen – schon aus Gründen des Datenschutzes für die Ärzte – keinen Anlaß, ein anderes Verfahren vorzuschlagen.

Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

22. Schufa

22.1 Mieterdatenschutz und Schufa- Selbstauskunft

Die Aufsichtsbehörde hatte sich in der Vergangenheit bereits mit der Praxis der Vermieter befaßt, von Mietinteressenten eine Selbstauskunft über ihre persönlichen und wirtschaftlichen Verhältnisse zu verlangen (vgl. 11. TB, 30.2). Im Berichtszeitraum sind uns nunmehr einige Fälle bekanntgeworden, in denen Vermieter von den Mietinteressenten bzw. deren Bürgen regelmäßig die Vorlage einer Schufa-Selbstauskunft verlangen.

Hierzu ist anzumerken, daß ein Vermieter selbstverständlich das Recht hat, sich ein Bild über die Einkommensverhältnisse eines Wohnungsbewerbers zu verschaffen. Jedoch bestehen aus folgenden Gründen datenschutzrechtliche Bedenken gegen eine regelmäßige Vorlage von Schufa-Selbstauskünften:

- Vertragspartner der Schufa können Kreditinstitute, Leasinggesellschaften, Einzelhandelsunternehmen einschließlich des Versandhandels, Kreditkartengesellschaften und sonstige Unternehmen sein, die gewerbsmäßig Geld- oder Warenkredite an Konsumenten geben. Wohnungsvermieter gehören also nicht zu den Schufa-Vertragspartnern mit der Folge, daß diese Unternehmen auch keine Auskunft aus dem Datenbestand der Schufa erhalten. In den Schufa-Richtlinien wird ausdrücklich darauf hingewiesen, daß Anfragen bei der Schufa zur Vermietung von Wohn-und Geschäftsräumen unzulässig sind. Durch die Forderung der Vermieter nach einer regelmäßigen Vorlage der Schufa-Selbstauskunft werden diese Schufa-Richtlinien unterlaufen.

- Eine Schufa-Selbstauskunft beinhaltet Angaben über Kontoverbindungen sowie registrierte kreditrelevante Merkmale. Hierzu gehören etwa Angaben über eingegangene Verpflichtungen. Es ist nicht ersichtlich, daß für die Beurteilung der Zahlungswilligkeit und Zahlungsfähigkeit bezüglich der Miete ein lückenloser Überblick über die bei der Schufa gespeicherten Daten erforderlich ist. Vielmehr werden dem Vermieter dadurch zahlreiche Informationen bekannt, die für den Abschluß eines Mietvertrages nicht benötigt werden. Das Mittel der Schufa-Selbstauskunft ist daher für diesen Zweck auch unverhältnismäßig.

- Nicht nachvollziehbar ist die Forderung nach einer Schufa-Selbstauskunft insbesondere in den Fällen, in denen die Zahlung der Miete auf andere Weise sichergestellt ist. Solange beispielsweise eine Mietübernahmeerklärung des Sozialamtes Gültigkeit hat, treten wirtschaftliche Risiken für den Vermieter nicht auf (vgl. 7. TB, 5.7.2).

- Nach § 34 BDSG haben diejenigen, deren Daten bei Kreditauskunfteien gespeichert sind, ein Recht auf eine Auskunft. Diese Vorschrift soll die Tätigkeit solcher Unternehmen transparenter machen und dazu beitragen, die Rechte der Betroffenen zu schützen. Die regelmäßige Nutzung dieses gesetzlichen Schutzrechts zu dem Zweck, die allgemeine Bonität eines Wohnungsbewerbers zu prüfen, bedeutet eine Verkehrung des gesetzlichen Sinns und der Zielrichtung des Auskunftsrechts.

Angesichts der dargestellten Bedenken sind Zweifel an der datenschutzrechtlichen Zulässigkeit eines derartigen Verlangens angebracht. Gemäß § 28 Abs. 1 Satz 2 BDSG müssen diejenigen Daten, die nach dieser Vorschrift verarbeitet werden, nach Treu und Glauben und auf rechtmäßige Weise erhoben worden sein. Es verstößt aber gegen Treu und Glauben, wenn eine Selbstauskunft nicht eindeutig freiwillig ist; den Mietinteressenten drohen unangemessene Nachteile, weil sie ohne „freiwillige" Selbstauskunft nicht weiter vom Vermieter berücksichtigt werden.

Die vorstehenden Überlegungen gelten auch für einen Bürgen, der sich zur Übernahme der finanziellen Verpflichtungen aus dem Mietverhältnis bereiterklärt. Es dürfte in aller Regel ausreichend sein, daß er seine Zahlungsfähigkeit anhand von Einkommensbelegen nachweist, ohne zusätzlich auch noch eine Schufa-Selbstauskunft beibringen zu müssen.

22.2 Überprüfung des berechtigten Interesses

Die von der Schufa gegenüber den Obersten Aufsichtsbehörden der Länder zugesagte Prüfung eines Kompromißvorschlags, nach dem sich die Anzahl der Stichproben gestaffelt nach der Anzahl der monatlichen Auskünfte pro Geschäftsstelle richten soll (vgl. 12. TB, 23.2), ist noch nicht endgültig abgeschlossen. Zwischenzeitlich teilte die Schufa jedoch mit, daß einem Unternehmen der Auftrag erteilt wurde, ein Programm auszuarbeiten, mit dessen Hilfe Anfragen zur Prüfung des berechtigten Interesses unter Eingabe verschiedener Varianten herausgefiltert werden können.

22.3 Zugriffsrechte der Geschäftsstellen

Die Aufsichtsbehörde hat sich im Berichtszeitraum mit der Frage der Zugriffsrechte auf personenbezogene Daten auch bei der Schufa-Organisation befaßt. Die Schufa unterhält in Deutschland acht Gesellschaften, die wiederum bis zu sechs Geschäftsstellen haben. Die jeweiligen Geschäftsstellen einer Gesellschaft, die auf mehrere Bundesländer verteilt sein können, haben dabei unbeschränkten Zugriff auf den gesamten Datenbestand der Gesellschaft, der sie angehören.

Es wird zu prüfen sein, ob diese Verfahrensweise ohne jegliche Einschränkung unter datenschutzrechtlichen Aspekten zulässig ist.

23. Versicherungswirtschaft

23.1 Automationsentwicklung

Nach der zunächst im Jahre 1993 eingetretenen Verzögerung bei der Einführung des phonetischen Strukturcode-Verfahrens (vgl. zuletzt 12. TB, 24.1) soll die Umstellung aller zentralen Warn- und Hinweissysteme nunmehr abgeschlossen werden. Die Versicherungswirtschaft hat den Obersten Aufsichtsbehörden zugesichert, daß nach der Kfz-Datei noch im Jahre 1994 die Unfall-, Rechtsschutz- und Sachversicherer-Dateien auf das neue Verfahren übergehen.

23.2 Gesetzliche Neuregelungen

Mit Einführung des europäischen Binnenmarktes auf dem Gebiet des Versicherungswesens zum 1. Juli 1994 wurde es erforderlich, das Versicherungsvertragsgesetz (VVG) und das Versicherungsaufsichtsgesetz (VAG) der veränderten Rechtslage anzupassen. Die Gespräche der Obersten Aufsichtsbehörden mit der Versicherungswirtschaft wurden dabei insbesondere von zwei Neuregelungen beeinflußt:

Geschäftsplanmäßige Erklärungen sind aufgrund der abschließenden Aufzählung der Geschäftsplanbestandteile in § 5 Abs. 3 VAG nicht mehr Gegenstand des Geschäftsplans, der durch das Bundesaufsichtsamt für das Versicherungswesen (BAV) zu genehmigen ist. Für die vor dem 29. Juli 1994 abgeschlossenen Versicherungsverträge sind die geschäftsplanmäßigen Erklärungen grundsätzlich weiterhin maßgebend. Dies gilt auch für solche Verträge, die unter Zugrundelegung der vom BAV genehmigten Versicherungsbedingungen bis zum 31. Dezember 1994 geschlossen wurden. Die Konsequenz daraus ist, daß die von den Obersten Aufsichtsbehörden unter Beteiligung des BAV mit der Versicherungswirtschaft vereinbarten und vom BAV genehmigten Einwilligungs- und Schweigepflicht-Entbindungserklärungen für Verträge nicht mehr verbindlich sind, die nach Inkrafttreten des neuen VAG abgeschlossen werden. Diese aus datenschutzrechtlicher Sicht erhebliche Verschlechterung hat das BAV zu folgender Verlautbarung veranlaßt:

> „Die Versicherer haben die Bestimmungen des BDSG zu beachten. Insofern empfiehlt es sich, die genannten Erklärungen weiterhin zu verwenden bzw. sich vor etwaigen Änderungen mit den zuständigen Datenschutz-Aufsichtsbehörden abzustimmen."

Außerdem hat das BAV gemäß § 81 Abs. 2 Satz 1 VAG das Recht, bei Vorliegen eines Mißstandes Anordnungen zu treffen. Das BAV hat angekündigt, von dieser Möglichkeit bei gegebener Veranlassung Gebrauch zu machen. Es ist

daher davon auszugehen, daß die Versicherungsunternehmen auch im Hinblick auf die Verpflichtungen des Bundesdatenschutzgesetzes die mit den Aufsichtsbehörden vereinbarten Formulierungen weiterhin verwenden werden.

Darüber hinaus sind die Versicherungsunternehmen nunmehr verpflichtet, jedem Kunden gleichzeitig mit der Versicherungspolice umfangreiche Informationen zu übersenden. Bedauerlicherweise müssen diese Informationen nicht schon vor Abschluß des Vertrages gegeben werden. Diese Regelung wirkt sich sowohl auf den Zeitpunkt für die neu vereinbarte Einwilligungsklausel (vgl. 23.4) als auch auf den Zeitpunkt der Aushändigung des Merkblatts zur Datenverarbeitung (vgl. 23.5) aus.

Erwähnenswert ist darüber hinaus im Zusammenhang mit der Neuregelung des VAG die erweiterte örtliche Zuständigkeit des BAV. Gem. § 85 VAG erstreckt sich die Aufsicht über das Inland hinaus auf die in anderen Mitgliedsstaaten der Europäischen Gemeinschaft und anderen Vertragsstaaten des EWR-Abkommens über Niederlassungen oder im Dienstleistungsverkehr ausgeübte Geschäftstätigkeit. Dabei wird – mit Ausnahme der Finanzaufsicht – die Aufsicht im Zusammenwirken mit der Aufsichtsbehörde des anderen Mitgliedsstaates wahrgenommen. Diese Bestimmung unterscheidet sich insofern von der datenschutzrechtlichen Zuständigkeit nach dem Entwurf der EG-Datenschutzrichtlinie (vgl. 1.8), als die Aufsichtsbehörde für den Datenschutz die Niederlassungen nur im Inland kontrolliert (vgl. Art. 4 Abs. 1 a) i.V.m. Art. 2 d) EG-Richtlinie).

23.3 Projektgruppe Datenschutz des Europarates

Die Arbeitsgruppe 14 „Versicherungswesen" der Projektgruppe Datenschutz des Europarates erarbeitet eine Empfehlung zum Schutz personenbezogener Daten, die zu Versicherungszwecken erhoben und verarbeitet werden. Das Bundesministerium des Innern hat die Obersten Aufsichtsbehörden für den Datenschutz um Stellungnahme zu einem ersten Entwurf der Empfehlung gebeten.

Zwar ist es zu begrüßen, daß auch auf europäischer Ebene der Schutz personenbezogener Daten von Versicherungsnehmern thematisiert wird. Der vorgelegte erste Entwurf enthält jedoch viele sprachliche und inhaltliche Abweichungen von der kurzfristig zu erwartenden EG-Datenschutzrichtlinie. Daher haben sich die Obersten Aufsichtsbehörden der Länder in ihrer Stellungnahme dafür ausgesprochen, im Ergebnis zu mit der Richtlinie übereinstimmenden Formulierungen zu gelangen.

23.4 Allfinanz-Konzepte und Einwilligungserklärung

Erwartungsgemäß wurde im Berichtszeitraum zwischen den Obersten Aufsichtsbehörden der Länder und der Versicherungswirtschaft die Neufassung

der Einwilligungsklausel nach dem Bundesdatenschutzgesetz vereinbart (vgl. 12. TB, 24.3). Die Versicherungsanträge werden künftig folgende, von den übrigen Erklärungen deutlich unterscheidbare, gesondert zu unterzeichnende Einwilligung enthalten:

„Ich willige [ferner] ein, daß der Versicherer im erforderlichen Umfang Daten, die sich aus den Antragsunterlagen oder der Vertragsdurchführung (Beiträge, Versicherungsfälle, Risiko-/Vertragsänderungen) ergeben, an Rückversicherer zur Beurteilung des Risikos und zur Abwicklung der Rückversicherung sowie zur Beurteilung des Risikos und der Ansprüche an andere Versicherer [und/oder an den ... Verband zur Weitergabe dieser Daten an andere Versicherer] übermittelt. Diese Einwilligung gilt auch [unabhängig vom Zustandekommen des Vertrages sowie] für entsprechende Prüfungen bei anderweitig beantragten (Versicherungs-) Verträgen und bei künftigen Anträgen.

Ich willige ferner ein, daß die Versicherer [Unternehmen] der ... Gruppe meine allgemeinen Antrags-, Vertrags- und Leistungsdaten in gemeinsamen Datensammlungen führen und an den/die für mich zuständigen Vermittler weitergeben, soweit dies der ordnungsgemäßen Durchführung meiner Versicherungsangelegenheiten dient.

[Gesundheitsdaten dürfen nur an Personen- und Rückversicherer übermittelt werden; an Vermittler dürfen sie nur weitergegeben werden, soweit es zur Vertragsgestaltung erforderlich ist.]

[Ohne Einfluß auf den Vertrag und jederzeit widerrufbar willige ich weiter ein, daß der/die Vermittler meine allgemeinen Antrags-, Vertrags- und Leistungsdaten darüber hinaus für die Beratung und Betreuung auch in sonstigen Finanzdienstleistungen nutzen darf/dürfen.]

Diese Einwilligung gilt nur, wenn ich bei Antragstellung vom Inhalt des Merkblatts zur Datenverarbeitung Kenntnis nehmen konnte, das mir vor Vertragsabschluß [mit weiteren Verbraucherinformationen], auf Wunsch auch sofort überlassen wird."

Durchgehend wurde das in der vorangegangenen Fassung verwendete Wort „Vertreter" durch „Vermittler" ersetzt, um klarzustellen, daß neben Einzelpersonen auch Vermittlungsgesellschaften Versicherungsverträge vermitteln können.

Im zweiten Absatz der Erklärung wird nunmehr deutlich, daß die gemeinsamen Datensammlungen der Versicherer ausschließlich dem Zweck der ordnungsgemäßen Durchführung der Versicherungsangelegenheiten dienen.

Der neu eingefügte 4. Absatz enthält die in langwierigen Verhandlungen zwischen den Obersten Aufsichtsbehörden und der Versicherungswirtschaft erzielte Einigung über die Einwilligung in die Nutzung personenbezogener Daten für andere als vertragsbezogene Zwecke. Dieser Textteil ist in Klammern gesetzt, weil er nur von solchen Unternehmen verwendet wird, die Allfinanzziele verfolgen.

Zu begrüßen ist, daß der Versicherungsnehmer diesen Absatz schon nach dem Wortlaut jederzeit folgenlos streichen und auch nachträglich widerrufen kann. Versicherungsnehmer, die die Verwendung ihrer personenbezogenen Daten auf die mit dem jeweiligen Vertrag in Zusammenhang stehenden Zwecke beschränken wollen, haben daher keine Nachteile für ihre Versicherung zu erwarten.

Klargestellt wird durch diese Formulierung auch, daß der Vermittler die personenbezogenen Daten nicht zum Zwecke der Beratung und Betreuung in sonstigen Finanzdienstleistungen erhält. Er darf lediglich die aus Gründen der Versicherungsvertragsabwicklung bei ihm vorhandenen personenbezogenen Daten für diese Zwecke bei entsprechender Einwilligung nutzen.

23.5 Merkblatt zur Datenverarbeitung

Die neugefaßte Einwilligungsklausel enthält erfreulicherweise nunmehr auch die Möglichkeit für den Versicherungskunden, sich das Merkblatt zur Datenverarbeitung schon bei Antragstellung aushändigen zu lassen. Spätestens muß es jedoch von den Unternehmen zusammen mit den übrigen Verbraucherinformationen bei Vertragsschluß übersandt werden.

Damit kann sich jeder Betroffene rechtzeitig und umfassend darüber informieren, wie die Versicherungsunternehmen mit seinen personenbezogenen Daten umgehen und welche Verarbeitungs- und Nutzungsmöglichkeiten konkret vorgesehen sind.

Dies gewinnt besondere Bedeutung vor dem Hintergrund, daß auch das Merkblatt unter Beteiligung der Obersten Aufsichtsbehörden verändert worden ist. Es enthält nunmehr genaue Darstellungen insbesondere auch zur Nutzung personenbezogener Daten für sonstige Finanzdienstleistungen.

Ein Abdruck an dieser Stelle ist wegen der Länge des Merkblatts nicht möglich.

23.6 Private Pflegeversicherung

Nach Inkrafttreten des Pflege-Versicherungsgesetzes vom 26. Mai 1994 zeigte sich, daß im neunten Kapitel des zentralen Teils des Gesetzes, nämlich des neuen 11. Buches Sozialgesetzbuch, zwar die Grundsätze der Datenverwendung für die soziale Pflegeversicherung geregelt sind, entsprechende Vorschriften für die private Pflegeversicherung jedoch fehlen.

Auch bei der privaten Pflegeversicherung besteht ein Kontrahierungszwang für die Vertragspartner. Daher war die Frage zu klären, ob die bei den privaten Krankenversicherern bereits vorhandenen Einwilligungs- und Schweigepflicht-Entbindungserklärungen auf die Pflegeversicherung erstreckt werden können.

Die Versicherungswirtschaft vertrat ursprünglich die Auffassung, daß der Pflegeversicherungsschutz eine kraft Gesetzes eingetretene Erweiterung des vorhandenen Krankenversicherungsschutzes sei und daher die in diesem Zusammenhang abgegebene Einwilligungserklärung nach dem Bundesdatenschutzgesetz auch für die Pflegeversicherung gelte. Im Rahmen der Gespräche zwischen den Obersten Aufsichtsbehörden und der Versicherungswirtschaft wurde diese Meinung jedoch aufgegeben. Es besteht Einvernehmen darüber, daß ohne die Einwilligungserklärung, die bei den übrigen Versicherungsverträgen abgefordert wird, lediglich eine Verwendung der Daten im gesetzlich zulässigen Rahmen möglich ist.

Die Versicherungswirtschaft vertrat die Ansicht, daß die Schweigepflicht-Entbindungserklärung im Leistungsfall der Pflegeversicherung bereits in der Geltendmachung von Ansprüchen gegen den Versicherer ohne ausdrückliche Erklärung enthalten sei oder sich sogar aus der Kranken- auf die Pflegeversicherung erstrecke.

Diese Auffassung konnte von den Obersten Aufsichtsbehörden nicht geteilt werden. Bei Schweigepflicht-Entbindungserklärungen handelt es sich um Einwilligungstatbestände nach dem Strafgesetzbuch, die Verschwiegenheitspflichten von Angehörigen der Heilberufe im Einzelfall aufheben. Insofern ist es ausgeschlossen, bereits vorliegende Erklärungen zu übertragen. Auch die Geltendmachung von Leistungsansprüchen berechtigt den Versicherer nicht, ohne ausdrückliche Einwilligung des Betroffenen weitergehende Erkundigungen bei Ärzten oder anderen Angehörigen von Heilberufen einzuholen.

Die Versicherungswirtschaft sicherte letztlich die Einholung der Schweigepflicht-Entbindungserklärung bei der Geltendmachung von Leistungsansprüchen im Rahmen der Pflegeversicherung zu.

Darüber hinaus wurde vereinbart, daß in einem von den Versicherungsunternehmen an die Betroffenen zu übersendenden Merkblatt über die Pflegeversicherung eine Passage über den Datenschutz aufgenommen wird.

23.7 Registrierung von Versicherungsvermittlern

Nachdem die Bundesregierung nicht zur Umsetzung der Empfehlung der EG-Kommission vom 18. Dezember 1991 (vgl. 12. TB, 24.8.4) tätig wurde, plant die Versicherungswirtschaft, den in der Empfehlung enthaltenen Gedanken mittels einer eigenen Datei zu verwirklichen.

Die EG-Empfehlung sieht vor, daß nur noch in ein Register eingetragene Personen, die bestimmten Anforderungen genügen, die Tätigkeit eines Versicherungsvermittlers aufnehmen und ausüben dürfen. Jeder Mitgliedsstaat soll eine zuständige Stelle benennen, die das Register führt.

Die Versicherungswirtschaft legte den Obersten Aufsichtsbehörden der Länder die Entwürfe für eine Satzung des Zentralregisters für Versicherungsvermittler in Deutschland e. V. sowie Richtlinien für die Registrierung und Auskunftserteilung durch das Zentralregister für Versicherungsvermittler in Deutschland e. V. zur datenschutzrechtlichen Beurteilung vor. Zweck des Vereins soll die Errichtung und Führung eines zentralen Registers für in Deutschland tätige hauptberufliche Versicherungsvermittler entsprechend der Empfehlung der EG-Kommission sein.

Neben der Tatsache, daß die Richtlinien für die Registrierung erhebliche datenschutzrechtliche Mängel aufweisen, werfen sie Probleme im Bereich des europäischen Gemeinschaftsrechts wie auch der verfassungsrechtlichen Zulässigkeit auf. So ist derzeit noch nicht ausreichend geklärt, ob nach der EG-Empfehlung auch ausländische Vermittler gespeichert werden dürfen, sofern sie auch für inländische Unternehmen tätig sind. Darüber hinaus sollen nicht registrierte Vermittler von der Ausübung dieses Berufs ausgeschlossen werden.

Angesichts der schwerwiegenden Bedenken haben die Obersten Aufsichtsbehörden der Versicherungswirtschaft mitgeteilt, daß letztlich auf die Empfehlung der EG-Kommission über Versicherungsvermittler abzustellen sei. Aus europa- und verfassungsrechtlicher Sicht wird keine Möglichkeit gesehen, eine derartige Datei ins Leben zu rufen, solange nicht die Bundesrepublik Deutschland als Mitgliedsstaat diejenige Stelle, die das Register führen soll, benannt hat.

23.8 Datensammlung über Versicherungsmakler

Durch eine Eingabe wurde die Aufsichtsbehörde Hamburg auf eine Datensammlung über Makler und Mehrfachagenten aus dem gesamten Bundesgebiet bei einem Versicherungsunternehmen aufmerksam gemacht.

Aus diesem Anlaß erfolgte bei dem Unternehmen eine unangemeldete Prüfung gemäß § 38 Abs. 1 BDSG. Es stellte sich heraus, daß die Betreuer, die jeweils für eine bestimmte Anzahl von vertraglich an das Unternehmen gebundenen Versicherungsvermittlern zuständig sind, mit tragbaren Computern (sog. Laptops) ausgestattet sind. Aus der bei dem Unternehmen vorhandenen Datenbank werden den Betreuern die vertragsbezogenen Daten der betroffenen Makler oder Mehrfachagenten übertragen. Darüber hinaus enthielt die Datenbank bestimmte Datenfelder, die mit freien oder auch mit vordefinierten Inhalten auszufüllen waren.

Zu den persönlichen Daten konnten z.B. Familienstand, Anzahl, Geschlecht und Geburtsdatum der Kinder, Ehrenämter, Hobbys und „Sonstiges" gespeichert werden. Das Wissen und die Kenntnisse der Betroffenen wurden regelrecht einer auf einer Skala auszuwählenden Bewertung unterzogen, die u.a.

Angaben über Fachwissen oder Personalführung enthielt. Ein weiteres Datenfeld führte zur Einstufung in den Bereichen Ausführungsarten, Verhaltensweisen, Eigenschaften zu Begriffen wie „kommunikativ, vertrauenswürdig, partnerschaftlich, analytisch, erfolgreich" und etlichen weiteren Kriterien.

In all diese Datenverarbeitungen hatten die Betroffenen nicht eingewilligt. Sie waren darüber nicht einmal informiert.

Maßstab der datenschutzrechtlichen Prüfung durch die Aufsichtsbehörde war § 4 Abs. 1 BDSG, wonach die Nutzung und Verarbeitung personenbezogener Daten nur zulässig ist, wenn eine Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.

Die Verarbeitung derjenigen Daten, die mit dem Agenturvertrag in direktem Zusammenhang stehen oder sich auf die aktuelle Erreichbarkeit der Betroffenen beziehen, ist gemäß § 28 Abs. 1 Nr. 1 BDSG im Rahmen der Zweckbestimmung des Vertragsverhältnisses zulässig.

Anders fiel die Beurteilung jedoch bei Daten wie Familienstand, Anzahl, Geschlecht und Geburtsdatum der Kinder, Ehrenämter, Hobbys und „Sonstiges" aus. Diese Daten standen in keinem Zusammenhang zu dem bestehenden Vertragsverhältnis, sondern dienten lediglich dem Sammeln von Informationen über persönliche Verhältnisse des jeweils Betroffenen. Dabei war zu berücksichtigen, daß selbst das Fragerecht eines Arbeitgebers bei Eingehung eines Arbeitsverhältnisses durch die Rechtsprechung auf tätigkeitsbezogene Fragen eingeschränkt ist. Hier handelt es sich sogar um Betroffene, die nicht als Arbeitnehmer, sondern selbständig tätig sind.

Ein noch strengerer Maßstab war bei den Bewertungen und Einstufungen der Versicherungsvermittler hinsichtlich Wissen, Kenntnissen, Ausführungsarten, Verhaltensweisen und Eigenschaften anzulegen. Jede Erhebung von Daten muß gemäß § 28 Abs. 1 Satz 2 BDSG nach Treu und Glauben und auf rechtmäßige Weise erfolgen. Die Tatsache, daß die Bewertungen ohne Einwilligung, sogar ohne Kenntnis der Betroffenen vorgenommen wurden, führte schon zur Unzulässigkeit der Erhebung dieser Daten. Dabei war erschwerend zu berücksichtigen, daß es sich hier um eine Art Beurteilungswesen handelte, das selbst in dem sehr viel engeren Verhältnis eines Arbeitsvertrages einem festen Verfahren mit Akteneinsichts- und Gegenäußerungsrecht unterliegt.

Die Aufsichtsbehörde hat dem Unternehmen ihre eingehende datenschutzrechtliche Bewertung zukommen lassen. Daraufhin wurden sämtliche als unzulässig bezeichneten Daten gelöscht. Eine Nachprüfung hat ergeben, daß die Betreuer der Makler und Mehrfachagenten auch nicht mehr die Möglichkeit haben, diese Daten erneut auf dem Laptop zu speichern.

23.9 Grenzüberschreitender Datenverkehr

Nachdem der Binnenmarkt auf dem Gebiet des Versicherungswesens geöffnet worden ist (vgl. 23.2), könnte es zu einer Teilnahme ausländischer Versicherer an den Zentralen Warn- und Hinweissystemen der Versicherungswirtschaft kommen. Damit würde die Kontrolle dieser äußerst sensiblen Daten, die sich auf das Verhalten von Versicherungsnehmern beziehen und nur unter besonderen Voraussetzungen in diese Systeme eingestellt werden dürfen, erheblich erschwert werden.

Auch die Vertreter der Versicherungswirtschaft schließen derartige Übermittlungen für die Zukunft nicht aus. Es wird insbesondere unter Berücksichtigung der europäischen Gesetzgebung zu prüfen sein, unter welchen Voraussetzungen die Weitergabe derart sensibler Daten ins Ausland zulässig ist.

23.10 Hamburger Feuerkasse

Am 1. Juli 1994 ist die Hamburger Feuerkasse mit der Eintragung in das Handelsregister in eine Aktiengesellschaft umgewandelt worden. Dieser Umwandlung lag das Gesetz zur Neuordnung der Rechtsverhältnisse der Hamburger Feuerkasse vom 29. März 1994 zugrunde. An der Beratung des Gesetzes sind wir erst spät beteiligt worden, obwohl davon in besonderem Maße personenbezogene Daten der betroffenen Versicherungsnehmer berührt waren.

Die Eigentümer von Gebäuden und Nebenanlagen im hamburgischen Staatsgebiet waren nach dem bisherigen Feuerkassengesetz verpflichtet, eine Gebäudeversicherung bei der Hamburger Feuerkasse abzuschließen. Sie konnten davon ausgehen, daß die aufgrund des Gesetzes von ihnen erhobenen Daten ausschließlich für Zwecke der Gebäudeversicherung verwendet worden sind. Dies wäre mit der Aufhebung des Versicherungsmonopols und dem geplanten Verkauf an ein Unternehmen, das auch in anderen Versicherungssparten tätig war, nicht mehr zweifelsfrei der Fall gewesen.

Zudem war zu diesem Zeitpunkt bereits festgelegt worden, daß die neue Aktiengesellschaft ihr Angebot an Sachversicherungen erweitern sollte. Hierfür hätten nicht nur die Adressen der Versicherungsnehmer für die Werbung von wirtschaftlichem Interesse sein können. Vielmehr hätten sich auch mit den in den Versicherungsunterlagen enthaltenen Zusatzinformationen, z. B. der Inneneinrichtung von Gebäuden und einzelnen Wohnungen, gezielte Angebote für Hausratversicherungen an bestimmte Eigentümer erstellen lassen.

Der Gesetzentwurf enthielt jedoch aus datenschutzrechtlicher Sicht keinerlei Bestimmungen, die eine solche Zweckentfremdung im Interesse der bisherigen Versicherungsnehmer ausgeschlossen hätte. Während die öffentlich-rechtlichen Versicherungsverhältnisse bereits zum 30. Juni 1994 in privatrechtliche umgewandelt und damit für das neue Unternehmen auch zu anderen Zwecken nutzbar geworden wären, sollten die einzelnen Versiche-

rungsnehmer erst zum 31. Dezember 1994 die Möglichkeit erhalten, ihre bestehende Gebäudeversicherung kündigen und nach eigener Entscheidung bei anderen Unternehmen einen neuen Vertrag abschließen zu können.

Zudem wäre für die Verarbeitung ihrer personenbezogenen Daten ab dem 1. Juli 1994 das Bundesdatenschutzgesetz zur Anwendung gekommen. Damit hätten die Versicherungsnehmer gegenüber dem bis dahin geltenden Hamburgischen Datenschutzgesetz einen geringeren Schutz.

Wir haben deshalb der Finanzbehörde Vorschläge zur Ergänzung des Überleitungsgesetzes unterbreitet. Diese beinhalteten, daß

— das Hamburgische Datenschutzgesetz bis zum Ablauf der Kündigungsfrist für die Verarbeitung der Versichertendaten Geltung behalten sollte,

— die neue Aktiengesellschaft bei fristgerechter Kündigung eines Versicherungsnehmers die Daten nur noch zur Abwicklung des Versicherungsverhältnisses nach Maßgabe des Hamburgischen Datenschutzgesetzes hätte verarbeiten dürfen,

— die Aktiengesellschaft sicherzustellen hätte, daß die Daten aus der gesetzlichen Gebäudeversicherung und die Daten aus dem Geschäft mit anderen Versicherungssparten durch personell und organisatorisch getrennte Stellen verarbeitet werden.

Die Finanzbehörde vertrat die Auffassung, daß dem Land Hamburg bei der Umwandlung der Feuerkasse in eine Aktiengesellschaft die Gesetzgebungskompetenz fehle, für einen wenn auch nur befristeten Übergangszeitraum das Hamburgische Datenschutzgesetz an die Stelle des Bundesdatenschutzgesetzes treten zu lassen. Wir haben daraufhin die datenschutzrechtliche Problematik zunächst in die Beratungen des bürgerschaftlichen Haushaltsausschusses eingebracht.

Nachdem auch die Justizbehörde die bereits von der Finanzbehörde vertretene Rechtsauffassung bestätigt hatte, wurden unsere Vorschläge zwar nicht direkt im Überleitungsgesetz berücksichtigt. Wir konnten aber eine Lösung erreichen, die den datenschutzrechtlichen Belangen der Versicherten Rechnung trug. Mit Zustimmung des Käufers der Aktiengesellschaft hat sich die Hamburger Feuerkasse im Februar 1994 schriftlich verpflichtet,

— ihren Versicherten bis zum 30. September 1994 ohne vorherige schriftliche Einwilligung keine gezielten Angebote von Versicherungen zu machen, denen über Name und Anschrift hinaus konkrete Daten aus dem bestehenden Versicherungsverhältnis zugrundelagen,

— bis zum 30. September 1994 keine Daten von Versicherten an Dritte weiterzugeben,

— soweit Versicherte fristgerecht von ihrem erstmaligen Kündigungsrecht Gebrauch gemacht haben, ihre Daten nur zur Abwicklung des Versicherungsverhältnisses zu verarbeiten.

24. Handels- und Wirtschaftsauskunfteien

24.1 Telefonisches Auskunftsverfahren

Die Überprüfung des telefonischen Auskunftsverfahrens (vgl. 12. TB, 25.1.4) durch die Handelsauskunfteien ist noch nicht abgeschlossen. Problematisch ist weiterhin, daß nicht einmal der anfragende Mitarbeiter eines Unternehmens im Auskunftsprotokoll erfaßt wird. Die Angelegenheit wird weiter verfolgt.

24.2 Zeitpunkt des Benachrichtigungsschreibens

Wie berichtet (vgl. 12. TB, 25.2.3), fertigte die von uns überprüfte Handelsauskunftei aus organisatorischen Gründen alle 6 Wochen bis 3 Monate schubweise Benachrichtigungsschreiben an die Betroffenen. Auf unseren Einwand hin, daß diese Frist zu lang sei, hat die Auskunftei die bisherige Praxis geändert. Sie führt nunmehr die nach § 33 BDSG erforderliche Benachrichtigung innerhalb eines Zeitraumes von 4 Wochen nach Auskunftserteilung durch.

24.3 Dauer der Speicherung des berechtigten Interesses

Bei der Prüfung der Handelsauskunftei stellten wir fest, daß die Daten über den Anfragenden nur 6 Monate beim Datensatz des Betroffenen gespeichert wurden (vgl. 12. TB, 25.2.4). Da das Benachrichtigungsschreiben nach § 33 BDSG regelmäßig erst alle 6 Wochen bis 3 Monate an die Betroffenen versandt wurde, hielten wir mindestens ein Jahr für die Speicherung des Auskunftsersuchens für erforderlich. Die zu diesem Aufbewahrungsverfahren geäußerten Bedenken konnten angesichts der mittlerweile erheblich kürzeren Benachrichtigungsfrist (24.2) aufgegeben werden.

24.4 Nachmeldungen

Nachmeldungen von Negativdaten werden von der geprüften Handelsauskunftei ohne weitere konkrete Anfrage 6 Monate nach der ersten Auskunft erteilt (vgl. 12. TB, 25.2.5). Gegen dieses Nachmeldeverfahren haben wir Bedenken erhoben, da die Übermittlung von personenbezogenen Daten gemäß § 29 Abs. 2 Nr. 1a BDSG nur zulässig ist, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat.

Die Angelegenheit ist noch nicht abgeschlossen und wird im Kreis der Obersten Aufsichtsbehörden weiterverfolgt.

25. Versandhandel

25.1 Adreßdatei von Negativkonten

Durch die Mitteilung einer anderen Aufsichtsbehörde haben wir davon erfahren, daß ein Versandhandelsunternehmen in Hamburg eine Adreßdatei führt, in der negative Daten über Kaufinteressenten und Kunden vorgehalten werden. Dies haben wir zum Anlaß genommen, die Datei gemäß § 38 Abs. 1 BDSG zu überprüfen. Da die Gespräche mit dem Unternehmen über unsere Feststellungen noch nicht abgeschlossen sind, soll an dieser Stelle lediglich über den mittlerweile erreichten Sachstand berichtet werden.

Das Unternehmen führt die Adreßdatei von Negativkonten auch über Personen, die bei einigen konzernverbundenen Versandhäusern mit Sitz in anderen Bundesländern als Kaufinteressenten oder Kunden aufgetreten sind. Die unterschiedlichen Firmennamen der Versandhäuser geben keinen Hinweis auf die Konzernverflechtung der Unternehmen.

Diese zum Firmenverbund gehörenden Versandhäuser können im Online-Verfahren lesend und schreibend auf die Datei zugreifen. Die Daten sind somit entweder vom anfragenden Versandhaus selbst zu einem früheren Zeitpunkt eingespeichert worden, d.h. es werden die dem Unternehmen bereits bekannten Daten abgerufen, oder es handelt sich um den Abruf von Daten, die von einem oder mehreren der anderen Versandhäuser eingespeichert worden sind. Der Abruf erfolgt routinemäßig, wenn ein Kunde die Lieferung der Ware gegen offene Rechnung wünscht. Hierbei wird nicht unterschieden, ob die Bestellung schriftlich oder telefonisch eingegangen ist.

Die Datei enthält zahlreiche personenbezogene Angaben sowie Beurteilungs- und Zuordnungskennziffern über die Kunden. Die Betroffenen werden weder vor der Bestellung einer Ware darüber unterrichtet, daß sie unter bestimmten Umständen in diese Datei aufgenommen werden, noch erhalten sie hierüber zu einem späteren Zeitpunkt eine entsprechende Nachricht.

Wir haben dem Unternehmen mitgeteilt, daß Zweifel an der datenschutzrechtlichen Zulässigkeit des gegenwärtigen Verfahrens angebracht sind. Unsere Kritik betrifft dabei im wesentlichen folgende Punkte:

1. Das Versandhaus darf zwar die Daten seiner Kaufinteressenten und Kunden in der Adreßdatei für eigene Zwecke grundsätzlich gemäß § 28 Abs. 1 Nr. 1 BDSG zur Abwicklung eines Bestellvorganges speichern und nutzen. Über die eigentliche Vertragsabwicklung hinaus ist dies jedoch ohne vorherige Information des Kunden nicht zulässig, weil der Kunde wegen der unterlassenen Unterrichtung eine weitere Streuung seiner eventuell vorhandenen Negativdaten nicht verhindern kann. Wüßte er von der Existenz der Datei, könnte er sich entscheiden, ob das Versandhaus z.B. über eine Schufa-Auskunft nähere Angaben über ihn erhalten soll oder ob er lieber per Nachnahme bestellt. Die Interessen des Kunden sind insoweit schützenswert und höher zu bewerten als die Interessen des Versandhauses.

2. Die Speicherung von problematischen Anschriften ohne Personennamen führt im Ergebnis dazu, daß einzelne Kunden von dem Unternehmen als sozial schwach oder sogar als Insassen von Strafvollzugsanstalten identifiziert werden. Ohne vorherige Information der Betroffenen über die Möglichkeit, diese Einzelanschriften zuzuordnen, kommt es ohne Wissen der Kunden zu einer Stigmatisierung. Daher besteht Grund zu der Annahme, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verwendung dieser Daten überwiegt. Von großer Bedeutung bei dieser Abwägung ist die Tatsache, daß mit einer vorherigen Information die Möglichkeit eröffnet würde, durch Bestellung gegen Nachnahme oder gar Verzicht auf die Bestellung einer Offenlegung sensibelster privater Verhältnisse aus dem Wege zu gehen.

3. Die schutzwürdigen Interessen der Versandhauskunden sind in jedem Fall der Maßstab, an dem sich die Zulässigkeit von Datenübermittlungen an die konzernverbundenen Unternehmen zu orientieren hat. Hierbei ist zu berücksichtigen, daß den Betroffenen selten die Verflechtung der Unternehmen bekannt ist. Insoweit rechnen sie auch in keiner Weise mit einer unternehmensübergreifenden „Warndatei". Somit ist auch in den Fällen, in denen die Speicherung für die eigene Nutzung zulässig ist, die Übermittlung an die übrigen Versandhäuser unzulässig. Wir können eine solche „Warndatei" nur akzeptieren, wenn die Kunden vor der Abgabe ihrer Bestellung in geeigneter Form darüber aufgeklärt werden, unter welchen Voraussetzungen ihre Daten in die Datei aufgenommen werden und wer die möglichen Übermitttlungsempfänger sind.

Das Versandhaus teilt bislang unsere datenschutzrechtliche Einschätzung des Verfahrens nicht. So vertritt das Unternehmen die Auffassung, die Übermittlung von Negativdaten im Konzern sei zur Wahrung berechtigter Interessen der einzelnen Unternehmen erforderlich, ohne daß Grund zu der Annahme besteht, daß der Kunde ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat (vgl. § 28 Abs. 2 Nr. 1a BDSG). Dies wird damit begründet, daß

— die Speicherung der Negativdaten nur für einen begrenzten Zeitraum erfolge,

— die einzelnen Tochtergesellschaften als Vertragspartner der Schufa auch von dort direkt Auskünfte über die Zahlungsfähigkeit des Kunden einholen könnten,

— der Betroffene selbst zur Streuung seiner Negativdaten beitrage, indem er nach Ablehnung durch ein Versandhandelsunternehmen bei einem anderen Versandhandelsunternehmen eine Bestellung aufgebe, obwohl er

wisse, daß dieses Unternehmen grundsätzlich nicht gegen Nachnahme, sondern nur gegen Rechnung liefere.

Im übrigen wird auf die im Katalog abgedruckten Allgemeinen Geschäftsbedingungen verwiesen, in denen ausreichende Hinweise für die Speicherung und Übermittlung der Daten enthalten seien. Der Kunde würde aufgrund dieses Hinweises durchaus damit rechnen, daß auch die bei der Kreditprüfung erlangten Daten weitergegeben werden würden.

Bei der Speicherung von problematischen Anschriften handele es sich im übrigen nicht um eine Datei mit personenbezogenen Daten. Vielmehr könnten diese Angaben beispielsweise auch aus örtlichen Straßenverzeichnissen entnommen werden.

Das Versandhaus hat sich bis zum Redaktionsschluß ungeachtet der von ihr vertretenen Rechtsauffassung bereiterklärt, die Hinweise zum Datenschutz im Katalog redaktionell neu zu fassen und optisch besser zu plazieren.

Da die Angelegenheit nicht nur für den hamburgischen Bereich von Bedeutung ist, werden wir die Gesamtproblematik zunächst grundsätzlich im Kreis der übrigen Obersten Aufsichtsbehörden der Länder erörtern. Sobald dieser Abstimmungsprozeß abgeschlossen ist, werden wir die Gespräche mit dem Versandhaus fortsetzen und das Ergebnis in unserem nächsten Tätigkeitsbericht darstellen.

26. Kreditwirtschaft

26.1 Beschränkung des Zugriffs auf Kontoinformationen

Bei Kreditinstituten, die innerhalb Hamburgs oder anderer örtlicher Grenzen mehrere Zweigstellen betreiben, ist es üblich, daß der Zugriff auf die Kontoinformationen von allen Zweigstellen erfolgen kann. Dies eröffnet dem Kunden die Möglichkeit, neben der kontoführenden auch weitere Zweigstellen aufzusuchen, die auf vollständige Kontoinformationen zurückgreifen können.

Damit verbunden ist jedoch eine erhebliche Erweiterung von Datenmißbrauchsmöglichkeiten, die bei einer Vielzahl von Mitarbeitern in unterschiedlichen Zweigstellen kaum noch kontrolliert werden können. Eine Anzahl von mehr als 200 Zweigstellen eines Unternehmens wird dabei keine Seltenheit sein. Die Aufdeckung von Mißbrauchsfällen ist allenfalls zufällig oder in den seltenen Fällen möglich, in denen ein Betroffener sich infolge eines entsprechenden Verdachts beschwert.

Vor diesem Hintergrund wird eine Abwägung zwischen dem Interesse der Kreditwirtschaft, ihre Kunden umfassend in mehreren Zweigstellen bedienen zu können, und dem berechtigten Anliegen von Betroffenen, sensible Daten vor dem Zugriff Unberechtigter zu schützen, zu treffen sein.

Die seitens der Kreditwirtschaft zu diesem Thema bisher vorliegenden Äußerungen weisen im wesentlichen darauf hin, daß Bankgeheimnis, Arbeitsverträge und Datenschutzgesetze Mißbräuche untersagen und daß die Mitarbeiter darüber informiert sind. Dennoch bekanntgewordene Fälle würden entsprechend geahndet.

Die Obersten Aufsichtsbehörden der Länder halten jedoch eine Eingrenzung der Zugriffsmöglichkeiten, um Mißbräuche von vornherein auszuschließen, für erforderlich. Dies muß auch nicht – wie von den Kreditinstituten befürchtet wird – zu Lasten der Kundenfreundlichkeit oder Praktikabilität gehen. Vielmehr sollte angestrebt werden, ein Wahlrecht mit der Möglichkeit des Zugriffs für eine, mehrere oder alle Zweigstellen des Unternehmens einzuführen. Im Einzelfall können die Mitarbeiter fremder Zweigstellen immer noch auf die fremden Daten zugreifen, wenn der Betroffene dies z.B. mit der EC-Karte ermöglicht.

Die Obersten Aufsichtsbehörden werden Gespräche mit der Kreditwirtschaft über die Beschränkung des Zugriffs auf Kontoinformationen aufnehmen.

26.2 Kartengestützte Zahlungsverfahren

26.2.1 Euroscheck-Karte und Chipkarten

Im 12. TB (26.1) hatten wir über die Überlegungen des Kreditgewerbes berichtet, die Euroscheck-Karte mit einem multifunktionalen Computer-Chip auszustatten. Auf Anregung der Aufsichtsbehörden für den Datenschutz kam es im Rahmen der Arbeitsgruppe Kreditwirtschaft im März 1994 zu einem Informationsaustausch zwischen Vertretern des Zentralen Kreditausschusses (ZKA) und den Obersten Aufsichtsbehörden. Die Vertreter des ZKA erklärten dabei, daß sobald wie möglich ein multifunktionaler Chip auf der EC-Karte eingeführt werden soll, um damit das elektronische Bezahlen an der Ladenkasse zu erleichtern.

Im Gegensatz zum bisherigen EC-Cash-Zahlungsverfahren (vgl. 11. TB, 27.1) ermöglicht der in der EC-Karte integrierte Chip eine Offline-Abwicklung von Zahlungsvorgängen, solange sich diese in dem Rahmen bewegen, der durch den Kartenausgeber festgelegt wurde. Eine Identifizierung gegenüber der Autorisierungszentrale entfällt, wodurch sich für den Handel die Kosten der Transaktion verringern. Erst bei Überschreiten des Maximalbetrages erfolgt eine Online-Autorisierung.

Diese Grundfunktion der Karte soll ergänzt werden durch eine Telefonanwendung. Sie enthält ein spezielles, aufladbares, vorausbezahltes Guthaben auf der Chipkarte, so daß die EC-Karte wie eine Telefonkarte nutzbar ist.

Das Kreditgewerbe beabsichtigt außerdem, eine Börse für Kleinbeträge auf dem Chip anzubieten. Es wird dabei zum einen die Variante einer vorausbezahlten Börse geplant, für die ein bestimmter Betrag als Guthaben geladen

wird (Prepaid-Verfahren). Die Zahlungen aus der Börse erfolgen dann anonym durch Abbuchung des auf der Chipkarte verfügbaren Betrages.

Andererseits wird an eine vorautorisierte Börse gedacht. Hierbei wird aus dem allgemeinen Verfügungsrahmen ein vorautorisierter Verfügungsbetrag geladen. Die Zahlung bei der vorautorisierten Börse erfolgt nicht anonym. Aus Sicht des Datenschutzes ist die „datenfreie" anonyme Zahlung, d. h. die vorbezahlte Börse, die datenschutzfreundlichere Lösung.

Eine abschließende datenschutzrechtliche Bewertung der verschiedenen Anwendungsmöglichkeiten der EC-Karte ist derzeit noch nicht möglich. Im Zusammenhang mit dem kartengestützten Zahlungsverkehr durch Offline-Abwicklung wird auf unsere Darstellung des EC-Cash-Verfahrens im 11. TB (27.1) verwiesen. Es bleibt abzuwarten, wie den datenschutzrechtlichen Anforderungen bei der weiteren Funktion des Offline-Verfahrens entsprochen wird.

Das Kreditgewerbe plante zunächst ab Januar 1995 in Stuttgart einen Feldversuch mit ca. 1,5 Millionen Kunden. Der Versuch sollte die drei verschiedenen Anwendungsmöglichkeiten der Chip-Karte (electronic-cash, Telefonanwendung und elektronische Geldbörse) erfassen. Nach Angaben des ZKA wird der geplante Feldversuch nicht stattfinden. Beabsichtigt ist nunmehr im Laufe des Jahres 1995 ein Testlauf mit einigen tausend Teilnehmern. Wir werden die weitere Entwicklung beobachten und darüber berichten.

26.2.2 Fahrkartenverkauf mit Euroscheck-Karte beim Hamburger Verkehrsverbund (HVV)

Der HVV hat am 21. Oktober 1994 zunächst mit dem Verkauf von Zeitkarten mit Hilfe der Euroscheck-Karte (EC-Karte) begonnen. Im Laufe des Jahres 1995 soll es auch möglich sein, Einzelfahrscheine des HVV mit der EC-Karte zu bezahlen. Damit ist – zumindest bis auf weiteres – eine Systementscheidung getroffen worden, deren datenschutzrechtliche Risiken wir bereits im 12. TB (27.1) dargestellt haben.

Das jetzt vom HVV eingeführte „Postpaid-Verfahren", bei dem das Fahrgeld nachträglich vom Konto des Fahrgastes abgebucht wird, ist zwar beim Verkauf von Zeitkarten weniger problematisch. Allerdings würde es beim Kauf von Einzelfahrscheinen dazu führen, daß Ort und Zeit nachvollziehbar werden.

In den Gesprächen mit dem HVV haben wir deshalb weiterhin die Einführung eines „Prepaid-Verfahrens" gefordert, das – wie bei den Telefonkarten – im voraus bezahlte Wertkarten verwendet und normalerweise eine Verarbeitung von Kundendaten vermeidet. Das vom HVV entwickelte System ist so aufgebaut, daß dort grundsätzlich auch solche vorausbezahlten Karten eingesetzt werden können. Der HVV will deshalb auch eine „Prepaid-Karte" neben der EC-Karte akzeptieren, sobald sie bundesweit verfügbar ist.

Im übrigen ist in den Bedingungen für die bargeldlose Fahrgeldzahlung im Bereich des HVV-Gemeinschaftstarifs festgelegt worden, daß die Möglichkeit erhalten bleibt, Fahrkarten mit Bargeld zu erwerben. Der Fahrgast kann sich daher – gemäß unserer Forderung – weiterhin für die „datenfreie" Fahrt entscheiden.

Das EC-Verfahren soll in den nächsten Jahren schrittweise auf weitere Verkaufswege z.B. im Bus und an Automaten ausgeweitet werden, insbesondere um neue Kunden für den Öffentlichen Personennahverkehr zu gewinnen und den Fahrkartenverkauf wirtschaftlicher zu gestalten. Wir haben dem HVV empfohlen, das „Postpaid-Verfahren" lediglich übergangsweise bis zum Einsatz eines „Prepaid-Verfahrens" zu verwenden und jedenfalls vor einer Ausweitung folgende Vorkehrungen zu treffen, um Bewegungsprofile auszuschließen:

Die Kassennummer, aus der sich der Standort des benutzten Fahrkartenautomaten herleiten läßt, und die genaue Uhrzeit des Fahrkartenkaufs dürfen nur wenige Tage gespeichert werden, um den technischen Ablauf kontrollieren zu können. Danach ist die Speicherung des Tages ausreichend, an dem die Fahrkarte gekauft wurde.

Demgegenüber sollen nach dem derzeitigen Verfahren die Kassennummer und die genaue Uhrzeit des Fahrkartenkaufs sieben Jahre gespeichert werden. Der HVV hat aber eine Prüfung durch seinen Wirtschaftsprüfer angekündigt, ob die Speicherung der genauen Uhrzeit, die vom Zentralen Kreditausschuß (ZKA) gefordert werde, und der Kassennummer über längere Zeit notwendig ist. Der HVV hat erklärt, er habe kein Interesse an der Speicherung entbehrlicher personenbezogener Daten.

27. Auftragsdatenverarbeitung

Auftraggeber, die andere Stellen mit der Verarbeitung oder Nutzung personenbezogener Daten beauftragen, haben ihren Sitz vielfach nicht am Ort des Auftragnehmers. Dies bedeutet, daß personenbezogene Daten auch über die Grenzen Hamburgs transportiert werden. Dies geschieht beispielsweise bei Service-Rechenzentren durch Online-Verbindungen oder Datenträgeraustausch.

Werden Akten oder Datenträger vernichtet sowie Schriftgut oder der Inhalt von Datenträgern verfilmt, findet die Dienstleistung am Ort des Auftragnehmers statt. Das Material muß zum Auftragnehmer gebracht werden oder vom Auftraggeber abgeholt werden.

Die hierbei zu treffenden technischen und organisatorischen Maßnahmen, die vom Auftraggeber in dem schriftlichen Auftrag nach § 11 Abs. 2 BDSG festgelegt werden müssen, haben somit einen besonderen Stellenwert. Bei unseren Prüfungen haben wir deshalb darauf hingewirkt, daß die Datenschutzvereinbarungen präzise Regelungen enthalten.

27.1 Verpflichtung des Auftraggebers nach § 11 BDSG

Bei den im Berichtszeitraum geprüften Unternehmen, die im Auftrag personenbezogene Daten verarbeiten oder nutzen, wurde erneut festgestellt, daß Auftraggeber ihren Verpflichtungen nach § 11 BDSG vielfach nur unzureichend nachgekommen sind (vgl. 12. TB, 28.). Beispielsweise regelte eine vom Auftraggeber entworfene Sicherheits-Vereinbarung, daß die Auftragskontrolle nach Nr. 8 der Anlage zu § 9 Satz 1 BDSG nur vom Auftragnehmer – einschließlich der dazu erforderlichen technischen und organisatorischen Sicherungsmaßnahmen – durchgeführt wird. Einige Datenschutzvereinbarungen enthielten lediglich den Hinweis, daß der Auftragnehmer sich zur Einhaltung der Datenschutzmaßnahmen nach § 9 BDSG verpflichtet oder die Anforderungen des Datenschutzes lückenlos zu beachten hat.

Eine Wiederholung des Gesetzestextes, die Bezugnahme auf § 9 BDSG oder andere globale Formulierungen reichen nicht aus. Es sind vielmehr angepaßt an die konkret vorliegenden Umstände die einzelnen Maßnahmen zu beschreiben.

Wir konnten bei unseren Prüfungen feststellen, daß die Auftragnehmer als meldepflichtige Unternehmen oft besser über die gesetzlichen Anforderungen an die vertraglichen Verpflichtungen nach § 11 Abs. 2 BDSG informiert sind als die Auftraggeber. Insbesondere wird den Auftragnehmern häufig die Formulierung der technischen und organisatorischen Maßnahmen überlassen. Dadurch umgehen die Auftraggeber ihre Verantwortung, Weisungen zur personenbezogenen Datenverarbeitung zu erteilen.

Soweit der Auftragnehmer der Ansicht ist, daß eine Weisung des Auftraggebers gegen Vorschriften des Datenschutzes verstößt, hat er den Auftraggeber gemäß § 11 Abs. 3 Satz 2 BDSG unverzüglich darauf hinzuweisen. Wir haben die Auftragnehmer auf diese Verpflichtung aufmerksam gemacht.

27.2 Akten- und Datenträgervernichtung

Bei der Prüfung der Akten- und Datenträgervernichter hatten wir in den Prüfberichten bemängelt, daß die Auftraggeber keine schriftlichen Aufträge erteilt oder nur unzureichende Regelungen getroffen hatten (vgl. 12. TB, 28.1). In einem Fall hatte die Aufsichtsbehörde erwogen, sich direkt an die Auftraggeber zu wenden, weil sie gegen die gesetzliche Pflicht nach § 11 Abs. 2 BDSG verstoßen haben.

Wir haben erfreut zur Kenntnis genommen, daß die Bemühungen der Auftragnehmer, entsprechende schriftliche Vereinbarungen zu treffen, erfolgreich waren. Darüberhinaus haben die Auftragnehmer erklärt, künftig Material mit personenbezogenen Daten nur aufgrund schriftlicher Aufträge zu vernichten. Dabei ist von Bedeutung, daß dieses Material auch als solches vom Auftraggeber gekennzeichnet wird. Bei einem Unternehmen haben wir festgestellt, daß

ein Auftraggeber personenbezogenes Material als normales Altpapier deklariert hatte. Das Material wurde dementsprechend nach einer geringeren Sicherheitsstufe vernichtet. Der Auftraggeber hatte damit nicht für die vollständige Unkenntlichmachung bei der Vernichtung bzw. Löschung personenbezogener Daten gesorgt.

28. Sonstige Probleme

28.1 Videoüberwachung in der Wirtschaft

Die Aufsichtsbehörde erhält zunehmend Anfragen, unter welchen Voraussetzungen der Einsatz von Videotechnik im nicht-öffentlichen Bereich zulässig ist, da eine Videoüberwachung in das Persönlichkeitsrecht der Betroffenen eingreift (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Schon die Videoaufnahme mit durchlaufenden Bildern ohne Aufzeichnung ist eine Datenerhebung; jede Aufzeichnung ist außerdem eine Datenspeicherung. Da die Betroffenen regelmäßig nicht erkennen können, ob es sich um eine Videoüberwachung ohne oder mit Aufzeichnung handelt, stehen sie unter dem Druck, ihr Verhalten vorsorglich auf die Beobachtung und auf eine etwaige Aufzeichnung auszurichten und dennoch nicht zu wissen, ob und wie etwaige Aufnahmen verwendet werden.

Besonders problematisch ist die Videoüberwachung dann, wenn die Aufnahme und Aufzeichnung der Bilder heimlich erfolgen. Die Intensität des Eingriffs kann auch dadurch erhöht werden, daß an demselben Ort eine regelmäßige Überwachung stattfindet und durch die wiederholte Erfassung der Betroffenen deren Verhalten kontrollierbar wird. Die Betroffenen werden einem zusätzlichen Überwachungsdruck ausgesetzt, wenn sie der Kamera nicht ausweichen können.

Falls es sich um digitalisierte und entsprechend auswertbare Aufnahmen handelt, würde eine Datei nach dem BDSG vorliegen. Die heimliche Datenerhebung und -speicherung könnte dann nach § 28 BDSG unzulässig sein, wenn sie weder auf einem Vertragsverhältnis beruht noch zur Wahrung berechtigter Interessen des Betreibers der Videoanlage im Vergleich mit den schutzwürdigen Interessen der Betroffenen erforderlich ist.

Auch wenn der Dateibegriff nach dem BDSG nicht erfüllt ist, könnten die Betroffenen einen Unterlassungsanspruch geltend machen, der sich unmittelbar aus dem Grundrecht auf Datenschutz als Teil des Persönlichkeitsrechts ergibt (Art. 2 Abs. 1 und Art. 1 Abs. 1 GG). Der Anspruch besteht immer dann, wenn die Überwachung nicht durch das Hausrecht oder durch überwiegende berechtigte Interessen des Betreibers der Videoanlage zu rechtfertigen ist.

Dabei ist der Grundsatz der Verhältnismäßigkeit hinsichtlich Anlaß, Ort und Dauer der Videoüberwachung zu berücksichtigen. Falls eine Videoüberwa-

chung im Einzelfall vertretbar ist, darf sie deshalb noch nicht uneingeschränkt und unbefristet eingeführt werden. Insbesondere sind auch die Rechte der Arbeitnehmer gemäß der Rechtsprechung zu dieser Thematik zu beachten.

Datenschutzrechtlich problematisch ist es erst recht, wenn die Videoüberwachung über den Betriebsbereich hinaus auf die angrenzenden öffentlichen Straßen und Plätze ausgedehnt wird. Allenfalls in aktuellen Gefahrensituationen z.B. nach einer entsprechenden polizeilichen Beratung könnte es vertretbar sein, daß private Unternehmen die Bürger auf öffentlichem Grund überwachen. Regelmäßig geht hier das Recht des Bürgers vor, sich in der Öffentlichkeit ohne private Überwachung frei zu bewegen (siehe auch 4.4).

Sofern die Aufsichtsbehörde Gelegenheit hat, vor der Einrichtung von Videoüberwachungsanlagen die Betreiber zu beraten, wird regelmäßig verlangt, folgende Punkte in einer Dienst- oder Benutzeranweisung festzuschreiben, um die Persönlichkeitsrechte unbeteiligter Dritter zu schützen:

— Beschreibung von Umfang und Zweck der Anlage,

— Festlegung des zulässigen Gebrauchs,

— Hinweise an die Betroffenen über Art und Zeit der Überwachung,

— kurze Aufbewahrungszeit von Aufnahmen, soweit sie nicht für ein strafrechtliches Ermittlungsverfahren benötigt werden,

— Zulässigkeit und Verfahren der Anfertigung und Auswertung von Videoaufzeichnungen,

— Bestimmung des Mitarbeiterkreises, der zur Kontrolle des Videosystems zugelassen ist,

— Festlegung des Verfahrens im Falle einer Mitbenutzung durch die Polizei,

— Vernichtung von Videobändern und evtl. gefertigter Videoprints.

29. Register nach § 32 BDSG und Prüftätigkeit

29.1 Register und Meldepflicht

Die Aufsichtsbehörde führt nach § 38 Abs. 2 BDSG ein Register der Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der personenbezogenen oder der anonymisierten Übermittlung speichern oder im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen. Diese Stellen unterliegen nach § 32 BDSG der Meldepflicht. Derzeit sind zu diesem Register 234 Unternehmen gemeldet. Unterteilt nach der Art der meldepflichtigen Tätigkeit ergibt sich folgendes Bild:

Speicherung zum Zwecke der Übermittlung
Auskunfteien/Warndienste 18
Direktmarketing/Adreßhändler 13

Speicherung zum Zwecke der anonymisierten Übermittlung
Markt- und Meinungsforschung 16

Auftragsdatenverarbeitung
Servicerechenzentren 33
Akten- und Datenträgervernichter 12
Mikroverfilmer 7
Datenerfasser 29
Mailboxen 3
sonst. Auftragsdatenverarbeitung 103

Weiterhin wurden eine Vielzahl von Unternehmen, die bislang nicht zum Register gemeldet waren, angeschrieben und um Prüfung der Meldepflicht und ggfs. Anmeldung gebeten. Der daraus entstehende Informations- und Beratungsbedarf nimmt nach wie vor breiten Raum ein.

Die Umstellungs- und Aktualisierungsarbeiten hinsichtlich einer Automatisierung des Registers und der inhaltlichen Angaben der gemeldeten Unternehmen im Register wurden im Berichtszeitraum fortgesetzt (vgl. 12. TB, 29.1). Dabei sind erneut in einigen Fällen Verstöße gegen die Meldepflicht festgestellt worden. Insbesondere wird gelegentlich übersehen, daß auch für Zweigniederlassungen und unselbständige Zweigstellen eine Meldepflicht besteht. Es reicht daher nicht aus, nur bei der für den Hauptsitz zuständigen Aufsichtsbehörde der Meldepflicht nachzukommen.

Wir haben bisher davon abgesehen, Ordnungswidrigkeitenverfahren einzuleiten, weil die betroffenen Unternehmen die Meldungen umgehend nachgeholt haben.

29.2 Prüfungen

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

Auskunfteien/Warndienste 3
Direktmarketing/Adreßhändler 3
Markt- und Meinungsforschung 17
Servicerechenzentren 1
Akten- und Datenträgervernichter 2
Mikroverfilmer 4
Datenerfasser 4
sonstige Auftragsdatenverarbeitung 3
gesamt 37

Als wesentliche Mängel wurden am häufigsten festgestellt:

— mangelhafte Zugangs- und Abgangskontrolle,

— keine ausreichende Funktionstrennung bei den Mitarbeitern innerhalb des Betriebes,

— kein ausreichender Paßwortschutz,

— Mängel in der Datenträgerkontrolle,

— ungenügende Arbeitsanweisungen zum Umgang mit Datenverarbeitungsanlagen,

— fehlende schriftliche Weisungen der Auftraggeber (vgl. 12. TB, 28.),

— nicht mehr aktuelle Registermeldungen.

Einige kleinere Unternehmen hatten keinen betrieblichen Datenschutzbeauftragten bestellt, obwohl die Voraussetzungen des § 36 BDSG vorlagen. In zahlreichen Fällen bezogen sich die betrieblichen Hinweise zum Datenschutz auf das alte Bundesdatenschutzgesetz. Die geprüften Stellen waren freiwillig bereit, festgestellte Mängel zu beheben. Bußgeldverfahren wurden deshalb nicht eingeleitet.

Darüber hinaus wurde im Rahmen der Anlaßaufsicht nach § 38 Abs. 1 BDSG eine Vielzahl von Unternehmen vor Ort aufgrund von Beschwerden oder Anlässen, z.B. Presseveröffentlichungen, geprüft.

Konferenz der Datenschutzbeauftragten
des Bundes und der Länder

47. Sitzung

9./10. 3. 1994 in Potsdam

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat – bei Stimmenthaltung Bayerns und in Abwesenheit Baden-Württembergs – die folgende

Bestandsaufnahme über die Situation des Datenschutzes „10 Jahre nach dem Volkszählungsurteil"

zustimmend zur Kenntnis genommen.

Nach Ablauf von über 10 Jahren seit der Verkündung des Urteils des Bundesverfassungsgerichtes zum Volkszählungsgesetz am 15. Dezember 1983 sieht sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder veranlaßt, eine Bestandsaufnahme der Situation vorzulegen, in der sich der Datenschutz derzeit befindet.

Entwicklung nach dem Volkszählungsurteil:

Bereits unmittelbar nach Inkrafttreten der Datenschutzgesetze in Bund und Ländern war die Frage heftig diskutiert worden, welchen Rang der Datenschutz gegenüber anderen Rechtsgütern habe. Befürwortern der Auffassung, dem Datenschutz komme Grundrechtsqualität zu, standen zurückhaltendere Stimmen gegenüber, die die Subsidiarität des Datenschutzes betonten.

Das Volkszahlungsurteil hat den Datenschutz zu einer elementaren Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens erklärt und den Grundrechtscharakter der informationellen Selbstbestimmung festgeschrieben. Dieses Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Damit wurde klargestellt, daß der Datenschutz unter den Bedingungen der modernen Datenverarbeitung das zentrale Mittel zur Gestaltung der Informationsbeziehungen zwischen den Einzelnen und den Institutionen in Staat und Gesellschaft ist. Das Bundesverfassungsgericht hat seine Grundposition in der Zwischenzeit in einer Reihe weiterer Urteile eindrucksvoll bestätigt.

Danach ist von dem verfassungsrechtlichen Grundsatz auszugehen, daß die Entscheidung über die Preisgabe und Verwendung personenbezogener Daten zuallererst beim Betroffenen selbst liegt. Einschränkungen der individuellen

Dispositionsfreiheit sind für die Rechts- und Gesellschaftsordnung von so wesentlicher Bedeutung, daß sie nur auf einer gesetzlichen Grundlage zulässig sind. Wie mit personenbezogenen Daten umzugehen ist, darf weder administrativer Zeckmäßigkeit noch dem Markt überlassen bleiben, sondern ist im Gesetzgebungsverfahren, d.h. vor den Augen der Öffentlichkeit zu entscheiden.

Bei der Regelung des Informationsumgangs ist von den individuellen Freiheitsrechten auszugehen; doch darf und muß der Gesetzgeber selbstverständlich berücksichtigen, daß der Einzelne in vielfältiger Weise auf den Schutz und die Hilfe des Staates angewiesen ist und daß die Tätigkeit des Staates kontrollierbar sein muß. In gesetzlich klar vorgegebenen Fällen ist daher die Verwendung personenbezogener Daten auch ohne selbstbestimmte Mitwirkung des Betroffenen erforderlich.

Das Grundrechtsverständnis mit der Selbstbestimmung des Bürgers als Regelfall und ihre Einschränkung als Ausnahme ist allerdings keineswegs von allen Seiten als Selbstverständlichkeit akzeptiert worden: Nach 10 Jahren ist eine positive, aber auch eine kritische Bilanz zu ziehen.

Nach der Entscheidung des Bundesverfassungsgerichts sind, wenn auch in vielen Fällen in langwierigen Verfahren, viele gesetzgeberische Aktivitäten entfaltet worden. Dabei mußte mancher datenschutzrechtlicher Fortschritt hart umkämpft werden.

Neben einer grundlegenden Novellierung der Datenschutzgesetze in Bund und Ländern wurden Spezialbestimmungen in zahlreichen Sondermaterien geschaffen. Auf der Ebene des Bundes zählen dazu:

— einzelne Bücher des Sozialgesetzbuches,

— das Personalaktenrecht für Beamte,

— das Straßenverkehrsrecht,

— die Gesetze über die Nachrichtendienste des Bundes,

— das Telekommunikationsrecht.

Besonderer Handlungsbedarf für die Verwirklichung der informationellen Selbstbestimmung entstand durch die deutsche Einigung. Dabei stellt die Aufarbeitung der Hinterlassenschaft des Staatssicherheitsdienstes der ehemaligen DDR auch für den Datenschutz eine besondere Herausforderung dar.

Noch weitergehend ist der Umfang der datenschutzrechtlichen Neuregelungen in den Ländern, in denen die Vorgaben des Bundesverfassungsgerichtes teilweise konsequenter umgesetzt wurden als im Bund.

Diese Verrechtlichungswelle hat auch Kritik hervorgerufen:

In Dutzenden von Gesetzen ist nunmehr das „Kleingedruckte" des Rechts auf informationelle Selbstbestimmung bereichsspezifisch geregelt. Das so entstandene Normengeflecht ist engmaschig und kompliziert. Dies steht der Intention des Verfassungsgerichtes, der Bürger solle bereits aus normenklaren Gründen erkennen können, mit welcher Verarbeitung seiner Daten er zu rechnen hat, gelegentlich bereits entgegen. Eine weitergehende Kritik stellt in Frage, ob diese Normenflut mit ihren perfektionistischen und detaillistischen Regelungen der Verwirklichung des Grundsatzes der Verhältnismäßigkeit dient und notwendig war. Geäußert wurde auch die Annahme, daß die Effizienz der staatlichen Verwaltung bei der Bewältigung ihrer Aufgaben unter der Last perfektionistischer detaillistischer Regelungen gelitten habe und daß die Kreativität der Gesellschaft und ihre Fähigkeit zur Anpassung und Bewältigung der gegenwärtigen Herausforderungen durch enge, starre Gesetze behindert würden.

Dem muß allerdings entgegen gehalten werden, daß die Fülle und Kompliziertheit der Datenverarbeitung in den verschiedensten Verwaltungsbereichen für die Regelungsdichte verantwortlich ist. Sie ist eine Konsequenz des Umstands, daß in allen Verwaltungsbereichen der – zunehmend automatisierten – Informationsverarbeitung immer mehr Bedeutung zukommt: Eine notwendige Folge der Entwicklung hin zur „Informationsgesellschaft".

Ein weiterer Grund für die Komplexität der Gesetzgebung liegt darin, daß die Gesetze häufig nicht darauf abzielen, die Rechtsposition des Bürgers zu stärken, sondern vielmehr Verarbeitung personenbezogener Daten zu ermöglichen, oft über das Maß hinaus, das bislang zulässig war. Viele Vorschriften sind so derart allgemein und umfassend zugunsten der Eingriffsseite formuliert, daß es schwerfällt, sie als „Datenschutzgesetze" im eigentlichen Sinn zu verstehen. Wann immer Verwaltungen sich durch den Datenschutz behindert glaubten, ertönte der Ruf nach dem Gesetzgeber, der – zugunsten der Verwaltung – korrigierend eingreifen soll.

Trotz alledem blieb der Datenschutz in wesentlichen Bereichen ungeregelt. Auf Bundesebene gibt es z.B. bis heute keine hinreichenden datenschutzrechtlichen Vorschriften auf den Gebieten des Arbeitnehmerdatenschutzes, der Justizmitteilungen und der Zwangsvollstreckung, des Abgabenrechts, des Mieterschutzes, der Arbeit von Auskunfteien, Detekteien und privaten Sicherheitsdiensten, der Bundespolizeibehörden, des Ausländerzentralregisters oder – am gravierensten – des gesamten Strafverfahrens.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, diese Lücken umgehend und im Sinne der informationellen Selbstbestimmung zu schließen.

Zur aktuellen Situation:

Die derzeitige Situation des Datenschutzes wird von den beiden großen Themenbereichen geprägt, die die Innenpolitik beherrschen: Die innere Sicherheit und der Zustand unserer Wirtschafts- und Sozialordnung. Diese Felder ängstigen die Menschen und stärken die Kontrollbedürfnisse des Staates. Auf beiden Gebieten wird die vermeintliche Lösung darin gesucht, daß die gesetzlichen Möglichkeiten zur Verarbeitung personenbezogener Daten erheblich ausgeweitet und auf der anderen Seite die Rechte der Bürger entsprechend eingeschränkt werden.

Auf dem Gebiet der **Strafverfolgung** haben sich bisher die Ermittlungen auf den Beschuldigten konzentriert und die prozessuale Aufklärung geschah im wesentlichen offen.

Jetzt setzt man auf Heimlichkeit und interessiert sich für Unbeteiligte. Ermittlungsverfahren ist nicht mehr Aufklärung eines konkreten Tatverdachts, sondern flächendeckende Sammlung personenbezogener Daten. Der Staat hält sich nicht mehr an die Grenzen der Ausforschung, die selbstverständlich waren, und er trifft dabei auf breite öffentliche Zustimmung.

Im Bereich der **Wirtschafts- und Sozialordnung** wird auf besonders drastische Weise versucht, durch die Einführung neuer Überwachungsverfahren eine Kostenminderung zu erreichen. Die Daten werden einerseits genutzt, durch Plafondierungen und Wirtschaftlichkeitsuntersuchungen eine Kostendämpfung zu erreichen (so etwa bei der Intensivierung der Kontrolle der Ärzte im Gesundheitsstrukturgesetz) oder eine angeblich mißbräuchliche Inanspruchnahme von Sozialleistungen aufzudecken (insbesondere durch regelmäßige Datenabgleiche bei Sozialhilfe und Arbeitsförderung).

Auf den Datenschutz wirkt sich dabei die Tendenz aus, weg von einer angeblichen egozentrischen Selbstbestimmung hin zu einer stärker betonten Gemeinschaftsverantwortung zu kommen. Individualrechte werden vielfach ohne zwingende Gründe zugunsten staatlicher Eingriffsrechte zurückgedrängt. Mehr und mehr begegnet der Staat dem einzelnen Bürger mit Mißtrauen und schafft ein immer dichteres Kontrollnetz. Es ist fraglich, ob dieses Menschenbild dem des Grundgesetzes entspricht.

Hinzu kommt, daß das reine Verwaltungsinteresse, das Bestreben nach größtmöglicher Perfektion und Einzelfallgerechtigkeit ein immer größeres Gewicht erhält. Je mehr Perfektion die Verwaltung angestrebt, desto mehr Daten muß sie erheben, nutzen, abgleichen oder sonst verarbeiten. Das Gespür für den „Mut zur Lücke" geht verloren. Kennzeichend für den demokratischen Rechtsstaat ist aber nicht seine Allwissenheit, sondern die bewußte Beschränkung seiner Informationsherrschaft.

Besonders gern wird zur Intensivierung der Kontrolle die Wunderwaffe des Datenabgleichs genutzt. Perfektion und Korrektheit lassen sich dadurch auf bequeme Weise erreichen: Auf Knopfdruck lassen sich die verschiedensten Kontrollmechanismen in Gang bringen, ohne daß sich die Behörde unmittelbar mit dem einzelnen Bürger auseinandersetzen muß. Mühelos ist die Prüfung von Zehntausenden in kürzester Frist möglich.

Wird der Weg zu intensiverer Kontrolle und Überwachung, insbesondere zum Abgleich der verschiedensten Datenbestände, ungebremst fortgesetzt, könnte sich aus einer Unsumme von automatisierten Dateien und aus einem Netz von Datenabgleichen, das schließlich alle Bürger und fast alle ihre Lebensbereiche erfaßt, der „gläserne Bürger" ergeben. Selbst wenn jeder einzelne Abgleich und Kontrollvorgang für sich eine gewisse Berechtigung haben sollte, trägt er bei zu einem umfassenden Netz von Überwachungs- und Überprüfungsmöglichkeiten. Jeder Bürger wird dabei potentiell zum Verdächtigen, dessen korrektes Verhalten es zu überprüfen gilt. Damit ändert sich das Verhältnis des Bürgers zum Staat auf grundlegende Weise.

Wie dem begegnen?

Zwar ist die verfassungsrechtliche Dimension des Datenschutzes unbestritten. Gleichwohl fehlt der informationellen Selbstbestimmung das Fundament im Grundgesetz. Eine grundlegende Verbesserung könnte erreicht werden, wenn 10 Jahre nach der Anerkennung des Grundrechts auf Datenschutz durch das Bundesverfassungsgericht dieses Grundrecht auch ausdrücklich in das Grundgesetz aufgenommen würde. Daß die erforderliche Mehrheit in Bundesrat und Bundestag hierfür bisher nicht erreicht werden konnte, bedauert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ausdrücklich.

Die verfassungsrechtliche Verbesserung bei einer derartigen Grundgesetzänderung bestünde auch darin, daß bei jedem Gesetzentwurf von Anfang an die Berücksichtigung des Grundrechts auf Datenschutz zu prüfen wäre. Eine Einschränkung des Grundrechts müßte künftig durch ausdrückliche Erwähnung im Gesetz unter Angabe des neuen Grundgesetzartikels kenntlich gemacht werden (sog. Zitiergebot nach Art. 19 GG); anderenfalls wäre das Gesetz nichtig. Dies wäre ein erheblicher „Mehrwert" zu Gunsten der Bürger.

Für die weitere Ausgestaltung des einfachen Datenschutzrechts sollten folgende Erwägungen zugrunde gelegt werden:

In der Informationsgesellschaft ist der effektive Schutz der personenbezogenen Daten die Voraussetzung für eine breite Teilnahme der Bürger an der Gesellschaft. Nur wenn der Bürger sicher sein kann, daß seine dem Staat und der Wirtschaft überlassenen Daten soweit wie möglich geschützt werden, nimmt er aktiv am Gemeinschaftsleben teil. Der Bürger kann seine Freiheit zur Kommu-

nikation (und umgekehrt ebenso seine Entscheidung zur Freiheit von Kommunikation) nur verwirklichen, wenn der Staat seine Schutzpflichten für die Daten der Bürger ernst nimmt.

Die wichtigste Folge dieser Einsicht ist, daß Datenschutzvorschriften nicht nur Rechtssicherheit, sondern auch **materielle Freiheitsräume** garantieren müssen. Dies bedeutet, daß bei der Frage, ob der Einzelne einer Auskunftspflicht unterworfen werden soll, ob seine Daten außer für den Erhebungszweck auch für andere Zwecke freigegeben werden sollen, wie lange belastende Daten aufbewahrt werden dürfen und welche Datenverarbeitungsvorgänge dem Betroffenen verborgen bleiben dürfen, jeweils strenge Maßstäbe angelegt werden müssen. Hierfür ist eine neue Grenzziehung für Eingriffe in das Recht auf informationelle Selbstbestimmung erforderlich: Der Begriff des „überwiegenden Allgemeininteresses", der alleine einen Eingriff in die informationelle Selbstbestimmung rechtfertigt, ist inhaltlich mehr aufzufüllen und mehr als bisher im Lichte der informationellen Selbstbestimmung zu interpretieren. In konkreten Konfliktfällen darf die Freiheitssicherung der Bürger gegenüber effektiver Staatstätigkeit nicht ins Hintertreffen geraten.

Für das Bundesverfassungsgericht ist die Beteiligung **unabhängiger Datenschutzbeauftragter** wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten im Interesse eines vorgezogenen Rechtsschutzes von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung. Dies gilt insbesondere in den Bereichen, in denen ein Auskunfts- oder Einsichtsanspruch des Bürgers nicht oder nur unvollständig besteht. Daraus folgt, daß Rolle und Kompetenzen der Datenschutzbeauftragten auch im Hinblick auf effektivere Eingriffsmöglichkeiten gestärkt werden müssen. Versuche, die Kontrollmöglichkeiten der Datenschutzbeauftragten zu beschränken, muß schärfstens widersprochen werden.

Datenschutzrechtliche Verstöße gehen meist auf Unkenntnis und mangelndes Problembewußtsein seitens der öffentlichen Stellen zurück. **Aus- und Fortbildung** in Fragen des Datenschutzes muß daher erheblich mehr Gewicht beigemessen werden als bisher. Insbesondere sind Bemühungen zu fördern, den Datenschutz in den einschlägigen Ausbildungsplänen (Informatikunterricht in der Schule, Rechts- und Informatikstudium an den Hochschulen) sowie den Fortbildungsveranstaltungen in der öffentlichen Verwaltung als obligatorisches Fach zu verankern.

Die **Datenverarbeitungstechniken** haben sich gegenüber der Zeit des Volkszählungsurteils geradezu revolutionär verändert. Der Umsetzung des Volkszählungsurteils durch die Schaffung der eigenen Rechtsgrundlagen muß daher verstärkt die Entwicklung geeigneter technisch organisatorischer Maßnahmen zur Seite gestellt werden. Der Blick des Datenschutzes muß sich stärker auf die Technik des Verarbeitunsprozesses selbst richten. Dies bedeutet

nicht nur die Entwicklung spezifischer Datenschutzvorkehrungen für neue informationstechnische Entwicklungen (Miniaturisierung der Rechner, Chipkarten, neue Vernetzungstechniken), sondern auch neuer komplexer Anwendungsformen (z.B. im Bereich des Zahlungsverkehrs, der Straßenbenutzung oder der Textverarbeitung).

Die **Europäische Union** wird zunehmend zur Informations- und Datengemeinschaft. Dies macht einen europäischen Datenschutz erforderlich. Die Konferenz teilt mit den europäischen Nachbarn nicht nur die Überzeugung, daß der Datenschutz in Europa harmonisiert werden muß, sondern auch daß die Rechte der Gemeinschaftsbürger auf einem hohen Niveau gesichert werden müssen, damit die Öffnung der Grenzen für Güter, Kapital und Dienstleistungen – und damit auch für persönliche Daten – nicht zu Nachteilen für den einzelnen führt.

Innerhalb von Deutschland wirft die **Integration der neuen und der alten Bundesländer** nach wie vor Probleme auf. Nach wie vor besteht die Neigung, über Bürger aus den neuen Bundesländern erheblich mehr Daten zu erheben und unter erleichterten Bedingungen Daten zu verarbeiten, als dies in den alten Ländern der Fall wäre.

Die Notwendigkeit für Übergangsregelungen in den neuen Bundesländern wird nicht bestritten; die Eingriffe in Persönlichkeitsrechte müssen aber dennoch verhältnismäßig, erforderlich und darüber hinaus zeitbefristet sein. Aus dem Einigungsprozeß herrührende Sonderregelungen und Verwaltungsvorschriften sind nicht festzuschreiben, sondern auch im Sinne der informationellen Selbstbestimmung schrittweise abzubauen.

Geschäftsverteilung (Stand: 15. Dezember 1994)

Der Hamburgische Datenschutzbeauftragte
Baumwall 7, 20459 Hamburg

Tel.: 040/3504-2044
BN: 9.41-2044
Fax: 040/3504-2372

			Durchwahl
Dienststellenleiter:	Dr. Hans-Hermann Schrader	D	-2044-
Stellvertreter:	Peter Schaar		-2231-
Vorzimmer:	Eva-Maria Reupke		-2045-

D 1 – Geschäftsstelle

			Durchwahl
Leiter:	Gunnar Hansen	D 1	-2223-
Sachbearbeiterin:	Annelies Franke	D 10	-2063-
Mitarbeiterinnen:	Eva-Maria Reupke	D 11	-2045-
	Irene Heinsohn	D 12	-2047-

D 1: Allgemeine Verwaltungsangelegenheiten
Tätigkeitsberichte
Konferenz der Datenschutzbeauftragten
Öffentlichkeitsarbeit
Geheimschutzangelegenheiten

D 10: Systemverwaltung
Bibliothek
Register nach § 24 HmbDSG
Bearbeitung von Eingaben
Verwaltung von Senats-/Bürgerschaftsdrucksachen

D 11: Vorzimmerdienst
Textverarbeitung
Eingabenverwaltung

D 12: PC-Textverarbeitung
Registratur
Postverteilung

D 2/1 – Referat

			Durchwahl
Leiter:	NN	D 2/1	-2046-
Sachbearbeiter:	Gunnar Hansen	D 21	-2223-

D 2/1: Grundsatzfragen des Datenschutzes
Datenschutzgesetze
Parlamentsangelegenheiten
Justiz
Strafvollzug
Verfassungsschutz
Meldewesen
Ausländerwesen
Ausbildungsleiter für die Juristenausbildung

D 21: Personenstandswesen

D 2/2 – Referat

			Durchwahl
Leiter:	Ulrich Werner	D 2/2	-2581-
Sachbearbeiter:	Gunnar Hansen	D 21	-2223-

D 2/2: Polizei und Feuerwehr
Staatsanwaltschaft
Straßenverkehrsverwaltung
Verkehrsordnungswidrigkeiten

D 21: Bau-, Vermessungs- und Wohnungswesen
Stadtentwicklung

D 3 – Referat

			Durchwahl
Leiter:	Peter Schaar	D 3	-2231-
Referent:	Dr. Uwe Schläger	D 30	-2564-
Referent:	Ulrich Kühn	D 31	-2564-
Sachbearbeiter:	Dietmar Nadler	D 32	-2236-

D 3: Grundsatzfragen der IuK-Technik und -Organisation
Telekommunikation
Online-Datenbanken
technisch-organisatorische Beratungs- und Prüftätigkeit für die Bereiche
- Justiz (außer Staatsanwaltschaft)
- Strafvollzug
- Verfassungsschutz
- Meldewesen
- Personalwesen
- Personenstandswesen
- Wissenschaft und Forschung
- Kultur
- nicht-öffentlicher Bereich für die jeweiligen IuK-Techniken

Datenschutzrechtliche Betreuung der Bereiche
- Statistik
- Wahlen
- Medien
- Natur- und Umweltschutz

D 30: LAN
MS-DOS
Host-PC-Kopplung
ec-cash
Richtlinien zur Datensicherung und Datenverarbeitung (mit D 31)
technisch-organisatorische Beratungs- und Prüftätigkeit für die Bereiche
- Soziales
- Gesundheitswesen
- Archivwesen
- nicht-öffentlicher Bereich für die jeweiligen IuK-Techniken

D 31: Verschlüsselungstechniken
UNIX
Richtlinien zur Datensicherung und Datenverarbeitung (mit D 30)
technisch-organisatorische Beratungs- und Prüftätigkeit für die Bereiche
- Schule und Berufsbildung
- Bezirksangelegenheiten
- Wirtschaftsverwaltung
- nicht-öffentlicher Bereich für die jeweiligen IuK-Techniken

D 32: Großrechnerbetriebssysteme
Speichertechniken
IuK-Gesamtplanung
technisch-organisatorische Beratungs- und Prüftätigkeit für die Bereiche
- Parlamentsangelegenheiten
- Polizei und Feuerwehr
- Staatsanwaltschaft
- Ausländerwesen
- Verkehrsordnungswidrigkeiten
- Straßenverkehrsverwaltung
- Bauwesen/Stadtentwicklung
- nicht-öffentlicher Bereich für die jeweiligen IuK-Techniken

datenschutzrechtliche Betreuung der Bereiche
- Finanz-, Steuer- und Rechnungswesen
- allgemeine Senatsangelegenheiten
- zentrales Organisationswesen
- zentrale Informationstechnik (LIT)

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: Soziales
Arbeitsschutz

D 5 – Referat			Durchwahl
Leiterin:	Verena Scheffler-Ritters	D 5	–2562–
Sachbearbeiter:	Achim Kruppke	D 51	–2563–

D 5: Personaldatenschutz, Gleichstellung
Archivwesen
Wirtschaft und Landwirtschaft

D 51: Schule und Berufsbildung
Wissenschaft und Forschung

D 6 – Referat			Durchwahl
Leiterinnen:	Helga Naujok	D 6-1	–2556–
	Elisabeth Duhr	D 6-2	–2541–
Referent:	Detlef Malessa	D 60	–2089–
Sachbearbeiterin:	Evelyn Seiffert	D 61	–2468–

Aufsichtsbehörde nach 38 Bundesdatenschutzgesetz

D 6-1: Versicherungswirtschaft einschließlich Vorsitz in der Arbeitsgruppe
Versicherungswirtschaft der Aufsichtsbehörden
Allfinanz-Gruppen
Handel, Industrie
Düsseldorfer Kreis der Aufsichtsbehörden

D 6-2: Auskunfteien, Wirtschafts- und Handelsauskunfteien
SCHUFA
Kreditwirtschaft
Internationaler Datenverkehr im öffentlichen und nicht-öffentlichen Bereich, insbesondere Datenschutzrecht der Europäischen Union

D 60 : Versandhandel
Werbung und Adreßhandel
Bauen und Wohnen, insbesondere Mietangelegenheiten
Transport und Verkehr einschließlich HVV
Freie Berufe und gewerbliche Dienstleistungen
Videoüberwachung in der Wirtschaft
Sonstige Rechtsfragen zum Datenschutz in der Wirtschaft
Kirchen

D 61 : Auftragsdatenverarbeitung
Markt- und Meinungsforschung
Datenbankbetreiber und Netzanbieter (mit D 3)
Bildschirmtext und Mailboxen (mit D 3)
Allgemeine Beratung von betrieblichen Datenschutzbeauftragten
Grundsätzliche Fragen zum Register nach 32 BDSG
Mikroverfilmung
Akten- und Datenträgervernichtung

Stichwortverzeichnis

Abkürzungen

ADV	Automatisierte Datenverarbeitung
AFIS	Automatisiertes Fingerabdruck-Identifizierungssystem
AG-Kripo	Arbeitsgruppe Kriminalpolizei der Innenministerkonferenz
AK	Allgemeines Krankenhaus
AO	Abgabenordnung
APIS	Arbeitsdatei PIOS „Innere Sicherheit“
APOK	Arbeitsdatei PIOS „Organisierte Kriminalität“
ARD	Arbeitsgemeinschaft der Rundfunkanstalten Deutschlands
Art.	Artikel
AsylVfG	Asylverfahrensgesetz
AuslG	Ausländergesetz
AZR	Ausländerzentralregister
AZRG	Gesetz über das Ausländerzentralregister
BACom	Projekt „Bauaufsicht mit Computerunterstützung“
BAGS	Behörde für Arbeit, Gesundheit und Soziales
BAV	Bundesaufsichtsamt für das Versicherungswesen
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
Bfl	Behörde für Inneres
BGS	Bundesgrenzschutz
BIOS	Basic Input Output System
BIS	Bodeninformationssystem
BKA	Bundeskriminalamt
BKK	Betriebskrankenkasse
BMI	Bundesministerium des Innern
BRat	Bundesrat
BSJB	Behörde für Schule, Jugend und Berufsbildung
Btm	Betäubungsmittel
Btx	Bildschirmtext, vgl. Datex-J
BVerfGE	Bundesverfassungsgerichtsentscheidungen
BVerfSchG	Bundesverfassungsschutzgesetz
BVSt	Besoldungs- und Versorgungsstelle
BZRG	Bundeszentralregistergesetz
CCITT	Internationale Organisation der Telekommunikationsorganisationen
CD-ROM	Compact Disc – Read Only Memory
CompuServe	US-amerikanischer Telekommunikations- und Informationsdienst
COMVOR	Projekt „Computerunterstützte Vorgangsbearbeitung“ bei der Polizei
Datex	Kunstwort für Data Exchange
Datex-J	Datex-„Jedermann“ – neue Bezeichnung für den Bildschirmtextdienst der Telekom

Datex-P	paketorientierter Datenübertragungsdienst der Telekom
DB	Deutsche Bundesbahn
DBP	Deutsche Bundespost
DES	Data Encryption Standard
DNA	Desoxyribonucleinsäure
DS-Hinweise	Hinweise zur Durchführung des HmbDSG und zu den datenschutzrechtlichen Regelungen des SGB/BDSG
DS-Richtlinie	Richtlinie zum Verfahren der Datensicherung im IuK-Bereich
DV	Datenverarbeitung
ec-cash	Electronic-cash
EC-Karte	Euroscheck-Karte
ed-Behandlung	erkennungsdienstliche Behandlung
EDV	Elektronische Datenverarbeitung
EDU	European Drug Unit – Europäische Drogenzentralstelle
EG	Europäische Gemeinschaften
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
EIS	Europäisches Informationssystem der Polizei
EM	Electronic Mail – elektronische Post
EU	Europäische Union
Europol	Europäisches Polizeiamt
FAG	Fernmeldeanlagengesetz
FIS	Flächenbezognes Informationssystem
FHH	Freie und Hansestadt Hamburg
GBG	Geschlossene Benutzergruppe
GVG	Gerichtsverfassungsgesetz
GG	Grundgesetz
GwG	Geldwäschegesetz
G 10	Gesetz zu Artikel 10 Grundgesetz
HmbMedienG	Hamburgisches Mediengesetz
HmbVerfG	Hamburgisches Verfassungsgericht
HALB	Hamburgisches Automatisiertes Liegenschaftsbuch
HGV	Hamburger Gesellschaft für Beteiligungsverwaltung
HmbBG	Hamburgisches Beamtengesetz
HmbDSG	Hamburgisches Datenschutzgesetz
HmbMG	Hamburgisches Meldegesetz
HmbMedienG	Hamburgisches Mediengesetz
HmbMeldeDÜV	Hamburgische Verordnung über regelmäßige Datenübermittlungen aus dem Melderegister
HmbPersVG	Hamburgisches Personalvertretungsgesetz
HmbPolDVG	Hamburgisches Gesetz über die Datenverarbeitung der Polizei
HmbStatG	Hamburgisches Statistikgesetz
HmbVermG	Hamburgisches Vermessungsgesetz
HVV	Hamburger Verkehrsverbund
ID	Individuelle Kennung eines Gerätes (z.B. Computers) oder eines Benutzers

INPOL	Informationssystem der Polizei (bundesweit)
ISDN	Integrated Services Digital Network Integriertes digitales Kommunikationssystem
ISO	Internationale Standardisierungs-Organisation
IuK	Informations- und Kommunikationstechnik
JVA	Justizvollzugsanstalt
KAN	Kriminalaktennachweis in –> INPOL
KORA	Koordinationsstelle zur Bekämpfung der offenen Rauschgiftszene in St. Georg
KpS	kriminalpolizeiliche Sammlung
KunstUrhG	Kunsturhebergesetz
LAN	Local Area Network – lokales Netzwerk
LBK	Landesbetrieb Krankenhäuser
LIT	Landesamt für Informationstechnik
LKA	Landeskriminalamt
LVA	Landesversicherungsanstalt
MDK	Medizinischer Dienst der Krankenversicherungen
MEWES	Projekt „Meldewesen“
MiStra	Anordnung über Mitteilungen in Strafsachen
MittVw	Mitteilungen für die Verwaltung
MOD	Modifiable Optical Disc
MRRG	Melderechtsrahmengesetz
NADIS	Nachrichtendienstliches Informationssystem
NDR	Norddeutscher Rundfunk
NFS	Network File System
NJW	Neue Juristische Wochenschrift
OK	organisierte Kriminalität
OLG	Oberlandesgericht
OrgKG	Gesetz zur Bekämpfung der organisierten Kriminalität
OPAL	Ordnungswidrigkeiten-Projekt – Abteilungsrechner-Lösung
OwiG	Ordnungswidrigkeitengesetz
PASTA	Projekt Automation Standesämter
PAULA	Projekt „Automation des Ausländer- und Asylwesens“
Pay per View	Form von –> Pay TV, bei der jede empfangene Sendung bezahlt wird
Pay TV	entgeltpflichtiges Fernsehen
PÄD	Personalärztlicher Dienst
PC	Personalcomputer
PHW	personenbezogener Hinweis in polizeilichen Dateien
PIOS	Personen, Institutionen, Objekte, Sachen – Dateityp in –> INPOL
POLAS	Polizeiliches Auskunftssystem (Hamburg)
PolDVG	Gesetz über die Datenverarbeitung der Polizei
PPS	Personalplanungssystem der Polizei
PROPERS	Projekt Personalwesen
PROSA	Projekt Sozialhilfe-Automation

ProStep	Projekt Automation der Stellenplanung
PStG	Personenstandsgesetz
PUA	Parlamentarischer Untersuchungsausschuß
PULS	Projekt „Pflegedienstunterstützung für die LBK-Stationen“
PVC	Permanent Virtual Circuit – virtuelle Festverbindung bei X.25-Netzen
Quasic	Projekt „Qualitätssicherung in der Chirurgie“
RAK	Referatsarbeitskartei des Landesamtes für Verfassungsschutz
RSA	nach den Entwicklern Rivest, Shamir und Adleman benanntes Verschlüsselungsverfahren
SDÜ	Schengener Durchführungsübereinkommen
SED	Sozialistische Einheitspartei Deutschlands
SfB	Senatsamt für Bezirksangelegenheiten
SfV	Senatsamt für den Verwaltungsdienst
SGB-I	Sozialgesetzbuch / Erstes Buch
SGB-IV	Sozialgesetzbuch / Viertes Buch
SGB-V	Sozialgesetzbuch / Fünftes Buch
SGB-VI	Sozialgesetzbuch / Sechstes Buch
SGB-VIII	Sozialgesetzbuch / Achtes Buch
SGB-X	Sozialgesetzbuch / Zehntes Buch
SINIX	Herstellerspezifische Variante des Betriebssystems –> UNIX
SIS	Schengener Informationssystem
SOG	Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung
SQL	Structured Query Language
StA	Staatsanwaltschaft
StDAV	Steuerdatenabrufverordnung
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrszulassungsordnung
TB	Tätigkeitsbericht
TK-Anlage	Telekommunikationsanlage
TK-RL	Telekommunikationsrichtlinie
UDSV	Teledienstunternehmen-Datenschutzverordnung
UIG	Umweltinformationsgesetz
UIR	EG-Umweltinformationsrichtlinie
UNIX	Betriebssystem für Mehrplatz-Computersysteme
VAG	Versicherungsaufsichtsgesetz
VVG	Versicherungsvertragsgesetz
WAN	Wide Area Network – behördenübergreifendes Netzwerk
WoBindG	Wohnungsbindungsgesetz
WORM	Write Once Read Multiple
WEG	Wohnungseigentumsgesetz
WRK	Wohnraumkartei

X.25	technischer Standard zur paketorientierten Datenübertragung
X.400	Standard für elektronische Post
ZDF	Zweites Deutsches Fernsehen
ZKA	Zentraler Kreditausschuß

Veröffentlichungen zum Datenschutz

Beim Hamburgischen Datenschutzbeauftragten sind derzeit folgende Veröffentlichungen kostenlos erhältlich:

Broschüren

Datenschutzkonzept für UNIX-Mehrplatzanlagen

Datenschutz in Netzen

Datenschutz in der Arztpraxis

Mobilfunk und Datenschutz

Berichte und Dokumente

Bericht über den Datenschutz bei Automation und Vernetzung der hamburgischen Verwaltung – IuK-Datenschutzbericht –

Grundrecht auf Datenschutz im Grundgesetz (Symposium mit Mitgliedern der Gemeinsamen Verfassungskommisssion)

Informationsblätter

Tips zum Adressenhandel

Datenschutz im privaten Bereich