16. Tätigkeitsbericht
des Hamburgischen Datenschutzbeauftragten
Berichtsjahr 1997

zugleich Tätigkeitsbericht der Aufsichtsbehörde für den nicht-öffentlichen Bereich
vorgelegt im Februar 1998
(Redaktionsschluß: 1. Dezember 1997)
Dr. Hans-Hermann Schrader

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Baumwall 7 · 20459 Hamburg · Tel.: 35 04 20 47
Auflage: 2.500 Exemplare
Druck: Lütcke & Wulff, 20097 Hamburg

INHALTSVERZEICHNIS

Zusammenfassung wichtiger Punkte

Selbstdatenschutz Durch verschiedene Wahlmöglichkeiten soll ein selbstbestimmter Umgang der Bürger mit ihren persönlichen Daten in Verwaltung und Wirtschaft gefördert werden. Zugleich ist durch datenschutzfreundliche Grundregelungen dafür zu sorgen, daß der Datenschutz auch ohne eigene Auswahlentscheidungen gewahrt bleibt (1.1).

SAP in den Krankenhäusern Die bereits früher generell festgestellten Datenschutzprobleme bei SAP wurden durch eine Prüfung des Allgemeinen Krankenhauses Eilbek bestätigt. Die Prüfung des SAP-Systems IS-H hat hauptsächlich Defizite im Administrationskonzept, beim Freigabeverfahren sowie bei der Vergabe der Zugriffsrechte ergeben (3.3).

Multimedia Mit den 1997 in Kraft getretenen Bestimmungen auf Bundes- und Landesebene zum Multimediarecht wurde auch der in diesem Bereich zu gewährleistende Datenschutz festgelegt. Noch mangelt es jedoch häufig an der Umsetzung der gesetzlichen Vorgaben (3.5 und 3.6). Allerdings zeichnen sich Standards ab, mit denen die informationellen Selbstbestimmungsmöglichkeiten der Internet-Nutzer verbessert werden können (3.7).

Gesetz über Untersuchungsausschüsse Das Gesetz über die Untersuchungsausschüsse der Hamburgischen Bürgerschaft vom 27. August 1997 regelt einen wichtigen Bereich des parlamentsspezifischen Datenschutzes. Die Belange des Parlaments und die Interessen der Betroffenen werden angemessen berücksichtigt (4.1).

Rentendaten unzulänglich geschützt Die Rentenversicherungsträger machen sich bundesweit Sozialdaten der Rentenversicherten gegenseitig zugänglich. Die generelle Einrichtung des Verfahrens ohne Rücksicht auf den Willen des Versicherten erscheint rechtwidrig (6.1).

Melderegisterauskünfte an Parteien für Zwecke der Wahlwerbung Die gegenwärtige gesetzliche Regelung trägt der informationellen Selbstbestimmung nicht hinreichend Rechnung. Zahlreiche Eingaben und Beschwerden unterstreichen, daß insbesondere die Information über das Widerspruchsrecht deutlich verbessert werden muß (11.2).

Polizeiliche DNA-Datenbank Wenn eine polizeiliche DNA-Analysedatei eingerichtet wird, dürfen keine Untersuchungsergebnisse erfaßt werden, die Aussagen über Erbanlagen ermöglichen. Speicherungen dürfen nur aufgrund richterlicher Anordnung über Personen erfolgen, bei denen mit weiteren relevanten Straftaten zu rechnen ist. Die Erfassung von Ergebnissen aus Reihenuntersuchungen ist auszuschließen (15.3).

Kontrolle von Schwarzfahrern Die Beteiligung der Polizei an Fahrausweiskontrollen im öffentlichen Personennahverkehr muß sich auf Fälle beschränken, in denen die Feststellung der Personalien im Einzelfall erforderlich ist. Die Polizei darf dagegen aus diesem Anlaß keine unterschiedslosen Personenkontrollen in Form einer Razzia vornehmen (15.5).

Neue Überwachungstechnik Der Einsatz von sog. "IMSI-Catchern" zur Überwachung von Mobiltelefonen ist abzulehnen, da er zu unvertretbaren Eingriffen in das Fernmeldegeheimnis Unbeteiligter und zu massiven Beeinträchtigungen der Netzsicherheit führt (16.2.2).

Bild-Ton-Aufzeichnungen von Vernehmungen im Strafverfahren Der Einsatz von Videotechnologie kann psychische Belastungen für Opferzeugen erheblich verringern. Dabei müssen allerdings wirksame Vorkehrungen zum Schutz des Persönlichkeitsrechts getroffen werden (17.1).

Auslagerung von Krankenhausaufgaben Das sog. Outsourcing auf private Unternehmen bedarf strenger Sicherungsmaßnahmen, um die ärztliche Schweigepflicht nicht zu verletzen. Ein Einblick externer Dritter in Patientendaten ist grundsätzlich zu vermeiden (18.1).

Arztpraxis-EDV Der EDV-Einsatz in Arztpraxen entspricht häufig nicht den Datenschutz- und Datensicherungsbestimmungen. Defizite liegen sowohl in der Systemsicherheit der Software selbst als auch im Umgang mit der EDV in den Arztpraxen (18.2).

Warndatei Zunehmend wollen Unternehmen Warndateien einrichten, z. B. mit Daten über das Zahlungsverhalten von Mobilfunkkunden oder mit Inkassodaten. Zulässig ist dies nur, wenn objektiv erforderliche Kriterien für die zu speichernden Merkmale festgelegt werden, die Betroffenen umfassend über das Verfahren informiert werden und ohne jeden Zwang eine Einwilligungserklärung abgegeben haben (25.).

Haushaltsumfragen Eine neue Form von Adressenhandel sind die vermehrt durchgeführten Haushaltsumfragen. Die Beantwortung ist freiwillig und bedarf der Einwilligung; auch noch nachträglich kann man der Nutzung für Marketing- und Werbezwecke widersprechen (26.).

Vorwort

Nachdem mich die Bürgerschaft am 12. Februar 1997 mit Dreiviertelmehrheit erneut zum Hamburgischen Datenschutzbeauftragten gewählt hatte, hat mich der Senat am 6. März 1997 für eine weitere Amtszeit von 6 Jahren bestellt. Im Sinne der amtlichen Begründung zum Hamburgischen Datenschutzgesetz wird es mir damit ermöglicht, "den Sachverstand und die Erfahrungen für eine zweite Amtszeit zu nutzen". Grundlage ist dafür insbesondere die Kompetenz der Mitarbeiterinnen und Mitarbeiter, denen ich für ihre engagierte Unterstützung danke.

Damit der Datenschutz effektiv umgesetzt werden kann, werden wir verstärkt von der Information zur Kommunikation mit dem Bürger, der Verwaltung und der Wirtschaft übergehen. Ihnen soll nicht nur unsere Auffassung von Beratung und Kontrolle vermittelt werden, sondern sie sollen auch Gelegenheit zur Äußerung ihrer Erwartungen an den Datenschutz erhalten.

Notwendig ist außerdem eine intensive Zusammenarbeit mit behördlichen und betrieblichen Datenschutzbeauftragten und ein verstärktes Zusammenwirken der Datenschutzbeauftragten von Bund und Ländern und der Aufsichtsbehörden. Bei der umfassenden Weiterentwicklung der Datenverarbeitung ist ein wirksam organisiertes Datenschutznetz der für diesen Bereich Verantwortlichen geboten - mit möglichst großer Unabhängigkeit im Interesse der Bürger.

Auch das Instrumentarium für den Datenschutz ändert sich. Bei einer globalen Datenverarbeitung können Rechtsvorschriften allein nicht mehr den Schutz der Selbstbestimmung gewährleisten. Der rechtliche Datenschutz durch staatliche Regulierung könnte und sollte sich ohnehin auf das Wesentliche konzentrieren und unnötige, für den Bürger nicht nachvollziehbare Detaillierungen vermeiden. Zugleich sollten die Möglichkeiten zur Selbstregulierung unterhalb von Rechtsvorschriften durch Verwaltung und Wirtschaft mehr genutzt werden.

Ergänzend wird der technische Datenschutz mit staatlichen Vorgaben für eine bürgerorientierte Techniknutzung immer größere Bedeutung bekommen. Dazu ist der Aufbau von Datenschutz-Auditverfahren anzustreben, mit denen datenschutzfreundliche Soft- und Hardware gutachterlich anerkannt werden kann.

In der Informationsgesellschaft werden wir den neuen Herausforderungen an den Datenschutz mit diesem erweiterten Spektrum von Handlungsansätzen begegnen. Unsere Aufgabe bleibt dabei unverändert: Das Recht des Einzelnen zu schützen, grundsätzlich selbst über die Verwendung seiner persönlichen Daten zu bestimmen.

Bisher stand im Mittelpunkt unserer Arbeit, die Fremdbestimmung des Einzelnen weitgehend zu begrenzen und dabei den vorbeugenden Datenschutz zu verstärken. Dies wurde durch die Novellierung des Hamburgischen Datenschutzgesetzes vom 18. März 1997 zu Beginn meiner neuen Amtszeit zukunftsweisend abgesichert. Erstmals wurde der Grundsatz zur Datenvermeidung ausdrücklich in ein Datenschutzgesetz aufgenommen; zugleich wurde der vorbeugende Datenschutz u. a. durch die gesetzliche Pflicht zur Risikoanalyse rechtsverbindlich festgelegt.

Die Begrenzung der Fremdbestimmung durch Verwaltung und Wirtschaft wird auch weiterhin eine Hauptaufgabe für uns sein. Die Selbstbestimmung des Einzelnen als das Ziel des Datenschutzes möchte ich in der neuen Amtszeit außerdem dadurch fördern, daß der Bürger mehr als bisher zum Selbstdatenschutz befähigt wird.

Es trägt zur Verwirklichung des Grundrechts auf informationelle Selbstbestimmung bei, wenn das Selbstbewußtsein und die Selbstverantwortung der Bürger soweit wie möglich gestärkt werden. Die

technische Entwicklung führt zu immer mehr Anwendungsmöglichkeiten für einen individuellen Umgang mit den eigenen persönlichen Daten. Es wird für uns eine zunehmend wichtige Aufgabe, durch Hilfe zur Selbsthilfe den Bürger dabei zu unterstützen, die Chancen für seine Selbstbestimmung wahrnehmen zu können und den Risiken entgegen zu wirken.

Die Selbstbestimmung der Bürger ist zugleich eine Grundbedingung für ein freiheitliches demokratisches Gemeinwesen, wie es bereits im Volkszählungsurteil des Bundesverfassungsgerichts heißt. Selbstbestimmung des Einzelnen und Freiheit der Gemeinschaft gehören daher untrennbar zusammen.

Der Aufbruch der Freiheitsideen veranlaßte Kant vor 200 Jahren zu seiner berühmten Umschreibung der Aufklärung. Entsprechend seinen Worten läßt sich heute sagen: "Selbstbestimmung ist der Ausgang des Menschen aus seiner Unmündigkeit. Unmündigkeit ist das Unvermögen, über sich selbst ohne Bestimmung durch andere zu entscheiden. Ursache dieses Unvermögens ist der Mangel an Wissen über die Chancen und Risiken eigener Entscheidungen und der Mangel an Mut zur Selbstbestimmung. Erst wägen, dann wagen ist daher der Wahlspruch der Selbstbestimmung."

1. Zur Lage des Datenschutzes

1.1 Schwerpunkt Selbstdatenschutz mit Wahlmöglichkeiten

Wie in der Einleitung zum 15. Tätigkeitsbericht (TB) dargestellt wurde, hat die persönliche Autonomie für den Bürger einen hohen Rang in der Wertehierarchie.

Die Bürger erwarten, daß ihre Persönlichkeit stärker von Verwaltung und Wirtschaft respektiert wird. Sie verlangen mehr Achtung vor ihrer Selbstbestimmung und damit zugleich weniger Fremdbestimmung. Der Selbstbestimmung im Sinne des Leitsatzes 1 des Volkszählungsurteils würde es daher entsprechen, wenn die Bürger vermehrt Auswahlmöglichkeiten für den Umgang mit ihren Daten haben oder künftig erhalten. Demgegenüber hat sich der Datenschutz bisher ganz überwiegend im Sinne des Leitsatzes 2 des Urteils darauf konzentriert, die Fremdbestimmung für den Bürger möglichst gering zu halten.

Auch zur Kundenorientierung nicht nur in der Wirtschaft, sondern ebenso in der Verwaltung gehört es, den vielfach unterschiedlichen Datenschutzbelangen der Bürger Rechnung zu tragen. Statt eines Pluralismus mit vielfältigen Handlungsmöglichkeiten gibt es aber bisher im Datenschutzrecht meistens nur eine Einheitsregelung für alle Bürger. Dem großen Vertrauen vieler Bürger in den Datenschutz und ihren hohen Erwartungen würde es jedoch entsprechen, möglichst viele Entscheidungsvarianten zu entwickeln und dadurch frühzeitig verständliche Kritik über einen unflexiblen Datenschutz bis hin zur Datenschutzverdrossenheit zu vermeiden.

1.1.1 Regulierung und Selbstregulierung

Der Gesetzgeber und auch der Verordnungsgeber sollten daher künftig stärker auf die Selbstbestimmung des Einzelnen eingehen und eine oder mehrere Alternativen zur Auswahl vorsehen. Im Rahmen der geltenden Vorschriften hat inzwischen auch die Rechtsprechung Ansätze für Wahlmöglichkeiten des Bürgers eröffnet. Bei der Auslegung und Anwendung des geltenden Rechts gibt es außerdem vielfach für Verwaltung und Wirtschaft eine Bandbreite von Möglichkeiten, die z. B. gemäß Art. 27 der europäischen Datenschutzrichtlinie als Verhaltensregeln ("Codes of Conduct") gemeinsam von Verwaltung und Wirtschaft festgelegt werden können; damit würden außerdem zusätzliche Rechtsvorschriften vermieden.

Die technische Entwicklung bei den Informationsdiensten geht bereits in die Richtung einer zunehmenden Individualisierung und zugleich Globalisierung: Onlinedienste und Internetangebote werden individualisiert und sind weltweit vernetzt. Bei der Nutzung dieser Dienste hat der Bürger die - inzwischen auch rechtlich abgesicherte (3.5) - Möglichkeit, in gewissem Umfang Selbstdatenschutz durch Technik zu verwirklichen; der neue Begriff "Selbstdatenschutz" wurde bei dem neuen Multimediarecht ausdrücklich verwendet. Dazu gehören anonyme und pseudonyme Datenverarbeitungen und vor allem eine wirkungsvolle Verschlüsselung (siehe zum Schwerpunkt Datenvermeidung durch Technik 15. TB, 1.3 und 3.1).

Da den Anbietern das Datenschutzbedürfnis der Bürger durchaus bekannt ist, entwickeln sie inzwischen selbst neue Standards, die zwar eine ungewollte Preisgabe von Persönlichkeitsprofilen verhindern können, jedoch andererseits die wirtschaftliche Verwertung von Benutzerprofilen - auch über Unternehmensgrenzen hinaus und unter Durchbrechung des Zweckbindungsgebotes - erleichtern (z. B. die Platform for Privacy Preferences - P3 - und der Open Profiling Standard - OPS -, siehe 3.7). Damit die Belange der Bürger wirksam geschützt werden, bedarf es auch hier rechtlich verbindlicher Vorgaben.

1.1.2 Grundregelung und Widerruf

Andererseits muß die Interessenlage der Bürger berücksichtigt werden, die sich nicht jeweils gesondert entscheiden wollen, sondern unabhängig von eigenen Entscheidungen eine Absicherung gegen Datenschutzrisiken erwarten. Ein erheblicher Teil der Bürger hat außerdem Schwierigkeiten im Umgang mit modernen Techniken oder ist aus sonstigen Gründen zu einer sachgerechten Auswahlentscheidung nicht in der Lage. Zu einem bürgerorientieren Grundrechtsverständnis gehört es deshalb, nicht nur Möglichkeiten für ein freiheitliches Verhalten vorzusehen, sondern zugleich für Schutzvorkehrungen im Sinne einer sozialen Informationsordnung zu sorgen.

Dieser Zielrichtung würde es entsprechen, wenn jeweils eine datenschutzfreundliche Grundregelung ohne Entscheidungsbedarf festgelegt wird und im übrigen Wahlmöglichkeiten offengehalten werden. Beispiele gibt es dafür schon jetzt im Telekommunikationsbereich mit einer Grundregel und mehreren Wahlmöglichkeiten z. B. für Telefonbucheintragungen oder Telefonabrechnungen. Der Telefonkunde hat zudem die Möglichkeit, kostenfrei zu entscheiden, ob seine Rufnummer auf dem Apparat seines Gesprächspartners angezeigt wird oder nicht.

Wichtig ist, daß die Entscheidungen später einer veränderten Interessenlage angepaßt werden können. Dazu kann die seinerzeit gewählte Möglichkeit - z. B. für Telefonbucheintragungen oder Telefonrechnungen - mit Wirkung für die Zukunft widerrufen werden; nach Bedarf kann ein Änderungsantrag gestellt werden.

Mit diesen Beispielen wird deutlich, daß man bei verschiedenen Wahlmöglichkeiten nicht etwa vor der Entscheidung steht, Datenschutz "abzuwählen" oder erst "zuzuwählen". Die datenschutzfreundliche Grundregelung des Gesetz- oder Verordnungsgebers wird sich vielmehr regelmäßig an der voraussichtlichen Interessenlage der meisten oder jedenfalls sehr vieler Bürger orientieren und für sie einen angemessenen Datenschutz vorsehen. Die Interessenabwägung des Einzelnen kann wegen seiner individuellen Belange davon erheblich abweichen, so daß mit einer oder mehreren Wahlmöglichkeiten ein Mehr an Selbstbestimmung überhaupt erst eröffnet wird. Ohne solche Alternativen würde der Einzelne eine zwar generell datenschutzfreundliche, für seine Belange aber gerade nicht passende Regelung hinnehmen müssen.

1.1.3 Einwilligung

Bei der Entscheidung zwischen verschiedenen Wahlmöglichkeiten handelt es sich zugleich um eine Fortentwicklung der Einwilligung, die dann über eine bloße Ja/Nein-Entscheidung hinausgeht. Deshalb sind sorgfältig die Risiken zu berücksichtigen, die mit einer Einwilligung verbunden sind, zumal die Wahlmöglichkeiten häufig vom Anbieter vorstrukturiert sind und nicht die Belange jedes Nutzers im Einzelfall umfassen. Die Einwilligung ist insbesondere problematisch, wenn der Bürger seine Daten auch bei mehreren Alternativen nur unter faktischem Zwang an Verwaltung und Wirtschaft weitergibt oder von sich aus persönliche Daten preisgibt, ohne die Tragweite zu überblicken.

Bei der rechtlichen Ausgestaltung und der Anwendung in der Praxis ist daher darauf zu achten, daß der Bürger über alle wesentlichen Kriterien informiert ist und dann eine diskriminierungsfreie Entscheidung treffen kann. Einwilligungen sind insgesamt nur als rechtswirksam anzuerkennen, wenn sie den datenschutzrechtlichen Anforderungen voll genügen (siehe dazu eingehend 14. TB, 1.2 mit zahlreichen Beispielen).

Wenn dies voraussichtlich nicht zu gewährleisten ist, verbleibt nur eine Datenschutzregelung ohne Alternativen. Dies kann auch der Fall sein, wenn eine Wahlmöglichkeit sich zu Lasten des

Datenschutzes Dritter ohne angemessene Vorkehrungen auswirken würde, z. B. beim Ausdruck der Daten der angerufenen Telekommunikationsteilnehmer ohne deren Kenntnis und Entscheidungsmöglichkeit für oder gegen dieses Verfahren.

1.1.4 Unterschiede zwischen Verwaltung und Wirtschaft

Bei den Wahlmöglichkeiten ist zwischen der Rechtslage in der Verwaltung, insbesondere der Eingriffsverwaltung, und der Wirtschaft zu unterscheiden (siehe 14. TB, 1.2.2).

Bei hoheitlich-repressiven Eingriffen in die informationelle Selbstbestimmung zugunsten eines überwiegenden Allgemeininteresses muß sich die notwendige Rechtsnorm auf die geringstmögliche Eingriffstiefe beschränken. Wenn dasselbe vorgegebene Ziel auf mehr oder weniger eingriffsintensive Weise erreicht werden kann, ist bereits vom Staat der weniger intensive Eingriff "auszuwählen". Hier besteht grundsätzlich kein Raum für Wahlmöglichkeiten des Bürgers - ebensowenig wie für Einwilligungslösungen.

Denkbar sind Wahlmöglichkeiten des Bürgers zwischen zwei verschiedenartigen, aber vergleichbar intensiven Eingriffen in die informationelle Selbstbestimmung. Ein Beispiel ist dafür im sensiblen medizinischen Bereich die schulärztliche Untersuchung; auf diese Untersuchung kann nach § 34 Abs. 6 Hamburgisches Schulgesetz verzichtet werden, wenn eine ihr entsprechende privatärztliche Untersuchung nachgewiesen wird. Ein weiteres Beispiel gibt es bei der Sicherheitsüberprüfung hinsichtlich der Art der Datenspeicherung (13.1).

In der Leistungsverwaltung geht in der Regel die Initiative vom Bürger aus; er beantragt eine Leistung aus einem gesetzlich vorgegebenen Katalog. Je nach "ausgewählter" Leistung sind unterschiedliche Voraussetzungen einschließlich erforderlicher Datenoffenbarungen zu erfüllen. Eine Wahlmöglichkeit bezüglich der Datenoffenbarungen bei feststehender Leistungsart besteht grundsätzlich nicht, weil auch hier nur der erforderliche Mindesteingriff zulässig ist. Bezüglich des Leistungsziels selbst - also hinsichtlich des Ob, nicht des Wie - kann der Bürger je nach Leistungsart ggf. einzelnen Teilleistungen bzw. Leistungsteilen mit begrenzten Datenoffenbarungen zustimmen.

Beim Handeln der Verwaltung in Privatrechtsform und insgesamt in der Wirtschaft ist für die informationelle Selbstbestimmung des Bürgers in der Regel die Vertragsfreiheit maßgeblich. Daher kann der Bürger in diesem Bereich rechtlich sowohl hinsichtlich des Ob als auch des Wie selbst bestimmen und "auswählen". Neue Wahlmöglichkeiten sind bei den Multimediadiensten in den seit August 1997 geltenden Rechtsvorschriften enthalten, insbesondere mit der Pflicht für die Anbieter, den Nutzern eine anonyme oder pseudonyme Variante anzubieten (3.5).

Im Banken- und Versicherungsbereich hat der Bürger zwar realistischerweise keine Wahl, ob er ein Konto einrichten oder sich gegen schwere Risiken durch Versicherungen schützen will. Beim Datenaustausch zwischen diesen Branchen hat er aber bestimmte Auswahlmöglichkeiten (21.1 und 15. TB, 25.1). Für kartengestützte Zahlungssysteme z. B. bei der Geldkarte kann man zwischen personenbezogenen und anonymen Alternativen wählen (21.2).

1.1.5 Widerspruchsrecht

Die bisher geregelten Fälle mit Widerspruchsmöglichkeiten sind dagegen weniger hilfreich für eine soziale Informationsordnung. Die Grundregelung wirkt sich dann regelmäßig zugunsten von Verwaltung und Wirtschaft und gegen den Bürger aus, wenn er nicht tätig wird; es bleibt dem Einzelnen überlassen, erst durch seinen Widerspruch den Datenschutz nachzubessern.

Um so wichtiger ist es dann, daß er über seine Möglichkeiten zum Selbstdatenschutz umfassend informiert ist. Deshalb haben wir z. B. gemeinsam mit den Landesbeauftragten für den Datenschutz in Bremen und Niedersachsen eine Informationsschrift "Tips zum Adressenhandel" herausgegeben, die über das Widerspruchsrecht gegen die Adressenverwendung für Zwecke der Werbung oder der Markt- und Meinungsforschung unterrichtet (12. TB, 22.2). Interessierten Bürgern stellen wir das Informationsblatt weiterhin zur Verfügung (siehe am Ende dieses TB bei Veröffentlichungen zum Datenschutz).

Die Unzulänglichkeit des Widerspruchsrechts hat sich am Beispiel der Datenübermittlung aus Melderegistern an Parteien zu Wahlwerbezwecken erneut besonders deutlich gezeigt. Die unverlangte Zusendung adressierter Wahlwerbung führte zur größten Zahl von Bürgerbeschwerden seit der Volkszählung; den Bürgern war das Widerspruchsrecht trotz wiederholter öffentlicher Hinweise weitgehend nicht bekannt, so daß sie in ihren Eingaben häufig dem Staat die Verantwortung für einen derart mangelnden Datenschutz anlasteten (11.2).

Ein neuer Ansatzpunkt könnte sich aus dem künftigen generellen Widerspruchsrecht aufgrund der europäischen Datenschutzrichtlinie ergeben (1.2). Gemäß der vorgesehenen Anpassung des Bundesdatenschutzgesetzes (BDSG) sind künftig gesetzmäßig verarbeitete Daten zu sperren, soweit der Betroffene ihrer Verarbeitung widerspricht und seine schutzwürdigen Interessen überwiegen. Als Beispiele für ein derartiges Widerspruchsrecht werden im Entwurf der amtlichen Begründung zur BDSG-Änderung die bereits bestehenden unterschiedlichen Möglichkeiten für Auskunftssperren nach dem Melderecht angegeben.

1.1.6 Verfahrensrechte

Schließlich kommen Wahlmöglichkeiten auch bei den Verfahrensrechten wie insbesondere dem Auskunftsrecht in Betracht. Im geänderten Hamburgischen Datenschutzgesetz wird nunmehr z. B. ausdrücklich die Möglichkeit einer Auskunft auch durch Akteneinsicht oder Datenausdruck genannt; der Betroffene hat dabei einen Anspruch auf ermessensfehlerfreie Entscheidung über die von ihm verlangte Auskunftsart (1.3.1). Nach unserer Auffassung haben die Behörden bei einer Verweigerung einer solchen Auskunftsart den Betroffenen darauf hinzuweisen, daß er sich zur Klärung an den Datenschutzbeauftragten wenden kann.

1.1.7 Schlußfolgerungen

Insgesamt werden diese Erweiterungen bei der informationellen Selbstbestimmung dem Bürger nur zugute kommen, wenn er darüber leicht zugänglich und allgemein verständlich informiert wird. Wie bereits früher in Hamburg praktiziert und insbesondere von Berlin und Brandenburg weiterentwickelt, kann dem Bürger dabei ein "Datencheckheft" nützen. In Form von Briefkarten sind dort vorformulierte kurze Schreiben über verschiedene Bürgerrechte einschließlich Einwilligung, Widersprüchen, Auskunftsrechten usw. zusammengefaßt. Im neuen Hamburger Datencheckheft haben wir auch verschiedene Wahlmöglichkeiten dargestellt (siehe auch 1.4.2).

Bei sämtlichen erwähnten Absicherungen und weitestgehender Transparenz ist nicht auszuschließen, daß Bürger dennoch eine Fehlentscheidung treffen, die sie - selbst bei einem Widerruf - jedenfalls für die Vergangenheit nicht mehr korrigieren können. Bei mehr Freiheit für mehr Bürger bleiben also unbestreitbar Risiken. Mit dem Recht aus informationelle Selbstbestimmung wäre es aber nicht vereinbar, wenn der Staat vertretbare Wahlmöglichkeiten von vornherein unterbinden und damit dem mündigen Bürger selbstverantwortete Entscheidungen vorenthalten würde.

Datenschutz soll die Bürger - auch in bester Absicht - nicht bevormunden, sondern die Selbstbestimmung so weit wie möglich fördern. Dazu soll die Darstellung vielfältiger Wahlmöglichkeiten als Schwerpunkt in diesem Tätigkeitsbericht beitragen. Die große Bandbreite im Umgang mit dem Selbst soll mit den Varianten zur Selbstbestimmung verdeutlicht werden, die auf der Rückseite dieses TB wiedergegeben sind.

1.2 EG-Datenschutzrichtlinie und Bundesdatenschutzgesetz

Auch über 2 Jahre nach Annahme der EG-Datenschutzrichtlinie am 24. Oktober 1995 liegt immer noch kein innerhalb der Bundesressorts abgestimmter Regierungsentwurf vor. Die Beteiligung der Länder und der Verbände erfolgt nach Abschluß des Abstimmungsverfahrens. Eine fristgerechte Umsetzung in das deutsche Datenschutzrecht wird auch wegen des Ablaufs der Legislaturperiode kaum noch erwartet.

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer Konferenz am 23./24. Oktober 1997 an die Bundesregierung appelliert, für eine fristgerechte Umsetzung der Richtlinie Sorge zu tragen. Sie haben ihre Forderungen zur Harmonisierung des europäischen Datenschutzrechts und Anpassung der gesetzlichen Regelungen an die Verhältnisse der modernen Informationsgesellschaft erneuert.

Dem Gesetzgeber haben sie folgende Grundsatzentscheidungen empfohlen:
- weitgehende Gleichbehandlung des öffentlichen und des privaten Bereichs bei gleichzeitiger Verbesserung der Datenschutzkontrolle
- Bestellung weisungsfreier Datenschutzbeauftragter auch bei öffentlichen Stellen
- Bürgerfreundlichkeit durch einfache und verständliche Formulierung des BDSG
- Gewährleistung eines einheitlichen, hohen Datenschutzniveaus durch Beibehaltung der Funktion des BDSG und der Landesdatenschutzgesetze als Querschnittsgesetze
- Sonderregelungen für Presse und Rundfunk nur, soweit zur Sicherung der Meinungsfreiheit notwendig.

Zur Anpassung an die Informationsgesellschaft haben die Datenschutzbeauftragten u. a. vordringlich gefordert:
- Verbindliche Grundsätze für anonyme und pseudonyme Datenverarbeitung, Verschlüsselung und Risikoanalyse
- Einführung eines Datenschutzaudits zur Transparenz für Verbraucher und Anbieter
- Regelung der Videoüberwachung und der Chipkarten-Anwendungen.

Der genaue Wortlaut der Entschließung ist im Internet unter der Adresse "www.hamburg.de/Behoerden/HmbDSB" abrufbar.

1.3 Hamburgische Datenschutzvorschriften

1.3.1 Hamburgisches Datenschutzgesetz

Das Gesetz zur Änderung des Hamburgischen Datenschutzgesetzes wurde von der Bürgerschaft am 18. März 1997 beschlossen. Über das Gesetzgebungsverfahren und unsere Vorschläge zum Gesetzentwurf des Senats haben wir ausführlich berichtet (vgl. 13. TB,1.5.1; 14. TB, 1.3.1; 15. TB, 1.1; 1.5.1).

1.3.2 Bereichsspezifische Datenschutzvorschriften

Einen bedeutsamen Beitrag zum parlamentsspezifischen Datenschutz leistet das am 27. August 1997 beschlossene Gesetz über die Untersuchungsausschüsse der Hamburgischen Bürgerschaft (vgl. 4.1).

Nach intensiver Beratung wurden das Hamburgische Schulgesetz (HmbSG) am 16. April 1997 und auf seiner Grundlage die Verordnung über die Verarbeitung personenbezogener Daten in den Schulen (Schul-Datenschutzverordnung) am 1. Juli 1997 erlassen. Die seit langem angestrebte Regelung des Datenschutzes im Schulbereich (s. 13. TB, 9.1) wurde damit endlich erreicht. Aufgrund unserer Vorschläge wurden insbesondere die Regelungen zum Datenschutz in den Schulgremien teilweise verbessert.

Mit dem Fünften Gesetz zur Änderung des Hamburgischen Meldegesetzes vom 25. Juni 1997 wurde die Rechtsgrundlage für die regelmäßige Übermittlung bestimmter Meldedaten an den Norddeutschen Rundfunk (NDR) geschaffen. Der NDR wird aussagefähige Berichte über die Anwendung und Auswirkungen dieser Regelung erstatten, wie von uns angeregt (vgl. 15. TB, 12.1).

Vorschriften über Online-Abrufe aus öffentlichen Registern enthalten die Verordnung über den automatisierten Abruf und die automatisierte Speicherung, Veränderung und Löschung von Daten aus dem Flächenbezogenen Informationssystem (FIS-OnlineVO) vom 17. Juni 1997 (vgl. 10.1) und die Verordnung zur Änderung von Verordnungen zur Durchführung des Hamburgischen Meldegesetzes vom 9. September 1997 (vgl. 11.1).

Mit dem Entwurf eines Hamburgischen Sicherheitsüberprüfungsgesetzes (HmbSÜG) hat sich der Senat bislang nicht befaßt. Es fehlt seit langem der Entwurf eines hamburgischen Gesundheitsdienstgesetzes; immerhin ist vor Jahresende 1997 eine Behördenabstimmung geplant.

1.4 Verhältnis zum Bürger

Das Interesse der Bürger an Datenschutzinformationen, -beratung und -unterstützung steigt weiter an. Bei besonderen Problemfällen reichte unsere Telefonkapazität zeitweise nicht aus; die unverlangte Zusendung adressierter Wahlwerbung führte im September 1997 zur größten Zahl von Bürgerbeschwerden seit der Volkszählung (11.2). Wir sind während der gesamten Arbeitszeit ohne feste Sprechstunden für die Bürger erreichbar; daher konnten wir auf die früheren zusätzlichen Bürgersprechstunden verzichten.

1.4.1 Eingaben

Aus dem öffentlichen und dem nicht-öffentlichen Bereich richteten die Bürger wieder viele Eingaben an uns. Bis Ende November 1997 gingen 426 schriftliche Eingaben - und damit noch mehr als nach dem hohen Stand von 1996 - zu folgenden Themen ein:

Öffentlicher Bereich	217
davon Inneres und Justiz	120
Gesundheit und Soziales	42
Sonstiges	55
Nicht-öffentlicher Bereich	209
davon Versandhandel	12
Versicherungswirtschaft	29
Kreditwirtschaft	16

Werbung, Direktmarketing 31
Arbeitnehmer-Datenschutz 13
Schufa und Auskunfteien 28
Gesundheitswesen 5
Wohnungswirtschaft 7
Verkehrswesen 4
Markt- und Meinungsforschung 3
Sonstiges 61

1.4.2 Öffentlichkeitsarbeit einschließlich eigenem Internet-Angebot

Gemäß meiner Ankündigung im Vorwort zu diesem TB haben wir uns verstärkt darum bemüht, von der Information zur Kommunikation mit dem Bürger, der Verwaltung und der Wirtschaft überzugehen.

Bei der Veranstaltung "Was erwartet die Wirtschaft vom Datenschutz?" zusammen mit der Handelskammer am 1. Oktober 1997 konnten wir intensiv mit den Vertretern der Wirtschaft, darunter zahlreichen betrieblichen Datenschutzbeauftragten, die aktuellen Fragen zum neuen Datenschutzrecht durch Novellierung des BDSG und zur Datenschutzaufsicht erörtern.

Außerdem führten wir mit der Volkshochschule einen Datenschutzkurs an vier Abenden durch. Die Fortsetzung derartiger Angebote werden wir mit der Volkshochschule besprechen.

Auf unserer Pressekonferenz zur Jahresmitte 1997 stellten wir die neue Broschüre zum hamburgischen Datenschutzrecht vor. Die Broschüre enthält den Text des im März 1997 novellierten Hamburgischen Datenschutzgesetzes (1.3.1) mit umfassenden Erläuterungen anhand der amtlichen Begründungen und der bürgerschaftlichen Gesetzesberatungen zu den weiterhin geltenden und den veränderten Vorschriften. Als Überblick über wichtige bereichsspezifische Regelungen wurden außerdem weitere hamburgische Datenschutzvorschriften abgedruckt, z. B. aus dem Melderecht, dem Polizei- und Verfassungsschutzrecht, dem Gesundheitsrecht, dem Medienrecht und dem Schulrecht. Weiteres Thema in dieser Pressekonferenz war der unzureichende Datenschutz in Arztpraxen (19.2).

Häufiger als bisher wandten wir uns außerdem mit gesonderten Pressemitteilungen an die Öffentlichkeit u. a. zum verbesserten Datenschutz bei Multimedia nach Inkrafttreten des Teledienstedatenschutzgesetzes des Bundes und des Mediendienste-Staatsvertrages der Länder (3.5) und zu datenschutzrechtlichen Problemen bei der Durchführung der Bürgerschaftswahl (11.2). Zur weiteren Bürgerinformation haben wir fast jeden Monat Datenschutzfälle, die viele Bürger betreffen, der Presse mitgeteilt, z. B. über ärztliche Fragebögen, Datenschutzmängel bei Online-Diensten, unzureichenden Datenschutz bei elektronischen Geldkarten sowie Datenschutzprobleme für Wohnungsuchende.

Erstmals haben wir zusammen mit dem Datenschutzbeauftragten eines großen Unternehmens eine Broschüre herausgegeben. Anläßlich des Inkrafttretens des neuen Multimediarechts (3.5) haben wir in der Reihe "Hamburger Datenschutzhefte" zusammen mit Prof. Büllesbach als Datenschutzbeauftragten des debis Systemhauses die Broschüre "Datenschutz bei Multimedia und Telekommunikation" veröffentlicht. In Kooperation mit der Fachhochschule München und mehreren Obersten Aufsichtsbehörden für den Datenschutz wurde das Faltblatt "Der betriebliche Datenschutzbeauftragte" hergestellt.

Als Bürgerservice haben wir Ende 1997 ein neugestaltetes Datencheckheft herausgegeben. In Form von Briefkarten sind dort Musterschreiben zusammengefaßt, mit denen die Bürger ihre Datenschutzrechte gegenüber verschiedenen öffentlichen und nicht-öffentlichen Stellen auf einfache Weise wahrnehmen können. Damit soll zugleich die Darstellung in diesem Tätigkeitsbericht über Selbstdatenschutz mit Wahlmöglichkeiten (1.1) praktisch umgesetzt werden. Damit das Datencheckheft viele Bürger erreicht, ist es nicht nur in unserer Dienststelle, sondern auch bei der Landeszentrale für politische Bildung, der Öffentlichen Rechtsauskunftsstelle, der Verbraucherzentrale und der Volkshochschule erhältlich.

Unsere lieferbaren Veröffentlichungen sind am Ende dieses TB zusammengefaßt. Dort wird auch auf unser inzwischen weiterentwickeltes Internet-Angebot hingewiesen, das seit dem Sommer 1996 existiert. Auf über 400 Seiten mit einem Gesamtumfang von 3,4 Megabyte sind zahlreiche Informationen zum Thema Datenschutz abrufbar. Der Zugang zu diesem Angebot ist allen Internet-Nutzern unter der Adresse "www.hamburg.de/Behoerden/HmbDSB" möglich.

Im Internet werden unsere aktuellen Pressemitteilungen bereitgehalten. Unter dem Stichwort "Neuigkeiten" wird über aktuelle Geschehnisse aus dem Bereich des Datenschutzes informiert, z. B. über die Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

Die bisher erschienenen Broschüren und Faltblätter des Hamburgischen Datenschutzbeauftragten lassen sich unter "Weitere Materialien zum Datenschutz" finden, z. B.
- Datensicherheit bei Windows NT
- Anforderungen zur informationstechnischen Sicherheit von Chipkarten
- Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet
- Datenschutz im privaten Bereich
- Was machen Handels- und Wirtschaftsauskunfteien?
- Datenschutz in der Arztpraxis
- Datenschutz bei Multimedia und Telekommunikation.

Weiterhin können die Tätigkeitsberichte des Hamburgischen Datenschutzbeauftragten (ab 1994) abgerufen werden. Dort ist auch unsere Geschäftsverteilung mit den Zuständigkeiten der Mitarbeiter wiedergegeben.

Unter der Rubrik "Veröffentlichungen von Mitarbeitern des Hamburgischen Datenschutzbeauftragten" wird auf deren Literaturbeiträge hingewiesen.

Einen großen Raum nimmt der Bereich "Datenschutzrecht" mit der geltenden Fassung des Bundesdatenschutzgesetzes und dem - im März 1997 novellierten - Hamburgischen Datenschutzgesetz einschließlich Erläuterungen ein. Ferner werden Auszüge aus weiteren hamburgischen Rechtsvorschriften mit datenschutzrechtlicher Relevanz bereitgestellt, z. B. zum Datenschutz bei der Polizei, im Krankenhaus und in den Schulen.

1.4.3 Zusammenarbeit mit Verwaltung und Justiz

Mit den hamburgischen öffentlichen Stellen haben wir weiterhin aufgeschlossen zusammengearbeitet. Das Datenschutz-Jahrestreffen wurde diesmal ersetzt durch die Einführung in meine zweite Amtszeit, an der Vertreter der Bürgerschaft, Justiz, Verwaltung, Kammern und Gewerkschaften teilnahmen. In den nächsten Jahren beabsichtige ich, jeweils im ersten Quartal

schwerpunktmäßig ein Treffen mit einem Bereich aus Verwaltung und Justiz zur Erörterung der dort anstehenden Datenschutzfragen durchzuführen.

Im Jahr 1997 habe ich zwei förmliche Beanstandungen wegen schwerwiegender Datenschutzverstöße vorgenommen. Die immer noch ungesicherten Zugriffsmöglichkeiten der Wartungstechniker aus Kalifornien auf die Patientenüberwachungsanlage im UKE (19.3) waren ebenso zu beanstanden wie die unzureichende Absicherung der Telekommunikationsanlage Behörden Alter Steinweg (3.4). In beiden Fällen konnte mit den betroffenen Behörden Einvernehmen hergestellt werden, daß seit langem bestehende Datenschutzmängel sobald wie möglich abzustellen sind.

2. Entwicklung der Dienststelle

Die von mir verlangte personelle Verstärkung im IuK-Bereich (15. TB, 2.) hat der Senat nicht beschlossen. Die Sparmaßnahmen führten sogar dazu, daß der Stellenbestand der Dienststelle reduziert wurde. Bei nunmehr 14,5 Stellen für den Datenschutz in Verwaltung und Wirtschaft bei gleichzeitig zunehmenden Aufgaben muß mindestens der Bestand erhalten bleiben.

Im Sachhaushalt beteiligten wir uns an den Einsparungen und werden auch künftig die für uns errechneten Sparbeiträge möglichst vollständig erbringen. Hier wurde unsere finanzielle Handlungsmöglichkeit dadurch erleichtert, daß die gegenseitige Deckungsfähigkeit dieser Haushaltsmittel aufgrund der zwischenzeitlichen Budgetierung für unseren Bereich erstmals voll genutzt werden konnte. Ohne die damit mögliche Umschichtung hätten die jeweils im Haushaltsplan festgelegten Mittel nicht ausgereicht.

Zum neuen Steuerungsmodell haben auch wir in der Dienststelle eine Gruppe zu Beginn meiner zweiten Amtszeit gebildet. Gemäß den Herausforderungen an den Datenschutz aktualisieren wir die Zielfindung und die Handlungsmöglichkeiten für einen effektiven Schutz zugunsten des Bürgers. Wir haben eingehend erörtert, wie wir unsere Arbeit angesichts knapper Ressourcen mit dem Hauptziel eines bürgerfreundlichen Datenschutzes umstrukturieren können. In diesen Zusammenhang gehören auch meine Bemühungen, inhaltlich und kostenwirksam mit verschiedenen Partnern zu kooperieren, z. B. bei Veranstaltungen und Veröffentlichungen (1.4.2).

3. Informations- und Kommunikationstechnik/Neue Medien

3.1 Datensicherheit bei Windows NT

Wir haben am Anfang des Berichtszeitraums ausführlich das Betriebssystem Windows NT unter datensicherheitstechnischen Gesichtspunkten getestet. Evaluiert wurden zwar die Workstation- und die Server-Version 3.51, die Grundaussagen des Tests sind jedoch auch für die NT-Version 4.0 gültig.

Insgesamt sind die zur Verfügung gestellten Datensicherheitsmechanismen als wirksam einzuschätzen. Dies gilt insbesondere für den abgesicherten Systemzugang, die differenzierte Vergabe von Zugriffsrechten, den Schutz von Windows-NT-Objekten und für die umfangreichen Protokollfunktionen. Dennoch weist das NT-System einige Schwachstellen auf, die beachtet und ggf. kompensiert werden müssen.

1. NTFS-Partitionen:
Ein Teil der Sicherheitsfunktionen kann nur dann aktiviert werden, wenn für das Windows-NT-System das spezifische NTFS-Format verwendet wird. Die Verwendung des NTFS-Formats ist

daher zwingend erforderlich. Windows-NT-Systeme, die bereits mit dem DOS-spezifischen FAT-Dateisystem eingerichtet wurden, sollten deshalb in das NTFS-Format konvertiert werden.

2. Windows-NT-Clients:
Die Sicherheit eines Windows-NT-Netzwerks hängt entscheidend von der Sicherheit des Client-Betriebssystems ab. Clients, die über keine abgesicherten Zugangsmechanismen verfügen (wie z. B. Windows 3.11), sollten daher in keinem Windows-NT-Netzwerk eingesetzt werden, in dem sensible personenbezogene Daten verarbeitet und gespeichert werden. Dies gilt in besonderem Maße für Peer-to-Peer-Umgebungen.

3. Stellung der Administratoren:
Windows NT kann nicht so konfiguriert werden, daß der Aufruf der Administratorkennung zwingend die Eingabe zweier korrekter Paßwörter erfordert. Sofern es notwendig ist, die Systemverwaltung nach dem Vier-Augen-Prinzip zu organisieren, sollte das Systemverwalterpaßwort geteilt werden.

4. Bootschutz:
Ein gravierendes Sicherheitsrisiko liegt im Vorfeld des Windows-NT-Systemstarts. Über ungesicherte Diskettenlaufwerke kann ein NT-fremdes Betriebssystem, wie z. B. MS-DOS, gestartet werden. Anschließend ist es möglich, über das fremde Betriebssystem Programme zu aktivieren, mit deren Hilfe die Windows-NT-Zugriffsmechanismen umgangen werden. Die Anwendung dieser Programme setzt keine besonderen System- oder Hardwarekenntnisse voraus.

Falls auf den Windows-NT-PC sensible personenbezogene Daten gespeichert werden, sind folgende Maßnahmen notwendig:
- Aktivierung eines Bootpaßwortes auf BIOS-Ebene,
- Sicherung des Gehäuses,
- Ausbau von Diskettenlaufwerken,
- Ggf. Einsatz von Sicherheitssystemen, die eine Laufwerkskontrolle und Verschlüsselung des Dateisystems vorsehen.

In Netzwerkumgebungen sollten sensible personenbezogene Daten grundsätzlich nur auf dem Server abgespeichert werden. Dieser muß durch entsprechende organisatorische Schutzmaßnahmen vor dem unautorisierten Zugriff Außenstehender geschützt werden.

5. Verschlüsselung:
Windows NT verfügt standardmäßig über keinerlei Mechanismen zur Verschlüsselung von Inhaltsdaten auf Datenträgern oder Backup-Medien. Sofern sensible personenbezogene Daten verarbeitet werden, sollten zusätzliche Softwareprodukte eingesetzt werden, die eine sichere Verschlüsselung gewährleisten. Entsprechende Produkte sind auf dem Markt verfügbar.

6. CD-ROM-Laufwerke:
CD-ROM-Laufwerke sind, ebenso wie ungesicherte Diskettenlaufwerke, eine potentielle Angriffsfläche für die Windows-NT-Sicherheit. Die Möglichkeit, daß ein Benutzer hierüber das NT-System neu installieren kann, um auf diese Weise bestehende Sicherheitseinstellungen zu unterlaufen, erfordert geeignete Schutzmaßnahmen. Es wird daher empfohlen, CD-ROM-Laufwerke grundsätzlich nicht auf Arbeitsplatzrechnern zuzulassen und nur dort einzusetzen, wo die Möglichkeit einer unautorisierten Neuinstallation organisatorisch ausgeschlossen werden kann.

7. Serielle Schnittstellen:

Unter Windows NT können nur die parallelen Schnittstellen geschützt werden, nicht jedoch die seriellen Schnittstellen. Dieser Mangel ist um so schwerwiegender, als über die seriellen Schnittstellen ein unautorisierter Datentransfer erfolgen kann. Sofern sensible Daten verarbeitet werden, empfiehlt es sich, zusätzliche Sicherheitssoftware zum Schutz der seriellen Schnittstelle einzusetzen.

Die ausführlichere Textversion befindet sich im Internet-Angebot des Hamburgischen Datenschutzbeauftragten (www.hamburg.de/Behoerden/HmbDSB).

3.2 Prüfung des Firewalls des Landesamtes für Informationstechnik (LIT)

Wir haben zuletzt im 14. TB über Firewall-Systeme berichtet und dabei grundlegende datenschutzrechtliche Anforderungen an solche Systeme gestellt
(14. TB, 3.1.3).

Seit einigen Monaten betreibt das LIT ein Firewall-System. Damit werden zum einen externe Nutzer sicher an das automatisierte Grundbuch (siehe 14. TB, 17.7) angebunden und zum anderen eine Internet-Nutzung für Verwaltungsstellen ermöglicht. Auf Grundlage der oben genannten Anforderungen haben wir dieses Firewall-System einer datenschutzrechtlichen Prüfung unterzogen.

Im Ergebnis läßt sich feststellen, daß ein erfreulich hohes Sicherheitsniveau erkennbar war und das eingesetzte System sowohl von der konzeptionellen, als auch von der technischen und administrativen Seite her in der Lage ist, die Anforderungen des Datenschutzes zu erfüllen. Eine Gefährdung personenbezogener Daten konnte nicht festgestellt werden. Dies gilt sowohl für solche Daten, die über den Firewall vermittelt werden, als auch für solche Daten, die im geschützten Verwaltungsnetz verarbeitet werden.

Besonders erfreulich ist für uns die Tatsache, daß das LIT zur Realisierung des Verfahrens Grundbuchautomation auf Verschlüsselungstechniken zurückgegriffen hat. Die sichere Anbindung externer Nutzer (z. B. Notare) erfolgt mit der Technik sog. Virtueller Privater Netze (VPN). Dabei wird in öffentlichen Netzen die Vertraulichkeit und die Geschlossenheit der Benutzergruppe durch kryptografische Methoden sichergestellt. Wir hoffen, daß die bisherigen Schwierigkeiten des LIT mit dem Thema der Verschlüsselung damit zumindest teilweise beseitigt sind. Eine Ausdehnung der Verschlüsselung auch auf Verfahren innerhalb des Verwaltungsnetzes ist jedenfalls nun technisch möglich.

Da die Prüfung zum Redaktionsschluß dieses Berichts noch nicht abgeschlossen ist, besteht noch Klärungsbedarf in der Frage der zentralen Virenkontrolle bzw. der Überprüfung von Java- oder Active-X-Programmen. Das LIT erarbeitet dazu zur Zeit eine Lösung. Ebenfalls offen ist der Umfang der Protokollierung nicht sicherheitsrelevanter Ereignisse auf dem Firewall; das Kommunikationsverhalten von Benutzern soll nicht analysiert werden.

3.3 SAP-Prüfung in Allgemeinen Krankenhäusern

Über den Datenschutz bei SAP-Systemen hat der Hamburgische Datenschutzbeauftragte bereits ausführlich berichtet (14. TB, 3.2 und 19.2). Die seinerzeit eher konzeptionell geprägte Darstellung wird nunmehr um Ergebnisse und Einschätzungen ergänzt, die aus einer Prüfung des SAP-Systems IS-H im Allgemeinen Krankenhaus (AK) Eilbek resultieren, das auch Daten für andere Krankenhäuser in Hamburg verarbeitet (AK Bergedorf, Heidberg und Wandsbek). Geplant ist weiterhin eine Prüfung des AK Altona.

3.3.1 Aufnahmemasken

Sehr positiv fiel bei der Prüfung des AK Eilbek auf, daß im Vergleich zum SAP-Standard weit weniger Daten über die Patienten erfaßt werden. So wird beispielsweise die Religionszugehörigkeit des Patienten in den Aufnahmemasken nicht mehr abgefragt. Damit wird unserer Forderung entsprochen, die Datenerhebung im Interesse der Patienten auf das für die Aufnahme erforderliche Maß zu beschränken.

3.3.2 Administration der SAP-Server

Im AK Eilbek sind für die Anwendung IS-H insgesamt 9 Server in Betrieb: Zwei getrennte Datenbank- und Anwendungs-Server für jedes der vier Krankenhäuser Bergedorf, Eilbek, Heidberg und Wandsbek sowie ein gemeinsamer Testrechner.

Die SAP-Hardware und -Software wird von 5 Personen mit umfassenden Zugriffsrechten auf sämtliche Server administriert. Zusätzlich können jedoch noch zahlreiche weitere Mitarbeiter der Krankenhausverwaltung auf Echtdaten zugreifen, ohne daß dies von der fachlich zuständigen Stelle bemerkt würde. Dies gilt auch für die Patientendaten, die vom AK Eilbek im Auftrag verarbeitet werden.

Programme können darüber hinaus ohne Auftrag von der Test- in die Produktionsumgebung überführt werden. Aufgrund fehlender Protokollierung kann nicht nachvollzogen werden, zu welchem Zweck und zu welcher Zeit welche Programmänderungen von welchem Mitarbeiter in die Produktion gegeben wurden. Hierdurch besteht u. a. die Gefahr, daß Zugriffsrechte erweitert werden, indem der für die Zugriffskontrolle entscheidende Authority Check in den Programmen gelöscht bzw. zugunsten bestimmter Benutzer manipuliert wird.

Die fehlende Trennung von Test und Produktion, das fehlende Freigabeverfahren sowie die viel zu hohe Anzahl von Benutzern mit privilegierten Zugriffsrechten ist datenschutzrechtlich problematisch. Zur Verbesserung der SAP-Administration haben wir gefordert, die Anzahl der Mitarbeiter, die auf die Produktionsdaten zugreifen können, erheblich zu reduzieren. Der Zugriff auf die Produktionsrechner sollte protokolliert werden.

Weiterhin sollten die von SAP zur Verfügung gestellten Funktionen eines Benutzer-, Berechtigungs- und Aktivierungsadministrators eingerichtet und
für eine arbeitsteilig organisierte SAP-Administration genutzt werden. Das Verfahren zur Freigabe von Programmen sollte schriftlich festgelegt werden. Die Übergabe von Programmen in den Echtbetrieb ist ebenfalls zu protokollieren.

3.3.3 SAP-Berechtigungskonzept

Ein wesentlicher Kritikpunkt hinsichtlich der Datensicherheit bei SAP-Systemen ist weiterhin das viel zu komplexe SAP-Berechtigungskonzept. Es bietet zwar umfassende Möglichkeiten, differenzierte Zugriffsrechte zu vergeben; aus Sicht eines für SAP verantwortlichen Systemverwalters im Krankenhaus ist das Berechtigungskonzept jedoch schwer administrierbar.

Bei der Prüfung im AK Eilbek konnte weder vollständig ermittelt werden, welche Benutzer auf ausgewählte Dateien oder Datenfelder zugreifen können, noch konnte auf einfache Weise bestimmt werden, für welche Daten einzelne Benutzer zugriffsberechtigt sind. Es ließ sich lediglich für einzelne Benutzer bestimmen, ob sie beispielsweise im Besitz der Zugriffsberechtigung für

Diagnosedaten sind. Ob auch andere Benutzer hierzu in der Lage sind, konnte nicht systematisch nachvollzogen werden.

Die Vergabe der Zugriffsrechte stellt sich im Basissystem R/3 als ein baumartiges Geflecht von Berechtigungen, Sammelberechtigungen, Profilen, Sammelprofilen und Benutzerstammsätzen dar. Wer im Rahmen einer Prüfung oder Systemrevision die Zugriffsrechte einzelner Benutzer überprüfen möchte, kann deshalb nur schrittweise versuchen, dieses Geflecht zu entwirren. Zunächst muß überprüft werden, welches Profil (Schlüsselbund) bzw. welche Profile mit welchen Berechtigungen (bzw. Schlüssel) die einzelnen Benutzer besitzen. Es können auch Sammelberechtigungen (Multifunktionsschlüssel) vorkommen, die sich wiederum aus mehreren Berechtigungen zusammensetzen. Anschließend wird festgestellt, in welchen Programmen und Transaktionen bzw. Dynpros (der bisherigen Analogie entsprechend mit Türen vergleichbar) die den Berechtigungen entsprechenden Berechtigungsobjekte (Schlösser) benutzt werden und auf welche Dateien die jeweiligen Programme und Transaktionen zugreifen.

Die Komplexität wird zusätzlich noch dadurch erhöht, daß es möglich ist, den Zugriff auf Programme und Transaktionen vom Besitz mehrerer Berechtigungen abhängig zu machen. Falls jedoch - in der bisherigen Analogie gesprochen - in eine Tür mehrere Schlösser eingebaut werden, für die mehrere Schlüssel notwendig sind, die wiederum an mehreren Schlüsselbunden hängen, ist es äußerst mühsam, den Kreis der Zutrittsberechtigten abschließend zu bestimmen.

Folglich kann in umgekehrter Reihenfolge auch nur sehr umständlich geprüft werden, welche Benutzer auf ausgesuchte Datenfelder zugreifen können. Eine vollständige Übersicht über sämtliche vergebenen Zugriffsrechte ist angesichts von über 300 IS-H-Tabellen, ähnlich vielen IS-H-Programmen, Berechtigungen und Berechtigungsobjekten nur sehr zeitaufwendig zu erstellen.

Als Folge der Intransparenz werden von den zuständigen Systemverwaltern zunächst die zur Verfügung gestellten Standardprofile dahingehend geprüft, ob sie direkt oder in leicht modifizierter Form für einzelne Benutzer übernommen werden können. Wenn die Standardrechte nicht ausreichen, werden die Profile solange erweitert, bis der Zugriff auf die gewünschten Systemressourcen gewährt wird. Hilfreich sind in dieser Hinsicht die vom SAP-Berechtigungskonzept eingeblendeten Fehlermeldungen, die darauf hinweisen, an welcher fehlenden Berechtigung der Zugriff bislang gescheitert ist. Leider wird bei dieser Art der Zugriffsvergabe nicht geprüft, ob durch die zusätzlich vergebenen Berechtigungen vielleicht auch der Zugriff auf andere Programme oder Masken freigegeben wird.

Dieses Verfahren hat im AK Eilbek beispielsweise dazu geführt, daß Ärzte grundsätzlich auf sämtliche Patientendaten - sowohl Aufnahmestammdaten als auch medizinische Daten - noch Jahre nach der Entlassung des Patienten zugreifen können. Eine Beschränkung des Zugriffs auf Patienten der eigenen Station erfolgt nicht. Dies gilt auch für die psychiatrische Klinik.

Ebenso kann die "Pförtnerliste" - sie ermöglicht Auskunft über Patientenname, Geburtsdatum und Station - nicht nur vom Pförtner, sondern auch von der Poststelle und von sämtlichen Pflegekräften aufgerufen werden. So kann jede Krankenschwester über die Pförtnerliste erfahren, welcher Patient im AK Eilbek aufgenommen bzw. wann er entlassen wurde. Wie lange die Patienteninformationen noch nach der Entlassung verfügbar sind, kann flexibel bis zu 99 Tagen vom Pförtner, der Poststelle und den Pflegekräften eingestellt werden.

Diese Art der Vergabe der Zugriffsrechte widerspricht der in § 10 HmbDSG geforderten ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen. Trotz der Komplexität und Intransparenz des SAP-Berechtigungskonzepts ist der Anwender von SAP-Systemen dazu

verpflichtet, die SAP-Benutzer und deren Zugriffsrechte revisionssicher zu dokumentieren. Dies ist seitens des AK Eilbek unterblieben.

Um die Ordnungsmäßigkeit des SAP-Verfahrens zu verbessern, ist es zunächst erforderlich, für sämtliche Benutzer bzw. Benutzergruppen (Ärzte, Pflegepersonal, Aufnahmepersonal, Systemadministratoren, Pförtner etc.) den Umfang ihrer Tätigkeit und darauf basierend das Ausmaß der notwendigen Zugriffsrechte schriftlich festzulegen. Eine Einrichtung bzw. Änderung von Zugriffsrechten "auf Zuruf" des jeweiligen Benutzers - wie es im AK Eilbek der Fall ist - sollte durch ein geordnetes Verfahren mit schriftlicher Dokumentation ersetzt werden.

Hierbei ist insbesondere die Frage zu klären, in welchem Umfang die Mitarbeiter - auch Ärzte - auf Daten von Patienten anderer Abteilungen und Stationen zugreifen müssen. Der gegenwärtige unbeschränkte Zugriff überschreitet die datenschutzrechtliche Grenze der "Erforderlichkeit" der Datenverarbeitung, wie sie in §§ 8 und 9 Hamburgisches Krankenhausgesetz (HmbKHG) festgeschrieben ist. Dringend erscheint vor allem, den Mitarbeitern anderer Abteilungen den unmittelbaren Zugriff auf Daten von Patienten der psychiatrischen Klinik zu verwehren. Soweit ein früherer Psychiatriepatient in einer anderen Abteilung behandelt wird, muß sichergestellt sein, daß die Psychiatrie-Daten nur mit Einwilligung des Patienten oder seines Vertreters hinzugezogen werden. Dies sehen auch die krankenhausinternen Dienstanweisungen zur Führung und Herausgabe von Krankenakten und Röntgenbildern vor.

Auch der weitgehende Zugriff auf die "Pförtnerliste" ist nicht erforderlich. Zumindest die Pflegekräfte auf den Stationen werden einen abteilungs- und stationsübergreifenden Zugriff auf Patientendaten kaum benötigen. Wie lange nach der Entlassung noch auf Patientendaten zugegriffen werden kann, sollte nicht vom Pförtner oder der Poststelle selbst, sondern nach strengen Erforderlichkeitskriterien durch die Systemadministration festgelegt werden.

§ 14 Satz 3 HmbKHG fordert darüber hinaus, daß "bei Daten, die in automatisierten Verfahren mit der Möglichkeit des Direktabrufs gespeichert sind, die Möglichkeit des Direktabrufs zu sperren (ist), sobald die Behandlung des Patienten in dem Krankenhaus abgeschlossen ist, die damit zusammenhängenden Zahlungsvorgänge abgewickelt sind und das Krankenhaus den Bericht über die Behandlung erstellt hat". Die zu treffenden Maßnahmen sollten dabei so gestaltet werden, daß Zugriffe bei einer Wiederaufnahme desselben Patienten mit seinem Einverständnis möglich sind.

Wir haben das AK Eilbek aufgefordert, die für die jeweiligen Aufgaben im Krankenhaus erforderlichen Zugriffsrechte schriftlich festzulegen und das SAP-System anschließend dahingehend zu prüfen, inwieweit die realen Berechtigungen den dokumentierten Zugriffsrechten entsprechen. Falls dieses Verfahren aufgrund der Intransparenz der vergebenen Berechtigungsobjekte und Berechtigungen für einige Benutzerkennungen nicht anwendbar ist, sollten für die jeweiligen Benutzer vollständig neue Kennungen bzw. neue Profile mit nachvollziehbaren Zugriffsrechten vergeben werden.

3.3.4 Weiteres Verfahren

Das AK Eilbek hat sich bereit erklärt, ein Freigabeverfahren sowie ein geordnetes Verfahren zur Einrichtung und Änderung von Zugriffsrechten zu erstellen und einzusetzen. Die anderen Forderungen werden zur Zeit noch mit dem AK Eilbek intensiv erörtert. Dabei spielt auch eine entscheidende Rolle, inwieweit die Forderungen durch den Anwender oder durch den Hersteller umgesetzt werden können.

Soweit die Datenschutzprobleme auf systemimmanente SAP-Schwächen zurückzuführen sind, können die Krankenhäuser die genannten Probleme nicht allein und ohne Unterstützung des Herstellers lösen. Wir haben daher
- auch im Zusammenhang mit anderen Sicherheitsdefiziten (u. a. terminalbezogene Zugriffsrechte, vgl. 14. TB, 3.2) - vorgeschlagen, die Schwachstellen des Berechtigungskonzepts sowie Lösungsansätze zur Verbesserung des Datenschutzes mit SAP zu erörtern.

3.4 Prüfung der Sicherheit von ISDN-Telekommunikationsanlagen

Die Prüfung einer ISDN-fähigen Telekommunikationsanlage, an die fast 1800 Nebenstellen (Telefon, Fax) angeschlossen sind, hat Hinweise auf erhebliche datenschutzrechtliche Mängel ergeben, die zu einer förmlichen Beanstandung gemäß § 25 HmbDSG führten.

Für den Betrieb der Anlage ist die Finanzbehörde - Landesamt für Informationstechnik (LIT) - zuständig. An die Telekommunikationsanlage sind zahlreiche Dienststellen der hamburgischen Verwaltung angeschlossen, darunter auch solche, deren Mitarbeiter der ärztlichen Schweigepflicht unterliegen. Hierzu gehören vor allem die Personalärztlichen und Betriebsärztlichen Dienste der FHH.

Es wurden insbesondere folgende Sicherheitsrisiken festgestellt: Die Räumlichkeiten, in denen die Telekommunikationsanlage untergebracht ist, waren unzureichend gegen unbefugten Zutritt gesichert. Personen, denen es infolge der unzureichenden Zugangssicherung gelungen wäre, in diesen Bereich einzudringen, hätten dort z. B. Gespräche abhören und Manipulationen an den Geräten vornehmen können. Da diese Räume nicht regelmäßig von Mitarbeitern des LIT betreten wurden, wären derartige Eingriffe erst viel später bemerkt worden.

Die Schlüsselverwaltung wies erhebliche Mängel auf. Obwohl der Kreis der Zutrittsberechtigten viel zu weit gezogen war, wurde keine Dokumentation darüber geführt, wer die Räumlichkeiten wann betreten hat. Dadurch war eine nachträgliche Feststellung, wer sich Zugang zur Anlage verschafft hat, unmöglich.

Es existierten keine verbindlichen Regelungen für den Zugang zur Anlage - weder für die Wartung vor Ort, noch für die Fernwartung. Der Bereich für die Fernwartung (in den Räumen des LIT) konnte auch von zahlreichen nicht zuständigen Personen betreten werden. Dies war besonders problematisch, weil die dort eingesetzten PC nicht ausreichend gegen unberechtigten Zugriff geschützt waren. Für die Fernwartung existierte zudem keine gesonderte Wartungskennung.

Die Verwaltung der Anlage erfolgte stets mit vollständigen Systemrechten, wobei alle Wartungskräfte dasselbe Paßwort benutzten. Weil keine Protokollierung der vorgenommenen Eingriffe auf Softwareebene existierte, konnten auch hier mögliche Mißbräuche nachträglich nicht festgestellt werden. Dies galt auch für die Fernwartung, die von Mitarbeitern der hamburgischen Verwaltung durchgeführt wird.

Es gab keine verbindlichen Regelungen über eine regelmäßige Änderung des Paßwortes, das zudem auf mehreren Anlagen gültig war. Dies war besonders dann problematisch, wenn externe Wartungskräfte Eingriffe an der Anlage vornehmen mußten. Ein zu diesem Zweck mitgeteiltes Paßwort wurde anschließend nicht regelmäßig geändert. Weiterhin war die Paßwortqualität nur unzureichend. Für einen Lese-Zugriff auf die Konfigurationsdaten der Anschlüsse war überhaupt kein Paßwort erforderlich.

Auch das mit der Anlage verbundene Elektronische Telefonbuch war nur unzureichend gesichert. Dadurch wurden weitere Zugriffsmöglichkeiten mit vollen Systemrechten auf die Anlage eröffnet.

Der Betrieb der Telekommunikationsanlage hat somit insbesondere gegen das Telekommunikationsgesetz und gegen die Telekommunikationsrichtlinie für die hamburgische Verwaltung verstoßen. Die Mängel wiegen deshalb besonders schwer, weil sie - nicht nur bezogen auf diese Anlage - den zuständigen Stellen zumindest im Wesentlichen seit langem bekannt waren. Bereits im 9. Tätigkeitsbericht für 1989 (2.3.3) war über wesentliche konzeptionelle Mängel einer behördlichen TK-Anlage berichtet worden. Im 13. Tätigkeitsbericht (3.5) hatten wir das Thema wieder aufgegriffen und dringend Abhilfe angemahnt. Obwohl die Bürgerschaft unserer Kritik beigetreten war, wurde von den verantwortlichen Stellen - zumindest bezogen auf die geprüfte Anlage - in den wesentlichen Kritikpunkten (unzureichende räumliche Absicherung; Schwachstellen im Administrationskonzept) bis zum Prüfungszeitpunkt keine Abhilfe vorgenommen.

Nach der Prüfung ist das LIT nunmehr endlich daran gegangen, im Rahmen seiner technischen Möglichkeiten mit der Beseitigung von Schwachstellen zu beginnen. So konnte durch kurzfristig durchgeführte Änderungen in der Schlüsselverwaltung das Risiko deutlich verringert werden, daß Unbefugte Zutritt zu TK-Anlagen erhalten. Auch im Hinblick auf den Einbruchsschutz wurden bereits Verbesserungen realisiert. Für die Beseitung weiterer Schwachstellen hat das LIT noch für das Jahr 1997 die Erarbeitung entsprechender Konzepte angekündigt.

Wir werden - ggf. durch weitere Prüfungen - feststellen, inwieweit der nun eingeleitete Prozeß zu einer ausreichenden Absicherung führt.

3.5 Datenschutzrechtliche Anforderungen an Tele- und Mediendienste nach Inkrafttreten des neuen Rechts

Am 1. August 1997 sind das Teledienstedatenschutzgesetz (TDDSG) und die Datenschutzregelungen im Mediendienste-Staatsvertrag (MDStV) in Kraft getreten, die weitgehend miteinander übereinstimmen. Damit besteht in Deutschland ein neuer datenschutzrechtlicher Rahmen für das Angebot und die Nutzung von Multimediadiensten. An der Vorbereitung des neuen Multimediarechts haben wir intensiv mitgewirkt.

Teledienste sind gemäß § 2 Abs. 1 Teledienstegesetz (TDG) alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt. Teledienste sind insbesondere

- Angebote im Bereich der Individualkommunikation (z. B. Telebanking),
- Angebote zur Information oder Kommunikation (z. B. Datendienste Verkehrs-, Wetter-, Umwelt und Börsendatendienste), soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht
- Angebote zur Nutzung des Internets oder weiterer Netze.

Dagegen sind Mediendienste gemäß § 2 Mediendienste-Staatsvertrag an die Allgemeinheit gerichtete Informations- und Kommunikationsdienste in Text, Ton oder Bild. Mediendienste sind insbesondere Verteildienste wie z. B. Fernsehtext oder vergleichbare Textdienste und Abrufdienste, bei denen Text-, Ton- oder Bilddarbietungen auf Anforderung aus elektronischen Speichern zur Nutzung übermittelt werden. Keine Mediendienste, sondern Teledienste sind solche Angebote, bei denen der individuelle Leistungsaustausch oder die reine Übermittlung von Daten im Vordergrund steht.

Für das Angebot von Telediensten und Mediendiensten gelten folgende Grundsätze:

- Personenbezogene Daten dürfen zur Durchführung von Mediendiensten nur erhoben, verarbeitet und genutzt werden, soweit dies durch Rechtsvorschrift erlaubt ist oder soweit der Betroffene eingewilligt hat.
- Die Daten unterliegen einer strengen Zweckbindung; sie dürfen nur für andere Zwecke verwendet werden, soweit eine Rechtsvorschrift es erlaubt oder der Betroffene eingewilligt hat.
- Der Anbieter darf die Erbringung von Medien- und Telediensten nicht von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig machen, z. B. für Werbezwecke.

Die Gestaltung und Auswahl technischer Einrichtungen für das Angebot von Diensten hat sich an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen (Minimierungsgebot). Der Anbieter hat dem Nutzer die Inanspruchnahme von Diensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Die Anbieter haben damit die Wahl, ob sie den jeweiligen Dienst mit oder ohne Preisgabe ihrer persönlichen Daten nutzen.

Weitere Informationen über den "Datenschutz bei Multimedia und in der Telekommunikation" enthält eine Broschüre, die der Hamburgische Datenschutzbeauftragte gemeinsam mit dem Datenschutzbeauftragten des debis Systemhaus herausgebracht hat. Sie kann gegen Zusendung von Briefmarken im Wert von 1,50 DM kostenlos beim Hamburgischen Datenschutzbeauftragten bestellt werden.

3.6 Umsetzung von datenschutzrechtlichen Anforderungen bei interaktiven Angeboten

Die im TDDSG und im Mediendienste-Staatsvertrag festgelegten datenschutzrechtlichen Anforderungen haben sowohl private als auch öffentliche Anbieter von Multimediadiensten zu beachten. Während sich bei reinen Abrufdiensten die datenschutzrechtliche Problematik im wesentlichen auf die Erhebung und weitere Verarbeitung der individuellen Nutzungsdaten reduziert, bestehen bei interaktiven Angeboten zusätzliche Datenschutzrisiken.

3.6.1 Protokollierung des Nutzungsverhaltens

Die Anbieter dürfen gemäß § 15 Mediendienste-Staatsvertrag bzw. § 6 TDDSG personenbezogene Daten über die Inanspruchnahme von Multimediadiensten nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist, um die Inspruchnahme der Dienste zu ermöglichen (Nutzungsdaten) oder um die Nutzung abzurechnen (Abrechnungsdaten). Die Nutzungsdaten sind frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung, zu löschen, soweit es sich nicht um Abrechnungsdaten handelt. Die Abrechnungsdaten sind zu löschen, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind. Dabei muß die Abrechnung so gestaltet werden, daß Anbieter, Zeitpunkte, Dauer, Art, Inhalt und Häufigkeit bestimmter von einem Nutzer in Anspruch genommener Angebote nicht erkannt werden können, es sei denn der Nutzer verlangt einen Einzelnachweis.

Diese strikten Vorgaben stehen im Widerspruch zu einer weithin üblichen Praxis insbesondere im Bereich des Internet, sämtliche Abrufdaten detailliert zu protokollieren, wobei als Identifikationsmerkmal entweder die IP-Nummer und/oder der Name bzw. die E-mail-Anschrift des jeweiligen Nutzers gespeichert wird. Derartige Protokolldateien werden standardmäßig von den meisten Web-Servern unterstützt.

Die Daten sind häufig auch dann personenbezogen, wenn als einziges Identifikationsmerkmal die IP-Nummer gespeichert wird: Zum einen gibt es viele Nutzer mit eigener IP-Nummer. Zum anderen ist es auch bei dynamischer Vergabe von IP-Nummern zumindest den Betreibern der jeweiligen Zugangsrechner möglich, die jeweils zugewiesenen IP-Nummern einzelnen Kunden zuzurechnen.

Diese Praxis hat zur Folge, daß sich der "Surfer" nicht mehr unbeobachtet in dem Internet bewegen kann, sondern daß jeder Schritt irgendwo eine Datenspur hinterläßt.

Die Vollprotokollierung sämtlicher Abrufe ist eine unzulässige Speicherung individueller Nutzungsdaten, denn die Protokolle sind weder für die Vermittlung der Angebote noch zur Abrechnung erforderlich. Üblicherweise liegt auch keine Einwilligung der Betroffenen in die Speicherung vor.

Auch der häufig vorgebrachte Hinweis auf statistische Auswertungen der Abrufdaten rechtfertigt die Speicherung nicht. Für derartige Statistiken wäre es vollständig ausreichend, die Abrufe einzelner Angebote anonymisiert zu erfassen, z. B. indem nur die jeweiligen Domains, aus denen die Abrufe erfolgt sind, gespeichert werden. In vielen Fällen wird es für statistische Zwecke völlig ausreichend sein, lediglich die Anzahl der Abrufe eines bestimmten Angebotes und ggf. die Uhrzeit und das dabei übertragene Datenvolumen zu protokollieren.

3.6.2 Speicherung von Nutzungsdaten bei Internet-Services Hamburg

Die Freie und Hansestadt Hamburg bietet seit Mitte 1996 ein eigenes interaktives Internet-Angebot an. Dieses Angebot wird in der Domain Hamburg.de von der Firma Internet-Services betrieben. Auch das Angebot des Hamburgischen Datenschutzbeauftragten befindet sich auf diesem Server. Dementsprechend haben wir uns frühzeitig dafür eingesetzt, daß der Server datenschutzkonform betrieben wird, insbesondere daß keine individuellen Daten über die Inanspruchnahme von Angeboten gespeichert werden.

Bei einer Prüfung haben wir festgestellt, daß auch hier ursprünglich entsprechend dem "Common Logfile Format" (CLF) eine Vollspeicherung sämtlicher Abrufdaten stattfand. Auf unsere Intervention hin ist diese Praxis Anfang 1997 abgestellt worden. Seither werden keine individuellen Nutzungsdaten über den Abruf gespeichert.

3.6.3 Sozialleistungsverfahren im Internet

Die Behörde für Wissenschaft und Forschung beabsichtigt, das Internet für die Stellung von BAföG-Anträgen nutzbar zu machen, und hat uns Gelegenheit zur Stellungnahme gegeben, welche datenschutzrechtlichen Anforderungen dabei zu erfüllen sind.

Im ersten Schritt ist beabsichtigt, allgemeine Informationen über BAföG im Internet anzubieten. Der Abruf der Informationen soll nicht individuell protokolliert werden, um die Akzeptanz des Angebots feststellen zu können. Dies ist datenschutzrechtlich unbedenklich.

In einem späteren zweiten Schritt soll das BAföG-Antragsformular angeboten werden nebst einer dahinterliegenden Datenbank, in welche die beim Ausfüllen des Formulars anfallenden Informationen aufgenommen werden. Dabei wird sicherzustellen sein, daß andere Internet-Nutzer nicht auf das ausgefüllte Formular bzw. auf die dahinterliegende Datenbank zugreifen können. Im

übrigen darf - wie beim Abholen eines Formulars im Ausbildungsförderungsamt - auch hierbei nicht individuell protokolliert werden, wer von dem Angebot Gebrauch macht.

Als dritte Stufe ist letztlich beabsichtigt, die Antragsdaten aus dem Internet direkt in das BAföG-Verfahren zu übernehmen. Dabei ist eine Verschlüsselung vorgesehen; wir haben dazu Produkte benannt, mit denen eine ausreichende Sicherheit erreicht wird. Da BAföG-Anträge nach geltendem Recht unterzeichnet sein müssen, halten wir eine digitale Signatur für erforderlich.

3.7 Entwicklung neuer Standard zum Datenschutz bei Multimediadiensten

Bei global angebotenen Multimediadiensten, insbesondere bei solchen Diensten, die über das Internet angeboten werden, stoßen die einzelnen Staaten auf faktische Grenzen bei der Durchsetzung von Rechtsnormen; dies gilt auch für das Datenschutzrecht. Um so wichtiger ist es, daß Standards und Verhaltensregeln etabliert werden, durch die ein Mindestmaß an Transparenz der Datenverarbeitung und an Datenschutz durchgesetzt werden können.

3.7.1 Platform for Internet Content Selection (PICS)

Dieses System wurde zunächst für die Auswahl von Inhalten unter dem Gesichtspunkt des Jugendschutzes entwickelt. Damit steht ein System zur Verfügung, das auch eine datenschutzrechtliche Auswahl von Anbietern und von Internet-Inhalten ermöglicht. Die Verantwortung für die Auswahl liegt dabei primär beim Nutzer, der anhand eigener Kriterien entscheiden kann, ob auf ein Angebot zugegriffen werden kann. PICS unterstützt - durch entsprechende Filtereinstellungen - diese Auswahl.

Die Problematik von PICS besteht weniger in der Filtereinstellung, sondern in der Bewertung von Anbietern und Angeboten. Weder ist geklärt, welche Kriterien für ein datenschutzkonformes Angebot zugrunde gelegt werden können, noch gibt es bisher allgemein akzeptierte Instanzen, die die Bewertung ("Rating") durchführen.

3.7.2 Open Profiling Standard (OPS)

Mit diesem Standard, der von einer größeren Zahl amerikanischer Firmen und Organisationen propagiert wird, soll ein gemeinsames Format für die Speicherung und Übermittlung personenbezogener Informationen über die Nutzer von Multimediadiensten geschaffen werden.

Die Befürworter von OPS sprechen davon, daß auf diese Weise ein höheres Datenschutzniveau erreicht werden könne, da der Nutzer selbst entscheiden könne, ob und ggf. welche seiner personenbezogenen Daten er gegenüber dem Anbieter preisgeben wolle. Dies bedeutet gegenüber der weit verbreiteten Praxis einen Fortschritt, daß Anbieter unbemerkt vom Nutzer personenbezogene Daten aus dessen System "absaugen" oder durch verdeckte Datenübertragung sogenannte "Cookies" auf seinem System speichern, um dadurch mehr Erkenntnisse über sein Nutzungsverhalten zu gewinnen.

Das Grundübel, daß der Zugang zu bestimmten Informationsangeboten nur gewährt wird, wenn der Nutzer in unangemessenem Umfang persönliche Daten offenbart, wird jedoch durch OPS eher verschärft. OPS könnte allenfalls dann einen Fortschritt für den Datenschutz im Internet bedeuten, wenn die Vorgabe aus § 12 Abs. 3 Mediendienste-Staatsvertrag bzw. § 3 Abs. 3 TDDSG (vgl. 3.5) allgemein akzeptiert würde; danach dürfen Anbieter die Erbringung von Diensten nicht von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke

abhängig machen, wenn ein anderer Zugang zu diesem Dienst nicht oder in nicht zumutbarer Weise möglich ist.

Sowohl PICS als auch OPS versuchen angesichts einer ungesicherten internationalen Rechtslage, Datenschutzmechanismen technisch zu unterstützen. Aufgrund der dargestellten Probleme ist es jedoch nicht sehr wahrscheinlich, daß diese Systeme allein einen ausreichenden Datenschutz gewährleisten können. Es bedarf vielmehr angesichts der Expansion grenzüberschreitender Multimediadienste mehr denn je einer Festlegung rechtlicher und technischer Datenschutz-Mindeststandards auf internationaler Ebene, damit das informationelle Selbstbestimmungsrecht des Nutzers nicht auf dem internationalen Datenhighway unter die Räder kommt.

Deshalb ist die Ministererklärung auf der Europäischen Ministerkonferenz "Globale Informationsnetze" vom Juli 1997 zu begrüßen, wonach globale Datenschutzgrundsätze gemäß den Arbeiten der Europäischen Union, des Europarats, der OECD und der Vereinten Nationen für den Online-Bereich entwickelt werden sollen (Abschnitt Datenschutz, Nr. 50 der Ministererklärung).

3.8 Datenverarbeitung bei der Anmeldung für Online-Dienste

Ein in Hamburg ansässiger großer Online-Dienst ermöglicht Interessenten eine kostenlose Nutzung für einen bestimmten Zeitraum, indem er Computerzeitschriften Disketten oder CD-ROMs mit Zugangsprogrammen beifügt.

Durch zahlreiche Eingaben sind wir darauf aufmerksam geworden, daß die so angesprochenen Interessenten dieses Angebot wahrnehmen können, auch wenn sie nicht die eigene Identität preisgeben, sondern einen anderen Namen verwenden. Der Online-Dienst verzichtet auf eine Prüfung der Identität für diese Testphase und erwartet erst für die weitere Nutzung eine unterschriebene Bankeinzugsermächtigung, die den Interessenten unter der angegebenen Adresse zugesandt wird.

Durch dieses Verfahren ist nicht nur die Nutzung dieses Online-Dienstes schnell und unkompliziert möglich, auch der Mißbrauch wird dadurch sehr leicht gemacht. So wurden unter mißbräuchlicher Verwendung eines Namens pornographische Darstellungen versandt und als Urheberin eine Frau, die gar keinen Computer besitzt, angegeben. Zudem wurde auf diesem Wege ihre Privatanschrift weitergegeben, was erhebliche Belästigungen zur Folge hatte. In anderen Fällen stellten Benutzer bei Überprüfung ihrer Konten Abbuchungen durch diesen Online-Dienst fest, obwohl sie niemals eine schriftliche Einzugsermächtigung erteilt hatten und noch nicht einmal Kunden dieses Dienstes waren. Andere Bürger wurden durch Mahnungen belästigt, die auch nicht aufhörten, nachdem klargestellt war, daß hier offenbar falsche Namen für Anmeldungen benutzt worden waren.

Auch wenn aufgrund dieser Problematik der Online-Dienst die Zugangsmöglichkeiten während dieser Testphase teilweise einschränkt, bleiben Mißbrauchsrisiken bestehen: So können die Nutzer innerhalb von chat-rooms Profile ins Netz stellen, die nicht nur Angaben über Äußeres oder die Anschrift enthalten können, sondern in denen auch z. B. sexuelle Vorlieben geschildert werden können. Damit kann unter falschem Namen ein Betroffener diffamiert, verleumdet oder beleidigt werden. Ferner können auch unter der fiktiven Identität elektronische Briefe versandt werden.

Aber es geht auch anders. Wer Kunde eines Konkurrenten dieses Online-Dienstes werden will, bekommt seine Nutzungsberechtigung von Anfang an nur gegen persönliches Einschreiben.

Einzelne Probleme des Datenschutzes im öffentlichen Bereich

4. Parlamentsspezifischer Datenschutz

4.1 Gesetz über die Untersuchungsausschüsse der Hamburgischen Bürgerschaft

Das Urteil des Hamburgischen Verfassungsgerichts vom 19. Juli 1995 zur Aktenvorlage an den Parlamentarischen Untersuchungsausschuß "Hamburger Polizei" (vgl. 14. TB, 15.1.3) hat den hohen Stellenwert bereichsspezifischer Rechtsvorschriften über die Verarbeitung personenbezogener Daten durch das Parlament unterstrichen. Die Bürgerschaft hat diesen Handlungsbedarf im Rahmen der Verfassungs- und Parlamentsreform zumindest teilweise umgesetzt und am 27. August 1997 das Gesetz über die Untersuchungsausschüsse der Hamburgischen Bürgerschaft beschlossen.

Das Gesetz enthält differenzierte Regelungen über die Verschwiegenheitspflicht der Ausschußmitglieder und der zur Unterstützung des Ausschusses herangezogenen Personen. Den Untersuchungsausschüssen ist die Möglichkeit eröffnet, durch besondere Beschlüsse strafbewehrte Geheimhaltungspflichten z. B. für Zeugen, Sachverständige, Dolmetscher und Zuhörer in nichtöffentlicher Sitzung zu begründen. Gewährleistet ist insbesondere der Schutz von Privat-, Betriebs-, Geschäfts- und Erfindungsgeheimnissen. Die Vorschriften über Einsicht in Unterlagen des Ausschusses und Auskunft aus diesen Unterlagen stellen einen angemessenen Ausgleich zwischen dem Recht auf informationelle Selbstbestimmung und sonstigen Interessen sicher. Die im Gesetz vorgesehene Einsetzung von Unterausschüssen sollte auch dazu genutzt werden, Beweiserhebungen über datenschutzrechtlich besonders sensible Sachverhalte auf einen engeren Kreis von Abgeordneten zu begrenzen.

Natürliche Personen, über die der Untersuchungsausschuß in seinem Bericht eine wertende Äußerung abgeben will (Betroffene), und Zeugen werden vom Gesetz mit eigenen Verfahrensrechten, z. B. dem Recht auf Hinzuziehung eines Beistands, ausgestattet. Unter besonderen Voraussetzungen kommt sogar eine Entschädigung aus der Staatskasse wegen der Kosten des anwaltlichen Beistands in Betracht. Gesetzliche Zeugnisverweigerungsrechte, die im Strafprozeß zu beachten sind, gelten sinngemäß auch bei Vernehmungen durch Untersuchungsausschüsse. Wir konnten, auf der Grundlage einer von uns angeregten Verfassungsänderung, erreichen, daß eine entsprechende Klarstellung auch für das Zeugnisverweigerungsrecht der oder des Hamburgischen Datenschutzbeauftragten in das Gesetz aufgenommen wurde. Dies halten wir zum Schutz der Bürgerinnen und Bürger, die sich mit Eingaben an uns wenden und dabei häufig sensible Daten offenbaren, für wesentlich.

Das Gesetz über die Untersuchungsausschüsse der Hamburgischen Bürgerschaft stellt einen bedeutsamen Fortschritt auf dem Weg zu einem umfassenden parlamentsspezifischen Datenschutz dar. Wir treten allerdings dafür ein, gesetzliche Vorkehrungen zum Schutz personenbezogener Daten auch für andere Bereiche parlamentarischer Aufgabenerfüllung zu treffen, z. B. durch eine Datenschutzordnung der Hamburgischen Bürgerschaft. Dieses Anliegen konnte der Verfassungsausschuß in der vergangenen Wahlperiode nicht mehr abschließend beraten.

5. Umweltschutz

5.1 Ordnungswidrigkeitendatei bei der Umweltbehörde

Nachdem sich herausgestellt hatte, daß in der Umweltbehörde eine unzulässige Datei geführt wurde, reagierte die Behörde umgehend und löschte diese Datei vollständig und kurzfristig.

In der Datei wurden Angaben über die seit 1986 erfolgten Ordnungswidrigkeiten-Anzeigen und die Ergebnisse der durchgeführten Verfahren gespeichert. Zugriff auf diese Datei hatten alle Sachbearbeiter der Umweltbehörde, die mit der Bearbeitung von Ordnungswidrigkeiten betraut sind. Löschungsfristen für diese sensiblen Daten gab es nicht.

Nach § 5 Abs. 1 HmbDSG ist die Verarbeitung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine besondere Rechtsvorschrift über den Datenschutz sie erlaubt.

Die Umweltbehörde führte zunächst als Rechtsgrundlage § 17 des Ordnungswidrigkeitengesetzes (OWiG) an. Aus dieser Vorschrift läßt sich aber nicht eine generelle Zulässigkeit von automatisierten Dateien über Ordnungswidrigkeiten entnehmen. Nach der Kommentarliteratur zu § 17 OWiG ist es lediglich möglich, früher begangene Ordnungswidrigkeiten jeweils zum Nachteil Betroffener zu verwerten, soweit im Einzelfall in sachlicher und zeitlicher Hinsicht ein innerer Zusammenhang zu der neuen Ordnungswidrigkeit gegeben ist.

Die Datei war auch nicht gemäß § 13 Abs. 2 Nr. 5 HmbDSG zulässig. Dies wäre nur der Fall gewesen, wenn die Datenverarbeitung zur Verfolgung von Ordnungswidrigkeiten erforderlich gewesen wäre. Nach der Kommentarliteratur zu § 17 OWiG kann zwar bei zeitlichem und sachlichem Zusammenhang ein früheres Verfahren zum Nachteil des Betroffenen verwertet werden. Das bedeutet jedoch nur, daß diejenigen Ordnungswidrigkeiten-Sachbearbeiter, die einen bestimmten Bereich von Ordnungswidrigkeiten betreuen, die damit in Zusammenhang stehenden zeitlich früheren Verfahren berücksichtigen können. Auf diese Unterlagen können sie auch zugreifen, weil das Hamburgische Datenschutzgesetz gemäß § 2 Abs. 5 Nr. 3 insoweit auf die Verarbeitung personenbezogener Daten in Akten keine Anwendung findet.

In die Gesamtbewertung mußte auch die Vorschrift des § 149 Abs. 2 Nr. 3 der Gewerbeordnung (GewO) einbezogen werden. Diese Rechtsgrundlage ermöglicht es, die rechtskräftigen Bußgeldentscheidungen wegen einer Ordnungswidrigkeit, die mit einer Geldbuße von mehr als 200,- DM belegt worden ist, in das Gewerbezentralregister eintragen zu lassen. Es ist völlig ausreichend, bei der Verwertung früher begangener Ordnungswidrigkeiten des Betroffenen allein auf die Angaben des Gewerbezentralregisters beim Bundeszentralregister zurückzugreifen. Dies wird insbesondere dadurch belegt, daß nur Bußgelder einzumelden sind, die mehr als 200,- DM betragen. Daraus ergibt sich, daß lediglich Informationen über Ordnungswidrigkeiten von einigem Gewicht über längere Zeit für eine Verwendung zu Lasten der Betroffenen zur Verfügung stehen sollen.

Eintragungen in dieses Register werden gemäß § 153 Abs. 1 GewO nach Ablauf einer Frist von 3 bzw. 5 Jahren getilgt. Daran zeigt sich, daß der Gesetzgeber selbst bei diesen Ordnungswidrigkeiten eine längere Aufbewahrungszeit nicht für erforderlich hält.

6. Sozialwesen

6.1 Überregionale Zugriffsrechte in der Rentenversicherung

Im 14. TB (5.4) berichteten wir bereits kurz über dieses Thema und forderten eine Beschränkung des unzuständigen Zugriffs auf Versicherungskonten der Rentenversicherungsträger. Obwohl der Senat diese Auffassung in seiner Stellungnahme vom 28. Mai 1996 (Bürgerschaftsdrucksache 15/5554) teilte, entspricht das Verfahren dieser Forderung in seiner gegenwärtig realisierten Form jedoch nicht.

Es gibt für jeden Rentenversicherten ein Versicherungskonto, in dem wesentliche Eckdaten für seine spätere Rente gespeichert sind. Zu dem möglichen Inhalt eines Versicherungskontos gehören u. a.

- Kennzeichnungen als
  - Zugehöriger zur Personengruppe nach dem Transsexuellengesetz,
  - als Verfolgter des Nationalsozialismus,
- Angaben zu Zeiten verminderter Erwerbs- bzw. Berufsfähigkeit,
- Angaben über Rentenpfändungen,
- Freiheitsentziehungszeiten,
- Krankheitszeiten.

Es handelt sich also um teilweise hochsensible Daten, an denen auch Unbefugte (z. B. Versicherungsunternehmen) Interesse haben können, so daß von einem relevanten Mißbrauchsrisiko ausgegangen werden muß.

Für jedes Versicherungskonto ist ein einzelner Rentenversicherungsträger zuständig und verantwortlich. Dies ist allerdings nicht immer der Träger, der für den aktuellen Wohnsitz des Versicherten zuständig ist. Denn wenn ein Versicherter seinen Wohnsitz in den Bereich eines anderen Trägers verlegt, erhalten davon der zu dem Zeitpunkt zuständige Träger und der für den neuen Wohnsitz zuständige Träger nicht ohne weiteres Kenntnis.

Deshalb konnte es bislang geschehen, daß z. B. ein nach Hamburg gezogener Versicherter bei der LVA Hamburg keine sofortige Auskunft über die ihn betreffenden Daten erhalten konnte. Auch eine sofortige Beratung aufgrund dieser Datenlage war der LVA Hamburg dann nicht möglich. Vielmehr mußte erst mit einer gewissen Zeitverzögerung veranlaßt werden, daß im Versicherungskonto die neue Zuständigkeit der LVA Hamburg berücksichtigt wurde.

Um solche Verzögerungen zu vermeiden und den Versicherten mehr Service zu bieten, sind die Träger in einer schriftlichen Vereinbarung bundesweit fast vollständig übereingekommen, ein Verfahren einzuführen, bei dem jeder Träger nicht nur auf die Versicherungskonten zugreifen kann, für die er zuständig ist, sondern auch auf die Versicherungskonten anderer Träger, die an diesem Verfahren teilnehmen. Will der Sachbearbeiter eines unzuständigen Trägers auf ein Versicherungskonto zugreifen, benötigt er dafür nur den Namen und das Geburtsdatum des Versicherten; die Kenntnis der Rentenversicherungsnummer ist nicht nötig.

In der letzten Ausbaustufe dieses Verfahrens wird bundesweit voraussichtlich jeder Träger auf die Versicherungskonten aller Versicherten (ca. 50 Millionen) zugreifen können. Dieser Service kommt dann nicht nur den Versicherten zugute, bei denen bislang die oben beschriebenen Verzögerungen auftreten konnten. Betroffen sind dann auch alle anderen Versicherten, die diesen Service überhaupt nicht benötigen; ihre Daten sind unnötig einem erhöhten Mißbrauchsrisiko ausgesetzt. Bei der LVA Hamburg sind insgesamt etwa 300.000 Versicherte betroffen.

Der Zweck des Verfahrens liegt in der Befriedigung eines möglichen individuellen Serviceinteresses des jeweiligen Versicherten. Dafür muß die Aussage des Bundesverfassungsgerichts aus seinem Volkszählungsurteil berücksichtigt werden, daß der Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen hat. Ein überwiegendes Allgemeininteresse, das die mit dem Verfahren - zu Lasten des Datenschutzes - vorgenommene Erweiterung der Zugriffsmöglichkeit auf alle Versicherungskonten rechtfertigen könnte, besteht nicht. Nach § 78 a Sozialgesetzbuch/Zehntes Buch (SGB X) muß die LVA Hamburg u. a. verhindern, daß Datenträger unbefugt gelesen werden können (Datenträgerkontrolle) und daß von gespeicherten personenbezogenen Daten unbefugt

Kenntnis genommen wird (Speicherkontrolle). Die generelle Einrichtung des Verfahrens ohne Rücksicht auf den individuellen Willen des Versicherten erscheint daher rechtswidrig.

Das Verfahren dürfte nur für Versicherungskonten eingerichtet werden, wenn die betroffenen Versicherten zuvor eine Einwilligung dahingehend erklärt haben, daß sie damit einverstanden sind, wenn auf ihre Daten bundesweit zugegriffen werden kann. Dabei müßten die Versicherten natürlich auch über die Risiken dieses Verfahrens informiert werden. Wenigstens sollte den Versicherten aber ein Widerspruchsrecht gegen die weitgehenden Zugriffsmöglichkeiten eingeräumt werden (vgl. nachstehend 6.2.1). Die Folge einer nicht erteilten Einwilligung oder eines erklärten Widerspruchs müßte dann sein, daß die Zugriffsmöglichkeit auf das jeweilige Versicherungskonto für unzuständige Träger gesperrt wird. Technisch ist dies möglich.

Die beste Möglichkeit, entsprechende Erklärungen der Versicherten einzuholen, läge naturgemäß in einem gesonderten Anschreiben an die Versicherten. Dadurch für die LVA Hamburg entstehende Portokosten wären zwar erheblich, aber letztlich durch sie zu verantworten. Es gibt aber auch Alternativen, sich an die Versicherten zu wenden, z. B. im Rahmen der Öffentlichkeitsarbeit der Rentenversicherungsträger (und der Datenschutzbeauftragten), im übrigen auch anläßlich der erstmaligen Versendung der Rentenversicherungsnummer (§ 147 Abs. 3 Sozialgesetzbuch/Sechstes Buch (SGB VI)) und der regelmäßigen Versendung des Versicherungsverlaufs (§ 149 Abs. 3 SGB VI i. V. m. § 17 Zweite Datenerfassungs-Verordnung).

Unabhängig von einer solchen Einwilligungs- oder Widerspruchslösung ist die LVA Hamburg in jedem Fall verpflichtet, hinsichtlich der technischen und organisatorischen Maßnahmen verbindliche Festlegungen zu treffen, welche die unzuständigen Träger einzuhalten haben, wenn sie auf Versicherungskonten der LVA Hamburg zugreifen (vgl. § 79 Abs. 2 Satz 2 Nr. 4 SGB X; § 80 Abs. 2 Satz 2 SGB X).

Dieser Pflicht ist die LVA Hamburg bislang nur unzulänglich nachgekommen. Es fehlen insbesondere präzise Festlegungen bezüglich der

- Anzahl der das Dialogverfahren jeweils anwendenden Mitarbeiter,
- technischen Begrenzung der Zugriffsmöglichkeit auf diese zugelassenen Mitarbeiter,
- Prüfung der Identität der Antragsteller,
- Schriftlichkeit des Antrags eines Versicherten beim unzuständigen Träger,
- Protokollierungen der erfolgten Zugriffe bei den beteiligten Trägern,
- Speicherungsfrist für die überlassenen Sozialdaten,
- stichprobenartigen Kontrollen, daß für erfolgte Zugriffe ein Auftrag vorlag.

Erfolgte Zugriffe werden zwar im Versichertenkonto insoweit protokolliert, als der anfordernde Träger, der anfordernde Sachbearbeiter, das Datum der Anforderung und die angeforderten Daten vermerkt werden. Aus dem einzelnen Versicherungskonto ist ein Zugriff also erkennbar, sobald es eingesehen wird. Technisch möglich sind auch Auswertungen dieser Protokolle, aus denen sich alle Versicherungskonten ergeben, auf die in einem bestimmten Zeitraum zugegriffen wurde.

Diese Protokolle können aber allein nicht aufdecken, ob der Zugriff befugt oder unbefugt erfolgte. Denn wenn ein Träger zu Kontrollzwecken bei anderen Trägern anfragen würde, ob dort eine Vorsprache des Versicherten den Zugriff auf das Versicherungskonto erforderlich machte, wäre dies nur verläßlich nachvollziehbar, wenn dort die Vorsprache des Versicherten revisionssicher dokumentiert wird. Für eine solche revisionssichere Dokumentation wäre es erforderlich, daß die Identität des Versicherten überprüft wird und er dann durch eine schriftliche Erklärung den Anlaß für den Versicherungskontozugriff bestätigt.

Solche schriftlichen Erklärungen, die keinen nennenswerten Aufwand bedeuten würden, werden nach unserer Kenntnis zwar durch einzelne Träger (LVA Mecklenburg-Vorpommern, LVA Thüringen) eingeholt. Die LVA Hamburg hat jedoch nicht als organisatorische Maßnahme festgelegt, daß die auf ihre Versicherungskonten zugreifenden Träger solche Einwilligungen einholen (s. o.). Sie hat auch bislang keinerlei Kontrollen dahingehend vorgenommen, ob unzuständige Zugriffe auf ihre Versicherungskonten befugt waren.

Insgesamt sind die Rentenversicherungsträger mit diesem Verfahren weit übers Ziel hinausgeschossen. Wir haben die LVA Hamburg zur Mitteilung aufgefordert, was sie zur Abstellung der beschriebenen Mängel unternimmt. Sie hat uns dazu mitgeteilt, ihre Auskunfts- und Beratungsstelle werde sich künftig von den Versicherten schriftlich bestätigen lassen, daß ihre Daten bei einem anderen Rentenversicherungsträger angefordert werden dürfen. Wegen weiterer Änderungen des Verfahrens will sie an den Verband Deutscher Rentenversicherungsträger herantreten, da ein abgestimmtes Vorgehen aller am Verfahren Beteiligten sinnvoll sei.

6.2 Gesetzliche Krankenversicherung

6.2.1 Geschäftsstellenübergreifende Zugriffsrechte bei der AOK Hamburg

Wie bereits mehrfach berichtet, ermöglicht die AOK Hamburg (wie auch andere Krankenkassen, die aber nicht unserer Kontrolle unterliegen) allen ihren Geschäftsstellen den Zugriff auf Versichertendaten, und zwar ohne Rücksicht darauf, ob die Versicherten damit einverstanden sind. Darin liegt ein Verstoß gegen § 35 Abs. 1 Satz 2 Sozialgesetzbuch/Erstes Buch und § 78 a Sozialgesetzbuch/Zehntes Buch (vgl. ausführlich 13. TB, 6.4 sowie 14. TB, 5.3 und 15. TB, 19.1.1). In ihrer Sitzung am 20./21. August 1997 hat die Bürgerschaft den Senat ersucht, "gegenüber der AOK Hamburg durch geeignete Maßnahmen darauf hinzuwirken, im Rahmen der technischen Möglichkeiten den Versicherten die Wahl einer oder mehrerer für sie zuständiger Geschäftsstellen zu überlassen und damit die anderen Geschäftsstellen vom Datenzugriff auszuschließen".

In Gesprächen mit der Behörde für Arbeit, Gesundheit und Soziales als Aufsichtsbehörde und der AOK Hamburg konnten wir inzwischen Fortschritte erreichen. Die AOK will beim AOK-Bundesverband darauf hinwirken, daß bei der Überarbeitung des EDV-Systems "IDVS II" die Möglichkeit geschaffen wird, für einzelne Geschäftsstellen den Zugriff auf die Versichertendaten zu sperren.

Nach Vorliegen dieser technischen Voraussetzungen (voraussichtlich im Laufe des Jahres 1998) will die AOK Hamburg in ihrer Mitgliederzeitschrift den Versicherten die verschiedenen Möglichkeiten darstellen, unter den Geschäftsstellen auszuwählen. Die Versicherten, die weiterhin einen Datenzugriff durch alle Geschäftsstellen erlauben wollen, müssen dann nichts veranlassen. Will jedoch ein Versicherter die Zugriffsmöglichkeit seitens bestimmter Geschäftsstellen ausschließen und damit den Schutz seiner Daten verbessern, muß er dies der AOK mitteilen. Der Zugriff wird dann nur durch die von ihm ausgewählten Geschäftsstellen möglich sein. Bei neuen Versicherten wird die AOK gleich zu Beginn des Versicherungsverhältnisses klären, durch welche Geschäftsstellen diese betreut werden wollen; sie werden dann eine entsprechende Einwilligung erklären können.

6.2.2 Vergabe der Abrechnungsprüfung durch Krankenkassen an private Stellen

Im Berichtszeitraum haben uns weiterhin die Tendenzen der gesetzlichen Krankenkassen beschäftigt, die Prüfung von Abrechnungen auf private Dienstleister zu verlagern, und zwar im

Falle der Betriebskrankenkasse (BKK) der Freien und Hansestadt (vgl. 15. TB, 6.3) und der BKK Blohm & Voß AG.

Beide Kassen hatten sich lange Zeit darauf beschränkt, ihrem Dienstleister vertraglich nur allgemein die Einhaltung der datenschutzrechtlichen Bestimmungen aufzuerlegen, ohne dafür hinreichend konkrete Vorgaben zu machen. Die Auftragsverhältnisse waren der Behörde für Arbeit, Gesundheit und Soziales als Aufsichtsbehörde von den Kassen zwar angezeigt worden; diese hatte die Mängel aber nicht beanstandet.

Als Auftraggeber sind die Kassen aber nach § 80 Sozialgesetzbuch/Zehntes Buch (SGB X) verpflichtet, in einer schriftlichen Vereinbarung mit dem Auftragnehmer möglichst konkret zu regeln, welche Maßnahmen bzgl. der Realisierung des Datenschutzes dieser zu treffen hat.

Unsere Diskussion mit den Kassen machte deutlich, daß ihnen das Bewußtsein dafür fehlte, daß sie für die Ordnungsmäßigkeit der Datenverarbeitung und
-nutzung auch dann verantwortlich bleiben, wenn sie sich eines Auftragnehmers gemäß § 80 SGB X bedienen. Sie vertrauten allzu leicht darauf, daß sich ihr Auftragnehmer rechtskonform verhält, und vernachlässigten ihre Pflicht, dies auch vertraglich zu sichern. Bezeichnenderweise waren es denn auch nicht die Kassen selbst, die auf unsere Intervention hin die Verträge nachbesserten. Vielmehr wandten sich die Auftragnehmer an uns, um eine rechtskonforme Ausgestaltung der Verträge zu erreichen. Dies ist inzwischen im Falle der BKK Blohm & Voß AG in ausreichender Weise gelungen.

6.2.3 Auflösung der Betriebskrankenkasse (BKK) Hamburg-Süd

Zur Klärung des Verbleibs der Versichertendaten der aufgelösten BKK Hamburg-Süd (vgl. 15. TB, 6.1) hat der Auflösungsvorstand vorgeschlagen, die weiterhin aufbewahrungspflichtigen Versichertendaten beim BKK-Landesverband NORD (LV) zu speichern bzw. aufzubewahren. Dieser Vorschlag entspricht dem Ansatz, den wir bereits im 15. TB (a.a.O.) gewählt haben.

Hinsichtlich der automatisiert gespeicherten Daten würde damit an die bereits bestehenden tatsächlichen Verhältnisse (Auftragsdatenverarbeitung durch den LV) angeknüpft werden. Hinsichtlich der Versichertenkarten und anderer Papierunterlagen (Rechnungen u. a.) haben wir dem LV empfohlen, diese in verschlossener Form aufzubewahren, um eine unbefugte Kenntnisnahme - auch innerhalb des LV - zu verhindern.

Zudem sollte der LV die früheren Versicherten der BKK Hamburg-Süd über den Verbleib der sie betreffenden Daten informieren. Für den Fall, daß Daten oder Unterlagen durch eine Krankenkasse beim LV angefordert werden sollten, müßten die Betroffenen auch über ihr Widerspruchsrecht nach § 76 Sozialgesetzbuch/Zehntes Buch hingewiesen werden.

6.3 Projekt Sozialhilfe-Automation (PROSA)

6.3.1 Datenschutzkonzeption

Das Senatsamt für Bezirksangelegenheiten (SfB) hat die Datenschutzkonzeption für das automatisierte Sozialhilfeverfahren PROSA (vgl. 9. TB, 4.1.1) unter unserer engen Beteiligung fortgeschrieben und den inzwischen eingetretenen Änderungen im Verfahren angepaßt.

Die Neufassung, die jetzt "Datenschutzregelungen im Dialogverfahren Sozialhilfe (PROSA) - DR-PROSA -" heißt, ist in stärkerem Maße als bislang auf die Beschreibung der Maßnahmen

ausgerichtet, mit denen die gesetzlichen Vorgaben des Datenschutzrechts umgesetzt werden. Insgesamt ist damit eine Dokumentation entstanden, mit Hilfe derer auch Nicht-Kenner des Verfahrens einen recht guten Eindruck vom Datenschutz im PROSA-Verfahren erhalten können. Wir haben dem SfB daher empfohlen, die DR-PROSA im Rahmen der nächsten Berichtsdrucksache auch der Bürgerschaft zur Kenntnis zu geben.

6.3.2 Zugriffsrechte

Ein gegenwärtig noch unbefriedigend gelöster Punkt ist der Umfang der internen Zugriffsbefugnisse. Von Ausnahmen abgesehen darf jeder Mitarbeiter einer Sozialhilfedienststelle auf die Datensätze aller Hilfeempfänger dieser Dienststelle zugreifen; dies sind bei größeren Dienststellen mehrere Dutzend Mitarbeiter. Nach § 35 Abs.1 Satz 2 Sozialgesetzbuch/Erstes Buch dürfen innerhalb einer speichernden Stelle aber nur diejenigen Personen Zugriff auf Daten haben, die diese für ihre Aufgabenerfüllung benötigen.

Das SfB will dies bei der Weiterentwicklung des Verfahrens berücksichtigen. Gedacht ist daran, die Zugriffsmöglichkeit auf die jeweilige Abteilung (bis zu
8 Personen) innerhalb einer Dienststelle zu beschränken. Damit würde einerseits der Notwendigkeit Rechnung getragen, innerhalb der Abteilung Vertretungen oder auch rotierende Zuständigkeiten zu organisieren. Andererseits wäre datenschutzrechtlich eine wesentliche Verbesserung erreicht. Zugleich könnte die Protokollierung lesender Zugriffe aufgegeben werden, wodurch das Verfahren erheblich entlastet würde.

6.3.3 Mangelhafte Sachstandsausdrucke bei Auskunftserteilung

Durch eine Eingabe wurden wir am Jahresanfang auf einen Fehler im PROSA-Verfahren aufmerksam, der bei dem Betroffenen für erhebliche Irritationen sorgte. Er hatte nämlich das Sozialamt Eimsbüttel um Auskunft darüber gebeten, welche ihn betreffenden Daten im Verfahren gespeichert waren. Das Sozialamt hatte daraufhin automatisiert einen sogenannten Sachstandsausdruck anfertigen lassen und dem Betroffenen übersandt.

Dieser Sachstandsausdruck enthielt Angaben, die offensichtlich unzutreffend waren. So war als Zahlungsempfänger ein dem Petenten völlig unbekannter türkischer Bürger angegeben und die Sparkassenfiliale, bei der das Konto geführt sein sollte, war gar nicht existent.

Nachdem das Sozialamt auf den Fehler hingewiesen worden war, wurde dem Betroffenen nicht etwa eine berichtigte Auskunft erteilt. Er wurde vielmehr mehrere Monate mit der Begründung hingehalten, daß die Behebung des Computerfehlers noch nicht erfolgt sei.

Der technische Fehler allein, so ärgerlich er für alle Beteiligten auch war, konnte dieses Verhalten des Sozialamts nicht rechtfertigen. Zum einen hätte der Sachstandsausdruck vor seinem Versand wenigstens kursorisch auf Richtigkeit und Vollständigkeit überprüft werden müssen. Zum anderen läßt sich ein Auskunftsanspruch auch erfüllen, wenn die Funktion des Sachstandsausdruckes defekt ist; ein evtl. höherer Arbeitsaufwand muß dann akzeptiert werden. Das Leistungsvermögen der modernen Datenverarbeitungstechnik sollte nicht dazu führen, sich bedingungslos von ihr abhängig zu machen.

6.4 Kinder- und Jugendhilfe

6.4.1 Projekt Jugendamts-Automation (PROJUGA)

Im Februar haben wir im Bezirksamt Altona das automatisierte Jugendhilfeverfahren PROJUGA (vgl. 11. TB, 6.3) geprüft. Im wesentlichen interessierte uns dabei der Umfang der Zugriffsberechtigungen. Auf unsere im Mai unterbreiteten Änderungsvorschläge haben wir bis zum Redaktionsschluß keine Reaktion erhalten.

- Aufgabenbezogene Rechtevergabe

  Gegenwärtig ist es so, daß die Benutzer im Verfahren bestimmte "Rollen" einnehmen. Mit jeder Rolle sind bestimmte Zugriffsrechte verbunden. Die Rollen werden von den Abteilungsleitern eingerichtet. Allerdings kann ein Abteilungsleiter Rollen nicht nur für seine eigene Abteilung einrichten, sondern auch für fremde Abteilungen. Z. B. kann die Abteilungsleitung "Wirtschaftliche Hilfen" für einen ihrer Mitarbeiter auch die Rolle eines Amtspflegers einrichten. Zur besseren Gewährleistung der Organisationskontrolle sollte künftig sichergestellt werden, daß Rechte nur bezogen auf die Aufgaben der Abteilung vergeben werden können, nicht jedoch abteilungsübergreifend.

- Interne Nutzungsbeschränkungen

  Innerhalb eines Jugendamtes kann ein Benutzer im Rahmen der Zugriffsrechte, die mit seiner Rolle verbunden sind, auf alle Einzelfälle zugreifen; er wird ggf. auf seine Unzuständigkeit für einen Fall hingewiesen. Das halten wir für vertretbar, weil es sich einerseits nur um wenige Benutzer handelt und es andererseits die Arbeitsorganisation erheblich erleichtert; zudem wird der Zugriff protokolliert.

  Allerdings werden dem Benutzer bereits nach Eingabe des Vor- und des Nachnamens von allen Hamburger Jugendämtern die Fälle angezeigt, die denselben Vor- und Nachnamen aufweisen. Damit soll vermieden werden, daß ein bereits vorhandener Fall erneut angelegt wird (Doppelfallkontrolle). Die angezeigten Fallinformationen bestehen aus dem Geburtsdatum, dem zuständigen Jugendamt, den vergebenen Rollen sowie den zu diesen Rollen gehörigen Benutzern (mit Namen und Telefonnummer).

  Aufgrund von § 35 Abs.1 Satz 2 Sozialgesetzbuch/Erstes Buch, der eine strikte interne Nutzungsbeschränkung vorschreibt, halten wir die beschriebene Doppelfallkontrolle für verbesserungsbedürftig. Denn bei ihr werden auch Fälle angezeigt, die - bei abweichendem Geburtsdatum - gar kein Doppelfall sein können. Der Fallaufruf und ggf. die Anzeige eines entsprechenden Doppelfalles sollte daher nur möglich sein, wenn sowohl der Name als auch das Geburtsdatum eingegeben wurden.

- Programmzugriffe

  Falldaten werden regelmäßig nur eingegeben und verarbeitet, wenn sich die Benutzer beim PROJUGA-Verfahren angemeldet haben; nur dann kann auf die zentral vorgehaltenen Daten zugegriffen werden, sowie auf Briefe und Vermerke, die mit einer lokalen Textverarbeitung erstellt und zentral abgespeichert werden. Dabei werden die rollenbezogenen Zugriffsbeschränkungen der Benutzer berücksichtigt. Dies ist datenschutzrechtlich unbedenklich.

  Im Einzelfall fließen aber auch Falldaten in die Textverarbeitung außerhalb der PROJUGA-Anwendung ein, um z. B. Vordrucke benutzen zu können, die nicht zentral zur Verfügung gestellt werden. Die entstehenden Textdokumente können auf Festplatte oder Diskette gespeichert werden; dabei ist den Benutzern eine umfangreiche Makroprogrammierung

möglich. Die damit verbundene Ausführung beliebiger Programme sowie der Zugriff auf die DOS-Shell sind datenschutzrechtlich nicht vertretbar. Daher sollten Falldaten ausschließlich über das PROJUGA-Verfahren verarbeitet werden, nicht jedoch in der lokalen Textverarbeitung. Der Erforderlichkeit einer lokalen Erfassung von Falldaten sollte durch die zentrale Bereitstellung geeigneter Vordrucke begegnet werden.

- Protokollierung von Zugriffen

  Innerhalb eines Jugendamtes werden die Zugriffe jedes Benutzers protokolliert. Soweit sie durch unzuständige Benutzer erfolgten, kann das System sie später dem zuständigen Benutzer zwar anzeigen. Diese Anzeigefunktion ist jedoch abschaltbar. Um die Kontrolle unzuständiger Zugriffe zu stärken, sollten sie dem zuständigen Benutzer generell angezeigt werden, indem auf die Möglichkeit verzichtet wird, diese Funktion auszuschalten.

6.4.2 Sicherstellung des Datenschutzes bei Freien Trägern

Mit der Behörde für Schule, Jugend und Berufsbildung (BSJB) sind wir in der Diskussion darüber, wie bei freien Trägern der Jugendhilfe ein Datenschutz sichergestellt werden kann, der dem Datenschutz bei öffentlichen Trägern der Jugendhilfe entspricht. Hintergrund dieser Diskussion ist § 61 Abs. 4 Sozialgesetzbuch/Achtes Buch (SGB VIII), der die öffentlichen Jugendhilfeträger zu einer solchen Sicherstellung verpflichtet.

Ein öffentlicher Träger kann faktisch nur begrenzt auf den Datenschutz bei freien Trägern einwirken. Er sollte aber zumindest darauf hinarbeiten, daß z. B. in Pflegesatzvereinbarungen und Zuwendungsbescheiden das Ziel konkretisiert wird, welches die freien Träger erreichen sollen.

Das Bundesverfassungsgericht hat in einer Entscheidung vom 25. März 1992 befunden, daß die Ermächtigung, Datenschutzvorschriften zu erlassen, nicht die Ermächtigung zum Erlaß von Datenerhebungsvorschriften beinhaltet. Übertragen auf § 61 Abs. 4 SGB VIII bedeutet diese Sichtweise, daß den freien Trägern nicht etwa Befugnisse zur Datenerhebung, -verarbeitung und -nutzung eingeräumt werden dürfen, sondern das Augenmerk speziell auf den Schutz der Daten bei der Datenerhebung, -verarbeitung und -nutzung zu richten ist.

In diesem Sinne kommen vor allem folgende Anforderungen in Betracht, auf deren Einhaltung der öffentliche Träger drängen sollte:
- Zweckbindung (§ 64 Abs. 1 SGB VIII),
- Zusammenführungsverbot (§ 63 Abs. 2 SGB VIII),
- interne Nutzungsbeschränkung (§ 35 Abs. 1 Satz 2 SGB I),
- persönliche Verschwiegenheitspflichten (§ 65 Abs. 1 Satz 1 SGB VIII),
- technische und organisatorische Maßnahmen (§ 78 a SGB X),
- Berichtigung, Sperrung und Löschung (§ 84 SGB X).

Mit freien Trägern sollte daher vereinbart werden, daß sie einen den Bestimmungen des SGB VIII entsprechenden Datenschutz gewährleisten und insbesondere die vorgenannten Anforderungen erfüllen, wobei diese teilweise noch konkretisierungsbedürftig sind. Um die Gewährleistungspflicht des öffentlichen Trägers nicht nur in Form von Regelungen zu erfüllen, kommt ergänzend in Betracht, den freien Trägern eine Berichtspflicht hinsichtlich ihrer Umsetzung der Anforderungen aufzuerlegen oder auch dem öffentlichen Träger ein diesbezügliches Prüfungsrecht auszubedingen.

Die BSJB ist in diesem Sinne an die Arbeitsgemeinschaft der Freien Wohlfahrtspflege herangetreten.

6.4.3 Neuorganisation der Jugendhilfe

Im Berichtszeitraum erhielten wir Informationen über das Projekt "Neuorganisation der bezirklichen Jugendämter", das im Mai 1995 eingesetzt wurde und am 1. April 1996 beginnen sollte. Eines der Projektziele sollte die Entspezialisierung und die Bündelung von Hilfen sein.

Der Bericht der Projektgruppe zur Neuorganisation der bezirklichen Jugendämter und der Abschlußbericht einer externen Unternehmensberatung lassen erkennen, daß auch datenschutzrechtliche Überlegungen in das Projekt eingeflossen sind. So ist u. a. die von uns seit längerem geforderte Trennung zwischen den Aufgaben der Amtsvormünder und -pfleger als gesetzliche Vertreter einerseits und anderen Aufgaben wie die Gewährung von Unterhaltsvorschuß oder die Bewilligung von Hilfen zur Erziehung (vgl. 12. TB, 6.3.3) andererseits vorgesehen. Auch die Notwendigkeit, Vertretungsregelungen einzuschränken und damit eine Begrenzung des Personenkreises vorzunehmen, welchem Informationen über dieselben Betroffenen zugänglich sind, ist in die Projektarbeit eingeflossen.

Anlaß zu unserer Befassung mit dem Projekt waren divergierende Auffassungen der Projektbeteiligten zur Erziehungsberatung (EB) nach § 28 Sozialgesetzbuch/Achtes Buch. Sie ist als eigene Organisationseinheit ausgestaltet und soll dies auch bleiben. Strittig war die Frage, ob der Durchführung der EB ein förmliches Bewilligungsverfahren voranzugehen hat und ob dieses von einer anderen Stelle im Jugendamt (den Allgemeinen Sozialen Diensten) durchgeführt werden darf.

Der Umstand, daß die EB als niedrigschwelliges Angebot ausgestaltet sein soll, spricht gegen die Durchführung eines außerhalb der Erziehungsberatungsstelle angesiedelten Bewilligungsverfahrens. Auch der Umstand, daß unseres Wissens in anderen Ländern kein Bewilligungsverfahren durchgeführt wird, ist ein Hinweis darauf, daß dessen Durchführung nicht zwingend ist.

Datenschutzrechtlich ist bedeutsam, daß die Zusammenführung von Daten stark eingeschränkt ist, die im Zusammenhang mit verschiedenen Aufgaben der Jugendhilfe erhoben worden sind. Diese Anforderungen müssen auch in die organisatorischen Bedingungen einfließen, unter denen im Jugendamt und somit auch in der EB gearbeitet wird. Die Erfüllung dieser Anforderungen würde begünstigt werden, wenn kein Bewilligungsverfahren außerhalb der Erziehungsberatungsstelle durchgeführt würde, denn im Bewilligungsverfahren fallen Daten zusätzlich zu denen an, die bei der Leistungsgewährung anfallen. Mit der Vorhaltung dieser Daten bei den Allgemeinen Sozialen Diensten würde zudem die Grundvoraussetzung geschaffen werden, sie dort auch mit anderen Daten zusammenzuführen und zweckdurchbrechend zu nutzen; dies sollte nach Möglichkeit vermieden werden.

Diese Überlegungen verdeutlichen im übrigen, daß das Projektziel einer Bündelung von Hilfen mit den gesetzlichen Anforderungen des Datenschutzes in einem latenten Zielkonflikt steht, der behutsam gelöst werden muß. Nach unseren Eindrücken von der bisherigen Projektarbeit kann dies aber durchaus gelingen.

6.5 Übermittlungen der Sozialleistungsträger an Finanzämter

Die Behörde für Arbeit, Gesundheit und Soziales (BAGS) bat uns um Stellungnahme, ob das Versorgungamt als Sozialleistungsträger befugt ist, dem Finanzamt die Honorare mitzuteilen, die

an beauftragte externe Ärzte für gutachterliche Tätigkeit gezahlt werden. Die BAGS fürchtet, daß solche Mitteilungen gegen das Sozialgeheimnis verstoßen könnten.

Die Finanzverwaltung hat ein Interesse an der Kenntnis dieser Zahlungen, um feststellen zu können, ob diese ordnungsgemäß versteuert wurden. Nach ihrer Auffassung müssen ihr solche Zahlungen mitgeteilt werden. Sie stützt sich dabei auf die Mitteilungsverordnung (MV) vom 7. September 1993, die die Bundesregierung aufgrund von § 93 a der Abgabenordnung (AO) erlassen hat. Die MV verpflichtet die Behörden (also auch Sozialleistungsträger), Zahlungen für Leistungen dem Finanzamt mitzuteilen. Aus der Begründung zur Mitteilungsverordnung ergibt sich, daß dazu auch "Honorarzahlungen, die von Sozialbehörden erbracht werden", gehören sollen.

Diese Mitteilungspflicht nach der MV greift jedoch dann nicht, wenn es sich bei den mitzuteilenden Angaben um Sozialdaten im Sinne des Sozialgesetzbuches (SGB) handelt. Denn für Sozialdaten sind Übermittlungsbefugnisse abschließend im SGB geregelt und das SGB erlaubt die genannten Mitteilungen nicht. Diese vom Bundestag als Gesetzgeber im SGB kodifizierten Vorstellungen können nicht von der Bundesregierung mit einer Rechtsverordnung nach der Abgabenordnung geändert werden.

Es kommt daher darauf an, ob man den Begriff Sozialdaten weit (so daß die Honorarzahlungen dazugehören) oder eng versteht (so daß sie nicht dazugehören). Dieses Begriffsverständnis läßt sich aber nicht mit Blick auf das im Einzelfall gewünschte Ergebnis klären. Vielmehr erfordert es die dem Bürger zustehende Rechtssicherheit, eine allgemeingültige Abgrenzung vorzunehmen. Daher hat diese Problematik eine grundsätzliche Bedeutung für alle Sozialleistungsbereiche.

Sozialdaten sind nach § 67 Abs. 1 Satz 1 SGB X personenbezogene Daten, die von einem Sozialleistungsträger im Hinblick auf seine Aufgaben nach dem SGB erhoben, verarbeitet oder genutzt werden. Wesentlich ist also, ob die Daten einen fachlichen Bezug zu den Aufgaben des Sozialleistungsträgers aufweisen oder nicht. Dies läßt sich - wie im Kommentar der Bundesversicherungsanstalt für Angestellte (BfA) zum SGB X vorgeschlagen - am besten anhand eines abstrakten Denkmodells feststellen: Gäbe es die Daten beim Sozialleistungsträger, wenn er zwar vorhanden wäre, aber keine Sozialleistungsaufgabe zu erfüllen hätte?

Nach einer solchen Prüfung besteht zwar kein fachlicher Bezug hinsichtlich der Angaben zu Mitarbeitern eines Sozialleistungsträgers (wie z. B. zum Gehalt), so daß diese Daten nicht dem Sozialdatenschutz unterliegen. Der fachliche Bezug besteht jedoch hinsichtlich der auf Honorarbasis arbeitenden externen Gutachter, denn ihre Honorare werden nur gezahlt, wenn der Leistungsträger im Hinblick auf seine gesetzliche Aufgabe nach dem SGB einen Gutachtenauftrag erteilt; externe Gutachter sind auch gerade keine Mitarbeiter des Leistungsträgers.

Im Ergebnis sind daher Daten von externen Gutachtern (wie Personalien, Konten, Honorare) Sozialdaten und dürfen nicht an das Finanzamt übermittelt werden. Daran ändert auch der Umstand nichts, daß fiskalische Daten bzw. Daten im Zusammenhang mit fiskalischen Hilfsgeschäften der Sozialverwaltung nicht unter den Sozialdatenschutz fallen sollen. Denn die fraglichen Honorarzahlungen haben eben nicht nur einen fiskalischen, sondern auch einen fachlichen Bezug. Dieses Ergebnis mag für die Finanzverwaltung unbefriedigend sein. Eine Beantwortung der strittigen Frage im Sinne der Finanzverwaltung würde aber eine entsprechende Änderung des SGB voraussetzen.

6.6 Dokumentation in der Pflege (DiP) bei pflegen & wohnen

Die Senatsstellungnahme zu Ziffer 6.3 unseres 15. Tätigkeitsberichts erweckt den Eindruck, alle Fragen zu DiP seien einvernehmlich geklärt worden.
Richtig ist hingegen, daß das Projekt ohne Abstimmung mit uns in Echtbetrieb genommen worden war. Die Klärung datenschutzrechtlicher Fragen mit pflegen & wohnen dauert noch an.

7. Personalwesen

7.1 Mitarbeiterbefragungen

Über den Datenschutz bei Mitarbeiterbefragungen haben wir bereits mehrfach berichtet (vgl. ausführlich 13. TB, 7.6.2 und 7.6.3; 14. TB, 6.2 und 15. TB, 7.3). Mit dem Personalamt und der Finanzbehörde haben wir nunmehr einen Konsens über den Entwurf einer Arbeitshilfe "Empfehlungen zum Datenschutz bei Mitarbeiterbefragungen" erreicht.

Die Arbeitshilfe gibt datenschutzrechtliche Hinweise, wenn Mitarbeiterinnen und Mitarbeiter in standardisierter Form durch Fragebögen oder Interviews nach Meinungen, Werturteilen, Einschätzungen oder Verbesserungsvorschlägen befragt werden. In der Regel wird diese Arbeitshilfe im Vorfeld von Maßnahmen im Bereich der Personal- und Organisationsentwicklung benötigt werden.

Nicht erfaßt sind Personalfragebögen, bei denen es gezielt um die Tätigkeit der einzelnen Mitarbeiterin oder des einzelnen Mitarbeiters geht; dafür gelten § 28 Hamburgisches Datenschutzgesetz (HmbDSG) und § 96 Hamburgisches Beamtengesetz (HmbBG). Auch Fragen nach der Art und Weise der Aufgabenerfüllung, die durch § 8 Bundes-Angestelltentarifvertrag bzw. §§ 57 ff. HmbBG i. V. m. § 28 HmbDSG legitimiert sind, werden von der Arbeitshilfe nicht erfaßt. Entscheidend für die Zuordnung zu diesen Normen ist jeweils die Einzelfallprüfung.

Das Personalamt wird die Arbeitshilfe "Empfehlungen zum Datenschutz bei Mitarbeiterbefragungen" den fachlich zuständigen Stellen zuleiten. Außerdem ist die Arbeitshilfe beim Hamburgischen Datenschutzbeauftragten erhältlich.

7.2 Sonstiges

- Bei dem Projekt Personalwesen (PROPERS) soll das Personalcontrolling entwickelt werden. Aus datenschutzrechtlicher Sicht kommt es dabei darauf an, die Kostenstellen so zu gestalten, daß sie regelmäßig mindestens drei Personen umfassen und auch sonst keinen Rückschluß auf individuelles Verhalten und persönliche Merkmale ermöglichen.

- Im Zusammenhang mit der Budgetierung der Personalkosten waren übergangsweise die tatsächlich gezahlten Bezüge zwischen den Fachbehörden und der Finanzbehörde personenbezogen abgeglichen worden. Wir haben gefordert, daß diese Verfahrensweise durch das anonymisierte Personalcontrollingverfahren im Rahmen von PROPERS abgelöst wird. Die Lenkungsgruppe hat diese Forderung zustimmend zur Kenntnis genommen. Das Personalamt arbeitet an der Umsetzung.

8. Finanzen und Steuern

8.1 Datenübermittlung der Finanzämter an die Handelskammer für die Erhebung von Mitgliedsbeiträgen

Auch in diesem Berichtsjahr erhielten wir wieder sehr viele Anfragen und Eingaben zur Beitragserhebung der Handelskammer. Die Übermittlung von Steuerdaten durch die Finanzämter an die Handelskammer stieß bei den Betroffenen vielfach auf Unverständnis.

§ 2 des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern (IHK-G) sieht vor, daß alle zur Gewerbesteuer veranlagten natürlichen Personen zur Industrie- und Handeskammer gehören, in deren Bezirk sie entweder eine gewerbliche Niederlassung oder eine Betriebsstätte oder eine Verkaufsstelle unterhalten. Gemäß § 3 IHK-G ist die Industrie- und Handelskammer eine Körperschaft öffentlichen Rechts. Die Kosten ihrer Errichtung und Tätigkeit werden durch Pflichtbeiträge der Kammerzugehörigen gemäß einer Beitragsordnung aufgebracht. Diese Beiträge sind öffentliche Abgaben und werden als Grundbeiträge und Umlagen erhoben.

Bemessungsgrundlage ist der Gewerbeertrag nach dem Gewerbesteuergesetz oder der nach dem Einkommen- und Körperschaftsteuergesetz ermittelte Gewinn aus dem Gewerbebetrieb. Die Beitragsveranlagung muß durch schriftlichen Bescheid erfolgen. In diesem ist auch auf die für die Beitragserhebung maßgeblichen Rechtsvorschriften hinzuweisen.

Jeder Kammerzugehörige ist gemäß § 3 Abs. 3 IHK-G verpflichtet, der Handelskammer Auskunft über die zur Festsetzung des Beitrags erforderlichen Grundlagen zu geben, soweit die Kammer diese Angaben nicht bereits direkt bei den Finanzbehörden erhoben hat. Dazu ist die Kammer gemäß § 9 Abs. 2 IHK-G berechtigt. Die Kammer muß sich zur Feststellung der Bemessungsgrundlagen also nicht an die Betroffenen selbst wenden. Die Finanzbehörden ihrerseits sind zudem gemäß § 31 Abs. 1 Abgabenordnung berechtigt, Besteuerungsgrundlagen, Steuermeßbeträge und Steuerbeträge an Körperschaften des öffentlichen Rechts wie die Handelskammern mitzuteilen, sofern auf diesen Daten die Festsetzung von Abgaben beruht.

Bei dem Datenaustausch zwischen den Finanzämtern und der Handelskammer liegt demnach weder ein Verstoß gegen das Steuergeheimnis noch gegen allgemeines Datenschutzrecht vor. Die Kritik der Betroffenen richtet sich in erster Linie auch nicht gegen das Datenschutzrecht, sondern gegen die Pflichtmitgliedschaft in den Kammern bzw. deren Finanzierung durch Pflichtbeiträge. Bundesweit formieren sich deshalb auch bereits Gewerbetreibende zu größeren Interessensvertretungen und führen vor den Verwaltungsgerichten Musterprozesse.

8.2 Sonstiges

Unsere Bemühungen, die Abgabenordnung (AO) der neueren Datenschutzgesetzgebung anzupassen und den Umgang mit Daten, die dem Steuergeheimnis unterliegen, deutlicher und verständlicher als bisher zu regeln, sind im Berichtszeitraum nicht vorangekommen.

Die bereits im Mai 1996 gemeinsam eingebrachten Veränderungsvorschläge der Datenschutzbeauftragten des Bundes und der Länder hat das Bundesministerium der Finanzen (BMF) im März 1997 im wesentlichen abgelehnt.
In Übereinstimmung mit den für Fragen der AO zuständigen Vertretern der obersten Finanzbehörden der Länder bestehe aus der Sicht des BMF kein Handlungsbedarf zur Änderung der Abgabenordnung aufgrund datenschutzrechtlicher Erwägungen.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich auf ihrer Konferenz im Oktober 1997 darauf verständigt, gegenüber dem BMF an den wesentlichen Änderungsvorschlägen weiter festzuhalten. Dazu gehören u. a.:
- begriffliche Klarstellungen in § 30 AO (Steuergeheimnis),

- die Präzisierung der Zweckbindung von Daten, die in Dateien und Akten für "zukünftige Verfahren" gesammelt werden dürfen (§ 88 a AO, vgl. 13. TB, 10.1.1),
- die Aufhebung der generellen Verpflichtung von Gerichten und Behörden, der Finanzbehörde alle Tatsachen mitzuteilen, die den Verdacht einer Steuerstraftat begründen (§ 116 AO),
- differenzierte Regelungen zur Verarbeitung von Daten durch die Steuerfahndung (§ 208 AO).

9. Wissenschaft und Forschung

9.1 Einsichtnahme in Personenstandsbücher für das Projekt der KZ-Gedenkstätte Neuengamme

Im 14. TB (9.3) hatten wir darüber berichtet, daß das Hessische Ministerium des Innern und das Regierungspräsidium Kassel zunächst ihre Bedenken gegen eine Einsichtnahme der Unterlagen beim Sonderstandesamt Arolsen zurückgestellt und anschließend erneut Bedenken gegen die begehrte Einsichtnahme durch die KZ-Gedenkstätte Neuengamme erhoben haben.

Nachdem zwischenzeitlich der Internationale Ausschuß für den Internationalen Suchdienst des Roten Kreuzes die Einsichtnahme in die Unterlagen beim Sonderstandesamt Arolsen grundsätzlich befürwortet hat, erklärte sind auch das Hessische Ministerium des Innern dazu bereit, seine Bedenken zurückzustellen, sofern sich das Regierungspräsidium Kassel, das Sonderstandesamt Arolsen und die KZ-Gedenkstätte Neuengamme auf ein praktikabeles Verfahren einigen.

Im gegenseitigen Einvernehmen konnte die Zustimmung zu folgendem Kompromiß erwirkt werden:
- Die Einsichtnahme wird auf die Urkunden und im Bedarfsfall auf die Suchkartei des Internationalen Suchdienstes des Roten Kreuzes (ISD) beschränkt. Eine Einsichtnahme in die Sammelakten des ISD wird ausgeschlossen.
- Die Gedenkstätte Neuengamme stellt sicher, daß das Projekt ausschließlich historischen und humanitären Zwecken dient. Eine andere Verwendung des Datenmaterials wird ausgeschlossen.
- Solange von den niederländischen Behörden keine Freigabe der mit Sperrvermerk versehenen Urkunden erfolgt ist, verpflichtet sich die KZ-Gedenkstätte Neuengamme, Daten aus diesen Urkunden nicht zu erfassen und zu verwerten. Gestattet ist allerdings, für eine mögliche spätere Erfassung die Registernummern der betreffenden Urkunden zu notieren.
- Der mit der Auswertung der Urkunden befaßte Mitarbeiter der KZ-Gedenkstätte Neuengamme verpflichtet sich vor Aufnahme der Tätigkeit zur Verschwiegenheit i. S. des § 61 PStG.

Nach mehr als zweieinhalbjährigen Bemühungen sind damit die datenschutzrechtlichen Bedenken hinsichtlich des geplanten Totenbuches mit den Angaben über die Opfer des früheren KZ-Neuengamme und seiner Außenlager zufriedenstellend geklärt.

10. Bauwesen und Stadtentwicklung

10.1 Online-Verordnung über Daten aus dem Flächenbezogenen Informationssystem

Im 15. TB (11.) hatten wir darüber berichtet, daß die Verordnung über den automatisierten Abruf und die automatisierte Speicherung, Veränderung und Löschung von Daten aus dem

Flächenbezogenen Informationssystem (FIS-OnlineVO) auf Grund von § 14 Abs. 5 und 6 Hamburgisches Gesetz über das Vermessungswesen in die behördliche Abstimmung gegeben wurde.

Das behördliche Abstimmungsverfahren ist zwischenzeitlich abgeschlossen worden, so daß der Senat am 17. Juni 1997 diese Rechtsverordnung erlassen konnte.

Durch die Verordnung wird ein automatisiertes Abrufverfahren und die Speicherung, Veränderung und Löschung von Daten aus dem Flächenbezogenen Informationssystem (FIS) erstmals geregelt.

Die FIS-OnlineVO ist in drei Teile untergliedert: Der erste Teil (§§ 1 bis 10) regelt den automatisierten Abruf für die dort genannten Stellen. Der zweite Teil (§ 11) betrifft die Zulässigkeit der automatisierten Speicherung, Veränderung und Löschung von Daten. Der dritte Teil (§§ 12 bis 14) bezieht sich auf die erforderlichen Maßnahmen zur Datensicherung und Datenschutzkontrolle (z. B. Benutzer-, Zugriffs-, Eingaben- und Übermittlungskontrollen, Protokollierungen).

Aus Gründen der Normenklarheit haben wir darauf gedrungen, daß für die Bürger aus der Verordnung klar erkennbar sein muß, an welche Stellen und für welche konkreten Zwecke ihre personenbezogenen FIS-Daten übermittelt werden. Denn diese Anforderung an ein automatisiertes Abrufverfahren ist auch in § 11 Abs. 2 Hamburgisches Datenschutzgesetz (HmbDSG) deutlich herausgestellt worden.

Die zuständige Baubehörde ist unserem Anliegen gefolgt und hat in den einzelnen Vorschriften die berechtigten Einheiten innerhalb der betroffenen Behörden (Ämter, Abteilungen bzw. Referate) konkret benannt. Dadurch ist die Datenverarbeitung in der neuen Rechtsverordnung so transparent geregelt, wie es für die informationelle Selbstbestimmung unverzichtbar ist.

10.2 Mietenspiegelbefragung 1997

Die Mietenspiegelerhebungen von 1995 als Grunderhebung und 1997 als Fortschreibung mit einer Brutto-Stichprobe von ca. 6.000 Wohnungen wurden auf der Grundlage der Mietenspiegelbefragungsverordnung vom 28. März 1995 (Hamburgisches Gesetz- und Verordnungsblatt Seite 67) durchgeführt (vgl. 14. TB, 10.1).

Der Einsatz von tragbaren PC (Laptop) hatte sich bei der Mietenspiegelerhebung 1995 bewährt. Die dafür verantwortliche Baubehörde und die beauftragten Unternehmen hatten die Einhaltung der zuvor gemeinsam festgelegten technischen und organisatorischen Maßnahmen zur Gewährleistung des Schutzes der personenbezogenen Daten zugesichert. Daher bestanden aus unserer Sicht keine Bedenken gegen den Einsatz von Laptops bei der Mietenspiegelbefragung 1997.

Die Auswertungen der Mietenspiegelbefragung 1997 haben im Vergleich zu der Mietenspiegelbefragung 1995 ergeben, daß die durchschnittlichen Verweigerungsquoten aus allgemeinen Gründen von 13,8 % auf 8,1 % zurückgegangen sind. Die Verweigerungen aus datenschutzrechtlichen Gründen lagen dagegen wie in den vergangenen Jahren nahezu unverändert bei 0,4 %.

Bereits im 12. TB (12.3) hatten wir berichtet, daß die vom Senat erlassenen Mietenspiegelbefragungsverordnungen jeweils eine Geltungsdauer von 3 Jahren haben und daß der Senat für jede künftige Mietenspiegelerhebung eine neue Rechtsverordnung zu erlassen hat. Die Baubehörde wurde daher nochmals an unseren Vorschlag erinnert, daß wegen der Periodizität der

Mietenspiegelaufstellung eine dauerhafte Regelung für den Mietenspiegel auf Bundesebene oder auf Landesebene realisiert werden sollte.

10.3 Vertragsstrafenregelung bei der Vergabe von Bauaufträgen

Nach den Richtlinien für die Vergabe von Bauleistungen nach Nr. 2.5 der Verwaltungsvorschriften zu § 55 der Landeshaushaltsordnung (LHO) vom 14. Februar 1997 sind alle Dienststellen und Landesbetriebe der Freien und Hansestadt Hamburg sowie die Körperschaften, Stiftungen und Anstalten des öffentlichen Rechts gehalten, mit den potentiellen Auftragnehmern eine Vertragsstrafenregelung in den Bauaufträgen zu vereinbaren, um so u. a. der Schwarzarbeit im Bereich des Bauwesens wirksamer begegnen zu können.

Nach dieser Regelung haben sich die Auftragnehmer bei der Vergabe von öffentlichen Bauaufträgen vertraglich zu verpflichten, daß sie im Falle von Verstößen gegen gesetzliche Vorschriften über die illegale Beschäftigung von Arbeitskräften, der Schwarzarbeit und des Arbeitnehmer-Entsendegesetzes eine Vertragsstrafe in Höhe von 5 % der Auftragssumme je Verstoß, höchstens jedoch 15 % der Abrechnungssumme an den Auftragsgeber zu zahlen haben. Dabei hat der Auftragnehmer auch für das Fehlverhalten Dritter (z. B. Subunternehmer) einzustehen.

Nach dem ursprünglichen Entwurf der Vertragsstrafenregelung sollten die Auftragnehmer bei Abnahme des Werkes für sich und alle Nachunternehmer einen Auszug aus dem Gewerbezentralregister (sog. Selbstauskünfte) vorlegen, um so Kenntnisse über entsprechende Verstöße zu erlangen.

Gegen diese Regelung haben wir Bedenken erhoben, weil das Verlangen einer Selbstauskunft aus dem Gewerbezentralregister einen beträchtlichen Eingriff in die Rechte der Betroffenen darstellt, der nicht durch die Regelungen der
§§ 150 (Auskunft an den Betroffenen) und 150 a (Auskunft an Behörden) der Gewerbeordnung (GewO) gedeckt ist. § 150 a GewO legt abschließend fest, an welche Behörden und für welche Zwecke Auskünfte aus dem Gewerbezentralregister erteilt werden dürfen. Diese Beschränkungen dürfen daher nicht durch eine an den Betroffenen gerichtete Aufforderung zu weitergehender Selbstauskunft umgangen werden. Hinzu kommt, daß derartige Auskünfte z. B. auch Ordnungswidrigkeiten einbeziehen, die in keinem Zusammenhang mit den vorgenannten Verstößen stehen und daher auch keinen Aussagewert für die Beurteilung der gewerberechtlichen Zuverlässigkeit des Auftragnehmers oder der Verwirkung einer Vertragsstrafe haben.

Die zuständige Baubehörde hat daraufhin auf die Vorlage einer Selbstauskunft aus dem Gewerbezentralregister verzichtet. Statt dieser Regelung hat der Auftragnehmer nunmehr bei Abnahme des Werkes eine Erklärung darüber abzugeben, ob gegen ihn bzw. seinen Erfüllungsgehilfen bei der Ausführung der übertragenen Leistung ein Ordnungswidrigkeitsverfahren, Ermittlungsverfahren oder Strafverfahren anhängig ist bzw. wie dieses rechtskräftig zum Abschluß gekommen ist. Gegen diese datenschutzfreundlichere Regelung haben wir keine Bedenken erhoben.

Nach unseren Feststellungen hat die Baubehörde zwar in den Vertragsstrafenregelungen auf die Selbstauskünfte verzichtet. In den Vordrucken über die Bewerbungsbedingungen für die Vergabe von Bauleistungen hat sie dagegen gleichwohl an den Selbstauskünften festgehalten. Eine abschließende Klärung konnte hierüber bis Redaktionsschluß noch nicht erzielt werden.

11. Meldewesen

11.1 Rechtsverordnung zur Durchführung des Hamburgischen Meldegesetzes

Am 9. September 1997 hat der Senat die Verordnung zur Änderung von Verordnungen zur Durchführung des Hamburgischen Meldegesetzes erlassen. Datenschutzrechtlich von besonderem Interesse ist dabei die Verordnung über regelmäßige Datenübermittlungen und automatisierte Abrufe aus dem Melderegister (Meldedatenübermittlungsverordnung - MDÜV). Sie dient der Vereinheitlichung und redaktionellen Anpassung bereits bestehender Einzelverordnungen. Neu eingeführt wurden automatisierte Abrufe für die Fahrerlaubnisbehörden, die Finanzämter, die Bußgeld-, Strafsachen- und Steuerfahndungsstelle, die Landeshauptkasse und die bezirklichen Vollstreckungsstellen. Erheblich erweitert wurde der automatisierte Zugriff der Polizeidienststellen auf Meldedaten.

In einem intensiven und konstruktiven Dialog mit der Behörde für Inneres (BfI) konnten wir erhebliche Verbesserungen für den Datenschutz erzielen. Die Daten, die von den Finanzämtern automatisiert abgerufen werden dürfen, wurden auf den für eine effiziente Sachbearbeitung zwingend erforderlichen Umfang begrenzt. Wie bereits nach bisherigem Recht die Sozialhilfedienststellen, dürfen auch Finanzämter, die Landeshauptkasse und die bezirklichen Vollstreckungsstellen automatisiert auf Meldedaten nur zugreifen, wenn über die Betroffenen im eigenen Datenbestand der abrufenden Stelle bereits Daten gespeichert sind; dies ist technisch sicherzustellen.

Soweit Teilnehmer am automatisierten Abruf über den eigenen Datenbestand hinaus Daten aus dem Melderegister erhalten, sind hierüber detaillierte Aufzeichnungen zu fertigen, die als Grundlage für die Wahrnehmung der Dienst- und Fachaufsicht in einem Stichprobenverfahren dienen. Wird im Rahmen der Dienst- und Fachaufsicht die Unzulässigkeit eines Abrufs festgestellt, so sind in schwerwiegenden Fällen die Einwohner, deren Daten abgerufen wurden, von der aufsichtführenden Stelle über Anlaß und Zeitpunkt des Abrufs, die abgerufenen Daten und die abrufende Stelle, von Ausnahmefällen abgesehen, unverzüglich von Amts wegen zu unterrichten. Schwerwiegende Fälle liegen insbesondere dann vor, wenn der Abruf ohne jeden sich aus der jeweiligen Aufgabenerfüllung ergebenden Anlaß (z. B. aus bloßer Neugier oder zu dienstfremden Zwecken) erfolgt ist oder die Unzulässigkeit des Abrufs wiederholt festgestellt wird. Ferner ist ein schwerwiegender Fall stets dann gegeben, wenn Daten von Personen, zu deren Gunsten eine melderechtliche Auskunftssperre besteht, unzulässig automatisiert abgerufen wurden. Soweit eine Unterrichtung der Betroffenen aus Rechtsgründen ausnahmsweise nicht in Betracht kommt, sind die wesentlichen Gründe hierfür aufzuzeichnen und der oder dem Hamburgischen Datenschutzbeauftragten mitzuteilen. Die oder der Hamburgische Datenschutzbeauftragte prüft in eigener Verantwortung nach, ob die aufsichtführende Stelle zu Recht von einer Unterrichtung der Betroffenen abgesehen hat.

Die im Vergleich mit dem Melderecht anderer Bundesländer bislang einmalige Benachrichtigung der Betroffenen in Fällen unzulässiger Online-Abrufe bildet eine wesentliche Voraussetzung dafür, die automatisierte Datenverarbeitung mit ihren spezifischen Risiken für die Betroffenen transparent zu gestalten und effektiven Rechtsschutz zu gewährleisten.

11.2 Melderegisterauskünfte an Parteien für Zwecke der Wahlwerbung

Die persönlich adressierte Wahlwerbung insbesondere der DVU vor der Bürgerschaftswahl am 21. September 1997 sowie persönlich adressierte Danksagungen für die (angebliche) Unterstützung der DVU bei dieser Wahl führten zu zahlreichen Eingaben und Beschwerden (vgl. 1.1.5). Viele Bürgerinnen und Bürger wandten sich nachdrücklich dagegen, durch die Adressierung mit den

Zielen und Aussagen der DVU identifiziert zu werden. Häufig wurde auch kritisiert, daß die Betroffenen über die Rechtslage nicht frühzeitig und deutlich unterrichtet worden seien.

Nach § 35 Abs. 1 des Hamburgischen Meldegesetzes (HmbMG) dürfen die Meldebehörden Parteien, Wählervereinigungen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit allgemeinen Wahlen in den sechs Monaten vor der Wahl Auskunft aus dem Melderegister über Vor- und Familiennamen, Doktorgrad und aktuelle Wohnanschrift von Wahlberechtigten übermitteln, soweit diese der vom Datenempfänger genannten Altersgruppe angehören. Die Betroffenen können Melderegisterauskünften für Zwecke der Wahlwerbung durch Erklärung gegenüber dem Einwohnermeldeamt (einem Bezirks- bzw. Ortsamt ihrer Wahl in Hamburg) widersprechen. Der Widerspruch muß nicht begründet werden. Seine Bearbeitung erfolgt gebührenfrei. Ein Widerspruch gegen kommerzielle Werbung, z. B. durch Eintragung in die Robinson-Liste des Deutschen Direktmarketing-Verbands e. V., ersetzt den melderechtlichen Widerspruch nicht.

Die Melderegisterauskünfte dürfen nur für Zwecke der Wahlwerbung, nicht hingegen zur Mitgliederwerbung, für Spendenaufrufe oder zur Förderung des Absatzes bestimmter Publikationen genutzt werden. Die Auskünfte sind innerhalb einer Woche nach dem Wahltag zu löschen. Das Verbot längerfristiger Speicherung gilt nach unserer Auffassung auch für Daten aus der Korrespondenz der Parteien mit Bürgerinnen und Bürgern, die sich über die persönlich adressierte Wahlwerbung beschweren oder Auskunft über die Herkunft der Daten verlangen.

Eine Bürgerschaftsfraktion hat sich für die Streichung des § 35 Abs. 1 HmbMG ausgesprochen (Bürgerschafts-Drucksache 16/23). Auch wir sind der Ansicht, daß § 35 Abs. 1 HmbMG zumindest in seiner gegenwärtigen Fassung dem Grundrecht auf informationelle Selbstbestimmung nicht hinreichend Rechnung trägt.

Sofern die Vorschrift nicht aufgehoben wird, bedarf es jedenfalls einer Reihe datenschutzfreundlicher Verbesserungen. Insbesondere sollten den politisch interessierten Bürgerinnen und Bürgern, die sich nicht generell, sondern nur gegen bestimmte Formen der Wahlwerbung wenden, entsprechende Wahlmöglichkeiten (vgl. 1.1) mit verbindlicher Wirkung gegenüber den Parteien eröffnet werden. Ferner treten wir für eine deutlich verbesserte Information über das Widerspruchsrecht und eine präziser formulierte Zweckbindung der Melderegisterauskünfte ein. Die Kontrollbefugnisse der oder des Hamburgischen Datenschutzbeauftragten bei Verstößen gegen § 35 Abs. 1 HmbMG sollten gestärkt, insbesondere anlaßunabhängige Überprüfungen bei den Parteien und den von ihnen in die Wahlwerbung eingeschalteten Auftragnehmern (z. B. Copy-Shops) ermöglicht werden. Schließlich halten wir es für erforderlich, die Sanktionen bei rechtswidrigem Umgang mit Melderegisterauskünften zu erweitern und zu verschärfen.

Vorschläge für entsprechende Gesetzesänderungen werden wir in den Ausschußberatungen unterbreiten. Auch diskutieren wir gegenwärtig mit der Behörde für Inneres (BfI) und dem Senatsamt für Bezirksangelegenheiten praktische Maßnahmen, die der verbesserten Aufklärung über das Widerspruchsrecht dienen.

Im Hinblick auf die Bundestagswahl im September 1998 hoffen wir, daß unsere Anregungen zügig aufgegriffen und umgesetzt werden.

12. Ausländerangelegenheiten

12.1 Übermittlung von Daten bosnischer Bürgerkriegsflüchtlinge

Im Juli / August 1996 wandte sich das Bundesministerium des Innern (BMI) an die Innenminister und -senatoren der Länder mit dem Ersuchen, personenbezogene Daten von Bürgerkriegsflüchtlingen aus Bosnien-Herzegowina an eine beim Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) eingerichtete Projektgruppe "Bosnien-Rück" zu übermitteln. Die Erhebung und Aufbereitung dieser Daten durch den Bund diene dazu, international finanzierte Wiederaufbauprojekte zu koordinieren und auf diese Weise die freiwillige Rückkehr von Bürgerkriegsflüchtlingen zu fördern. Erfolgreiche Verhandlungen mit den internationalen Geldgebern seien nur dann gewährleistet, wenn dem jeweiligen Projektantrag eine Liste mit Daten der Eigentümer und Wohnberechtigten der wiederaufzubauenden Häuser beigefügt werde. Eine zielstrebige Koordinierung der Hilfsmaßnahmen setze voraus, daß die Gesamtheit der potentiell begünstigten Flüchtlinge von der Projektgruppe "Bosnien-Rück" erfaßt werde, unabhängig davon, ob bereits eine Erklärung über die freiwillige Rückkehr vorliege oder nicht.

Mit der Behörde für Inneres (BfI) haben wir eingehend die Frage erörtert, ob und in welchem Umfang es erforderlich ist, Daten der Flüchtlinge personenbezogen an das BAFl und von dort an weitere Stellen, z. B. das Auswärtige Amt, die deutsche Botschaft in Sarajewo und die Europäische Union (EU), zu übermitteln. Das Ergebnis dieser Diskussion, die wir im Juli 1997 abgeschlossen haben, wurde wesentlich dadurch beeinflußt, daß der Bundesbeauftragte für den Datenschutz (BfD) mitgeteilt hatte, er halte die vom BMI vorgetragene Begründung für überzeugend. Unsere anfänglichen Bedenken gegen eine personenbezogene Übermittlung konnten wir auch deshalb zurückstellen, weil die BfI bedeutsame datenschutzrechtliche Anliegen aufgegriffen hat.

Bosnische Asylbewerber und Bosnier mit einer Aufenthaltsbefugnis sind von der Datenübermittlung nicht betroffen. Angaben zur ethnischen Zugehörigkeit und zum religiösen Bekenntnis dürfen nicht an die Projektgruppe weitergegeben werden. Die Datenübermittlung wurde ferner an die Bedingung geknüpft, daß die Bundesregierung nur der EU einen vollständigen Überblick über die Daten gewähren darf. An andere Organisationen dürfen Informationen nur weitergegeben werden, wenn und soweit es für die Umsetzung konkreter Projekte der EU unabdingbar auf den Personenbezug ankommt und eine mißbräuchliche Verwendung oder Weitergabe der Daten ausgeschlossen ist. Schließlich sagte uns die BfI zu, sich gegenüber dem Bund in geeigneter Form dafür einzusetzen, daß die Daten nur unter strikter Zweckbindung genutzt und unverzüglich gelöscht werden, sobald und soweit sie für die Projektdurchführung nicht mehr erforderlich sind.

Wir haben der BfI gegenüber zum Ausdruck gebracht, daß ein sensibler und verantwortungsbewußter Umgang mit den Daten vor Ort, gerade angesichts der humanitären Zielsetzung, für uns von zentraler Bedeutung ist. Von der BfI erwarten wir, daß uns nach Abschluß der Projekte im einzelnen erläutert wird, wie die Durchführung gemäß diesen Anforderungen sichergestellt und kontrolliert wurde.

13. Verfassungsschutz

13.1 Referentenentwurf eines Hamburgischen Sicherheitsüberprüfungsgesetzes (HmbSÜG)

Wiederholt berichteten wir darüber, daß in Hamburg noch immer eine bereichsspezifische Rechtsgrundlage für Sicherheitsüberprüfungen fehlt (vgl. 13. TB, 1.5.3, 18.2; 14. TB, 1.3.2; 15. TB, 1.5.2). An der - noch nicht abgeschlossenen - Behördenabstimmung zum Referentenentwurf eines Hamburgischen Sicherheitsüberprüfungsgesetzes (HmbSÜG) haben wir uns intensiv beteiligt.

In seiner Konzeption folgt der Entwurf dem Sicherheitsüberprüfungsgesetz des Bundes vom 20. April 1994 (BGBl. I S. 867), bezieht jedoch neben dem personellen Geheimschutz (Verschlußsachen) auch den vorbeugenden Sabotageschutz ein. In der Diskussion mit dem Landesamt für Verfassungsschutz Hamburg (LfV) haben wir die besondere Sensibilität der bei Sicherheitsüberprüfungen verarbeiteten personenbezogenen Daten unterstrichen. Insbesondere haben wir uns für die Berücksichtigung folgender Anliegen eingesetzt:

In die Sicherheitsüberprüfung einbezogene Ehegatten und Lebenspartner sollten die Möglichkeit erhalten, eine gesonderte Sicherheitserklärung abzugeben. Dies ist insbesondere dann von Bedeutung, wenn sie ihrem Partner (dem Betroffenen) bestimmte Tatsachen (z. B. anhängige Strafverfahren) nicht offenbaren möchten.

Den Betroffenen, die eine sicherheitsempfindliche Tätigkeit bei einem privaten Arbeitgeber (z. B. einem Rüstungsbetrieb) wahrnehmen wollen, sollte die Wahlmöglichkeit (vgl. 1.1.4) eingeräumt werden, ihre Sicherheitserklärung unmittelbar dem LfV zuzuleiten, wenn sie Wert darauf legen, daß ihr Arbeitgeber bestimmte Tatsachen (z. B. Zwangsvollstreckungsmaßnahmen) nicht erfährt. Verfahren die Betroffenen in dieser Weise, darf ihnen daraus weder im Rahmen der Sicherheitsüberprüfung noch im Verhältnis zu ihrem Arbeitgeber ein Nachteil erwachsen.

Die Rechtsstellung der Betroffenen sollte ferner durch eine Reihe von Anhörungserfordernissen gestärkt werden, z. B. bei Mitteilungen sicherheitserheblicher Erkenntnisse von der Personalverwaltung an den Geheimschutzbeauftragten oder vom privaten Arbeitgeber an das LfV. Nach dem Vorbild des Art. 15 der EG-Datenschutzrichtlinie und des Personalaktenrechts für Beamte sollte daneben ein umfassendes Verbot von Persönlichkeits- und Zuverlässigkeitsbewertungen verankert werden, die sich ausschließlich auf automatisiert gewonnene Erkenntnisse stützen.

Eine automatisierte Speicherung von Daten einbezogener Personen sollte - wie bereits nach dem Hamburgischen Verfassungsschutzgesetz (HmbVerfSchG) - nur mit ihrer Einwilligung zulässig sein. Damit wird den einbezogenen Personen die Wahlmöglichkeit (vgl. 1.1.4) eingeräumt, der Sicherheitsüberprüfung zwar grundsätzlich zuzustimmen, aber mit der Einschränkung, daß ihre Daten nur in Akten verarbeitet werden dürfen. Die Ausübung dieses Wahlrechts sollte durch ein Benachteiligungsverbot und die Möglichkeit des Widerrufs der Einwilligung in automatisierte Speicherung gesichert werden.

Im Vergleich zur Regelung des Bundes sollte auch die Zweckbindung von Erkenntnissen aus Sicherheitsüberprüfungen stärker betont werden. Diese Erkenntnisse sollten nicht allgemein zur Verfolgung von Straftaten von erheblicher Bedeutung, sondern nur zur Verfolgung bestimmter, eng umschriebener Katalogtaten (z. B. Staatsschutzdelikte, Mord, Geiselnahme, Brandstiftung) an die Strafverfolgungsbehörden übermittelt werden. Auch die Nutzung von Daten aus Sicherheitsüberprüfungen für sonstige Aufgaben des LfV sollte gegenüber der Regelung des Bundes eingeschränkt werden.

Schließlich sollte die Aufbewahrungsfrist beim LfV für Unterlagen aus Sicherheitsüberprüfungen Ü 2 (Erweiterte Sicherheitsüberprüfungen) mit (im Regelfall) fünf Jahren nach Ausscheiden aus der sicherheitsempfindlichen Tätigkeit deutlich kürzer bemessen werden als nach dem Recht des Bundes (zehn Jahre).

Damit wäre insgesamt ein hoher Datenschutzstandard erreicht. Wir erwarten, daß der Entwurf im Senat und anschließend in der Bürgerschaft zügig beraten wird. Da auch nach Ablauf der 15. Wahlperiode der Bürgerschaft ein konkreter Zeitpunkt für die Verabschiedung des HmbSÜG

immer noch nicht abzusehen ist, werden wir Einschränkungen in der Praxis der Sicherheitsüberprüfung bis zum Inkrafttreten einer gesetzlichen Regelung noch mit dem LfV erörtern.

13.2 Datenschutzkontrolle im Referat Sicherheitsüberprüfungen des Landesamtes für Verfassungsschutz (LfV)

Im Zeitraum April bis Juli 1997 führten wir eine umfangreiche Kontrolle im Referat "Geheimschutz" des Landesamtes für Verfassungsschutz Hamburg (LfV) durch. Diesem Referat obliegt die Sicherheitsüberprüfung von Personen, die eine sicherheitsempfindliche Tätigkeit künftig ausüben sollen oder bereits ausüben. Da für Sicherheitsüberprüfungen in Hamburg bislang eine gesetzliche Grundlage fehlt (vgl. 13.1), orientierte sich unsere Bewertung vornehmlich am Maßstab der Sicherheitsrichtlinien (SiR) des Senats vom 20. November 1990 oder, soweit sich hieraus ein datenschutzfreundlicheres Ergebnis ableitet, am Referentenentwurf eines Hamburgischen Sicherheitsüberprüfungsgesetzes (HmbSÜG).

Unsere Prüfung wurde vom LfV in fachlicher und organisatorischer Hinsicht voll unterstützt. In seiner Stellungnahme zu unserem Prüfbericht hat sich das LfV unserer Einschätzung der Sach- und Rechtslage in allen Punkten angeschlossen und unsere Anregungen konstruktiv aufgegriffen. Erfahrungen, die hierauf beruhen, haben auch Eingang in den Referentenentwurf eines HmbSÜG gefunden.

Besonders kritisch wurde von uns bewertet, daß das LfV in der ersten Jahreshälfte 1993 in einer erheblichen Anzahl von Fällen Auskünfte bei Stellen außerhalb des Nachrichtendienstlichen Informationssystems der Verfassungsschutzämter (NADIS) über Personen eingeholt hat, die weder Betroffene noch in die Sicherheitsüberprüfung einbezogen waren (z. B. die Eltern oder die im Haushalt der Betroffenen lebenden volljährigen Kinder). Die Anfragen richteten sich in diesen Fällen auch an den Bundesnachrichtendienst (BND), an das Bundeszentralregister (BZR) und einzelne Landeskriminalämter (LKA). Mit dem LfV besteht Einvernehmen darüber, daß diese Anfragen durch die SiR nicht gedeckt waren und Gründe für die Auskunftsersuchen aus den Sicherheitsüberprüfungsakten auch nicht nachvollziehbar sind.

Andererseits konnte festgestellt werden, daß in der Zeit seit August 1993 unzulässige Abfragen nur noch in einzelnen Ausnahmefällen erfolgten. Da das LfV somit seine rechtswidrige Abfragepraxis bereits vor längerer Zeit weitgehend selbst korrigiert hat, sahen wir keinen Anlaß für eine förmliche Beanstandung. Das LfV hat zugesagt, in Zukunft noch strenger darauf zu achten, daß die Anfragen sich ausnahmslos auf den zulässigen Umfang beschränken. Unsere Erfahrungen unterstreichen allerdings, daß eine umfassende Kontrollbefugnis der oder des Hamburgischen Datenschutzbeauftragten gerade im sensiblen Bereich der Sicherheitsüberprüfungen nicht nur zum Schutz der Betroffenen, sondern auch zur konstruktiven Begleitung und Unterstützung der Tätigkeit des LfV weiterhin unverzichtbar ist.

Bei erweiterten Sicherheitsüberprüfungen mit Sicherheitsermittlungen (Ü 3) werden in der Regel Befragungen von Referenzpersonen durch Mitarbeiter des LfV durchgeführt. Nach dem Grundsatz der Verhältnismäßigkeit dürfen in die Befragungsberichte Angaben über Gesundheit, Intimangelegenheiten, dienstliche Leistungen und Parteizugehörigkeit sowie Daten Dritter nicht aufgenommen werden, es sei denn, gerade in diesen Feststellungen liegt ein unmittelbarer Geheimschutzbezug.

Unter Heranziehung dieses Maßstabs kann die aktuelle Praxis der Abfassung von Befragungsberichten durch das LfV insgesamt als erfreulich bezeichnet werden. Im allgemeinen

halten sich die Angaben über Charaktermerkmale, soziale Verhaltensweisen, psychische Probleme, Abhängigkeiten und Freizeitbeschäftigungen der Betroffenen im Rahmen des Erforderlichen und Angemessenen. Gleiches gilt für Schilderungen über Verlauf und Atmosphäre der Gespräche mit den Referenzpersonen. Einzelne Abweichungen von dieser Praxis haben wir mit dem LfV einvernehmlich besprochen.

14. Verkehrswesen

14.1 Telefaxwerbung für "Radarwarngeräte"

Zu Beginn des Jahres 1997 wandten sich Bürger an die Medien und an uns, weil sie den Verdacht hatten, daß es bei Behörden in Hamburg eine "undichte Stelle" gebe, die ihre Daten mißbraucht habe.

Hervorgerufen wurde dieser Verdacht durch unangefordert eingehende Telefaxe, in denen für sogenannte "Radarwarngeräte" geworben wurde. Diesen Faxschreiben selbst hätten die Bürger eigentlich keine besondere Bedeutung zugemessen. Merkwürdig kam ihnen jedoch vor, daß sie zuvor wegen einer Geschwindigkeitsüberschreitung oder einer überfahrenen roten Ampel "geblitzt" worden waren. Wenn es einen derartigen zeitlichen Zusammenhang dann auch noch mehrfach im Abstand von einigen Monaten gab, waren sich viele Betroffene fast sicher, daß hier etwas nicht mit rechten Dingen zugehen konnte: Hatte die Firma etwa Informationen über die Bußgeldverfahren erhalten, um dann gezielt für ihre Geräte, die angeblich vor Radarfallen warnen, zu werben?

Nachdem die Medien ausführlich über diesen Verdacht berichtet hatten, gab es eine ganze Flut von Hinweisen auf gleichgelagerte Fälle, die teilweise bei uns und vor allem bei der Innenbehörde eingingen, die dazu aufgerufen hatte, Auffälligkeiten mitzuteilen. Nach der Auswertung der geschilderten Einzelfälle sind wir in Übereinstimmung mit der Innenbehörde zu dem Ergebnis gelangt, daß es keine konkreten Anhaltspunkte für die Annahme gibt, die Zusendung der Faxschreiben sei auf irgendeine undichte Stelle im Behördenbereich zurückzuführen.

Gegen diese Annahme sprach neben weiteren Umständen insbesondere, daß sich die von den Bürgern geschilderten Geschwindigkeitskontrollen und auch die anschließenden Bußgeldverfahren nicht auf einen bestimmten Bereich oder die Zuständigkeit bestimmter Behörden konzentrierten. Vielmehr wurden Fälle aus dem gesamten Bundesgebiet geschildert, so daß es keine bestimmten örtlichen Verkehrs- oder Bußgeldbehörden gab, bei der sich die Auffälligkeiten konzentrierten. Auch das Kraftfahrt-Bundesamt in Flensburg als einzige Behörde, in der - theoretisch - Informationen über sämtliche Fälle vorliegen könnten, ließ sich nach näherer Überprüfung ausschließen.

Andererseits sprach viel dafür, daß das zeitliche Zusammentreffen von Bußgeldverfahren und Empfang der Werbefaxschreiben auf Zufälle zurückzuführen war. Die Firma versandte ihre Faxschreiben in so großer Zahl und auch mehrfach an dieselben Adressaten, daß Überschneidungen zwischen aktuellen Bußgeldverfahren und dem Eingang der Telefaxe keinesfalls ungewöhnlich erschienen.

Auch wenn man somit keinen Mißbrauch behördlicher Daten vermuten muß, sind die Werbeaktionen der Firma keinesfalls unbedenklich. Nach der Rechtsprechung des Bundesgerichtshofes verstößt die unaufgeforderte Zusendung von Werbung per Telefax gegen § 1 des Gesetzes gegen den unlauteren Wettbewerb (UWG), wenn dies - wie hier - außerhalb bereits bestehender Geschäftsbeziehungen erfolgt (BGH NJW 1996, 660 f.). Betroffene können sich an die

örtlichen Verbraucherzentralen wenden, die gegen derartige Wettbewerbsverstöße gerichtlich vorgehen können.

Klärungsbedürftig war ferner, aufgrund welcher Datenbestände die Firma die Faxschreiben offenbar computergesteuert versendet und ob Widersprüche von Empfängern gegen die Verwendung ihrer Daten beachtet werden. Der Landesbeauftragte für den Datenschutz in Niedersachsen als zuständige Aufsichtsbehörde für die Firma hat sie gemäß § 38 Abs. 3 S. 1 BDSG zu entsprechenden Auskünften aufgefordert. Da diese nicht erteilt wurden, ist ein Bußgeldverfahren eingeleitet worden.

15. Polizei

15.1 Projekt Computerunterstützte Vorgangsbearbeitung bei der Polizei (COMVOR)

Im Herbst 1997 war die Einführung wesentlicher Teile des neuen Verfahrens zur computerunterstützten Vorgangsbearbeitung (COMVOR) bei der Polizei vorgesehen. Bekanntlich konnte dies jedoch aufgrund technischer Probleme nicht realisiert werden. Die geplanten ersten Teilleistungen von COMVOR sind aus datenschutzrechlicher Sicht wie folgt zu bewerten:

Der Teilbereich Vordruckbearbeitung ersetzt die bisherigen Papierformulare bei polizeilichen Strafermittlungen (z. B. Strafanzeige, Beschuldigten- oder Zeugenvernehmung) durch eine Vielzahl von vordefinierten Bildschirmmasken. Hierdurch wird zwar die Arbeitsweise der Anwender wesentlich verändert; datenschutzrechtliche Probleme entstehen jedoch nicht. Denn die reine Vordruckbearbeitung führt - noch - nicht zur automatisierten Speicherung der erfaßten Daten. Die ausgefüllten Bildschirmmasken werden vielmehr ausgedruckt und zur Akte genommen. Eine dauerhafte automatisierte Speicherung von Akteninhalten wird erst durch zukünftige Teilleistungen ermöglicht.

Als weiterer Schritt der Vorgangsbearbeitung mit COMVOR soll die Möglichkeit zur automatisierten Übertragung von Vorgangsteilen an andere Dienststellen geschaffen werden. Dies kann z. B. erforderlich sein, wenn eine Strafanzeige beim Polizeirevier aufgenommen wird, zuständig für die weitere Sachbearbeitung jedoch das Landeskriminalamt ist. Zu begrüßen ist, daß mit der Polizei von Anfang an Konsens über der Notwendigkeit bestand, diese Daten bei ihrer Übertragung zu verschlüsseln. Darüber hinaus muß allerdings auch gewährleistet sein, daß die Abgabe eines Vorgangs an eine andere Dienststelle zur Beendigung der Zugriffsrechte der abgebenden Dienststelle führt. Aufgrund der Schwierigkeiten bei der Einführung des Systems bestand bisher noch keine Gelegenheit zu überprüfen, ob diese Vorgabe eingehalten wird.

Von der inhaltlichen Bearbeitung eines polizeilichen Vorgangs zu unterscheiden ist die sogenannte Vorgangsverwaltung. Sie gibt insbesondere Auskunft darüber, wo sich ein bestimmter Ermittlungsvorgang - eine Akte - zur Zeit befindet.

Zum Zweck der Vorgangsverwaltung werden bisher Tagebücher teilweise in automatisierter Form, zum großen Teil aber auch noch in manuellen Sammlungen geführt. Die Tagebuchfunktion von COMVOR soll diese Systeme ablösen und führt dann an Stelle der bisherigen dezentralen Vorgangsverwaltungen zu einem einheitlichen Tagebuch für die gesamte Polizei. Mit der Erfassung einer Strafanzeige soll künftig ein einheitliches Aktenzeichen als Vorgangsnummer automatisch gebildet werden. Es setzt sich zusammen aus den rechnergesteuerten Angaben zum minutengenauen Zeitpunkt, in dem der Vorgang erstmals bearbeitet wird, und der Dienstnummer des Sachbearbeiters. Die Angaben zur Dienstnummer des Sachbearbeiters sind nicht gesondert

recherchierbar, so daß - problematische - automatisierte Auswertungen, welche Mitarbeiter welche Vorgänge angelegt haben, ausgeschlossen sind.

Ein einheitliches Tagebuch für die gesamte Polizei wirft datenschutzrechtlich nicht unerhebliche Probleme auf. Mit einer Tagebuchabfrage kann festgestellt werden, ob es zu einer bestimmten Person irgendwo bei der Polizei einen Vorgang gibt. Vergleichbare polizeiweite Abfragemöglichkeiten gibt es bisher nur im polizeilichen Auskunftssystem POLAS. Es enthält aber nur Daten über Beschuldigte, bei denen auch nach Ausgang des Ermittlungsverfahrens der Tatverdacht nicht ausgeräumt ist und aufgrund einer Negativprognose die Erforderlichkeit der Speicherung für etwaige künftige Fälle überprüft worden ist. POLAS ermöglicht daher nur Auskünfte über einen Teil aller in polizeilichen Vorgängen als Beschuldigte erfaßten Personen. Im Tagebuch sind dagegen neben allen Beschuldigten insbesondere auch Anzeigeerstatter, also häufig Opfer von Straftaten erfaßt. Eine besondere Überprüfung der Erforderlichkeit der Speicherungen findet im Unterschied zu POLAS nicht statt.

Um zu vermeiden, daß die COMVOR-Tagebuchfunktion künftig als flächendeckende und umfassende Personenauskunftsdatei gebraucht wird, sind reine Namensabfragen regelmäßig nicht möglich. Vielmehr müssen als zusätzliche Suchkriterien immer auch vorgangsbezogene Daten eingegeben werden. Wenn allerdings diese Suchstrategien nicht zum Wiederauffinden eines Vorgangs führen, kann von bestimmten Benutzern auch eine reine Namensabfrage im Tagebuchbestand durchgeführt werden, die dann protokolliert wird.

Die polizeiweite Auskunft aus dem einheitlichen COMVOR-Tagebuch stellt einen Bruch mit der übrigen Konzeption von COMVOR dar, wonach polizeiweite Zugriffe nur auf Daten möglich sind, die den oben geschilderten POLAS-Kriterien entsprechen. Zugriffe auf Daten, die diese Kriterien nicht erfüllen, also insbesondere die Daten von nicht beschuldigten Personen, sollen dagegen nur im Rahmen der Zuständigkeit für den Einzelfall möglich sein.

Wir haben die polizeiweite Tagebuchauskunft gleichwohl akzeptiert, weil ihre Erforderlichkeit zum Auffinden von Vorgängen nachvollziehbar begründet ist, z. B. wenn ein Anzeigenerstatter sich im Polizeirevier erkundigt, was aus seiner Anzeige geworden ist, und diese inzwischen an eine andere Dienststelle weitergeleitet wurde. Die Erfahrung in der Praxis wird zeigen, ob von der polizeiweiten Tagebuchauskunft tatsächlich nur in diesem Rahmen Gebrauch gemacht wird.

15.2 Digitalisierte Lichtbilddatei

Wenn Opfer oder andere Zeugen einer Straftat den Täter gesehen haben, besteht die Chance, daß sie ihn anhand von Fotos wiedererkennen, die bei der Polizei aufgrund erkennungsdienstlicher Maßnahmen vorliegen. Bisher führte die Polizei zu diesem Zweck die sogenannte Lichtbildvorzeigekartei. Sie umfaßte ca. 16.000 Fotos. Damit aus dieser Menge eine gezielte Lichtbildvorlage erfolgen konnte, war sie gegliedert nach kriminalistischen Kriterien (z. B. Straßenraub oder Sexualstraftaten) und nach persönlichen Merkmalen (z. B. männliche und weibliche Beschuldigte; Altersgruppe; Tätowierungen).

Diese Lichtbildvorzeigekartei ist inzwischen digitalisiert worden. Die Fotos aus der bisherigen Kartei sind gescannt, die kriminalistischen Kriterien und die Personenbeschreibungsmerkmale als ergänzende Datenfelder eingegeben worden.

Aufgrund der von Zeugen gegebenen Personenbeschreibung und der in Betracht kommenden kriminalistischen Kategorie stellt der zuständige polizeiliche Sachbearbeiter am PC eine sog. "Arbeitsmappe" zusammen, innerhalb derer die Zeugen unmittelbar am Bildschirm die Lichtbilder

einsehen können. Personalien der abgebildeten Personen sind für die Zeugen bei der Einsichtnahme nicht sichtbar. Bei der Erstellung der "Arbeitsmappe" wird jeweils dokumentiert, aus welcher Menge welche Teilmenge nach welchen Kriterien ausgewählt worden ist. Die Bilder können vergrößert oder in Ausschnitten dargestellt und ausgedruckt werden. Es sind Zusammenstellungen über Personen mit ähnlichem Aussehen für sog. Wahllichtbildvorlagen möglich. Die digitalisierten und ausgedruckten Bilder haben dieselbe Qualität wie die bisherigen Papierfotos.

Die neue Technik hat darüber hinaus auch zu einer anderen Verfahrensweise mit den übrigen erkennungsdienstlichen Lichtbildern geführt, die nicht den besonderen kriminalistischen Kategorien der Lichtbildvorzeigedatei zugeordnet werden. Diese insgesamt mehr als 80.000 Fotos wurden bisher in den Kriminalakten der jeweiligen Personen aufbewahrt. Seit Einführung der neuen Lichtbilddatei werden auch diese erkennungsdienstlichen Fotos digital aufgenommen und gemeinsam mit dem Lichtbildvorzeigebestand gespeichert.

Wir hatten ursprünglich Kritik an diesem neuen Verfahren geübt. Sie richtete sich insbesondere dagegen, daß hiermit der bisherige begrenzte Lichtbildvorzeigebestand auf ein Vielfaches ausgeweitet werde.

Diese Bedenken konnten wir jedoch zurückstellen. Denn auch wenn der Gesamtbestand insgesamt beträchtlich vergrößert wird, führt dies nicht dazu, daß künftig regelmäßig für Zeugenvorlagen mehr Lichtbilder verwendet werden als bisher. Um aus der Gesamtmenge der digitalisiert erfaßten Bilder überhaupt eine Auswahl treffen zu können, müssen hinreichend genaue Suchkriterien verwendet werden. Bei Eingabe der kriminalistischen Kategorien erfolgt die automatisierte Recherche nur im begrenzten Bestand der bisherigen Lichtbildvorzeigekartei. Nur wenn präzise persönliche Merkmale bekannt sind (z. B. Tätowierungen), die eine Identifizierung in einer überschaubaren Anzahl von Lichtbildern ermöglichen, ist eine Recherche im erweiterten Gesamtbestand erfolgversprechend. Ohne derartige präzise Merkmale beantwortet das System die Suchanfrage nicht, weil zu viele Bilder zur Verfügung stehen, auf die die groben Suchkriterien zutreffen.

Die nunmehr eingerichtete digitalisierte Lichtbilddatei ist nur an der zuständigen Dienststelle zentral im Landeskriminalamt verfügbar. In anderen Ländern gibt es inzwischen Pläne, den Zugriff auf derartige Dateien über das polizeiliche Informationssystem auch dezentral allen Dienststellen mit kriminalpolizeilichen Aufgaben zu eröffnen. Auch die Polizei Hamburg wünscht einen solchen dezentralen Zugriff. Sofern sich diese Pläne konkretisieren, müßten zusätzliche Vorkehrungen zur Zugriffskontrolle getroffen werden.

15.3 Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 17./18. April 1997 zu diesem Problem folgende Entschließung gefaßt:

Immer häufiger wird bei der Verfolgung von Straftaten am Tatort oder beim Opfer festgestelltes, sog. biologisches Material als Spurenmaterial durch die Polizei sichergestellt, mittels DNA-Analyse untersucht und mit anderen DNA-Materialien verglichen. Die DNA-Analyse ist zur Standardmethode geworden, um die Herkunft von Spurenmaterial von bestimmten bekannten Personen (Verdächtigen, Opfern, unbeteiligten Dritten) oder die Identität mit anderem Spurenmaterial unbekannter Personen feststellen zu können.

Der Gesetzgeber hat zwar vor kurzem im Strafverfahrensänderungsgesetz - DNA-Analyse ("Genetischer Fingerabdruck") - die Voraussetzungen und Grenzen genetischer Untersuchungen im

Strafverfahren geregelt. Eine Festlegung, ob und in welchen Grenzen die Speicherung und Nutzung der durch eine DNA-Analyse gewonnenen Untersuchungsergebnisse in Datenbanken der Polizei zu erkennungsdienstlichen Zwecken zulässig ist, enthält dieses Gesetz jedoch nicht.

Bezüglich des Aussagegehalts der gespeicherten Daten der Analyseergebnisse ist ein grundsätzlich neuer Aspekt zu berücksichtigen:

Die automatisiert gespeicherten Informationen aus DNA-Merkmalen, die zum Zweck der Identitätsfeststellung erstellt worden sind, ermöglichen derzeit tatsächlich zwar keine über die Identifizierung hinausgehenden Aussagen zur jeweiligen Person oder deren Erbgut. In Einzelfällen können die analysierten nicht codierten persönlichkeitsneutralen DNA-Merkmale jedoch mit codierten Merkmalen korrespondieren. In Anbetracht der weltweiten intensiven Forschung im Bereich der Genom-Analyse ist es nicht ausgeschlossen, daß künftig auch auf der Basis der Untersuchung von bisher als nicht codierend angesehenen Merkmalen konkrete Aussagen über genetische Dispositionen der betroffenen Personen mit inhaltlichem Informationswert getroffen werden können.

Dieser Gefährdung kann dadurch begegnet werden, daß bei Bekanntwerden von Überschußinformationen durch die bisherigen Untersuchungsmethoden andere Untersuchungsmethoden (Analyse eines anderen Genomabschnitts) verwendet werden, die keine Informationen über die genetische Disposition liefern. Derartige Ausweichstrategien können jedoch zur Folge haben, daß die mit anderen Methoden erlangten Untersuchungsergebnisse nicht mit bereits vorliegenden vergleichbar sind. Datenspeicherungen über verformelte Untersuchungsergebnisse können daher dazu führen, daß einmal verwendete Untersuchungsformen im Interesse der Vergleichbarkeit beibehalten werden, obwohl sie sich als problematisch herausgestellt haben und unproblematische Alternativen zur Verfügung stehen, z. B. durch Verschlüsselung problematischer Informationen.

In Anbetracht dieser Situation und angesichts der Tendenz, mittels der DNA-Analyse gewonnene Daten nicht nur in einem bestimmten Strafverfahren zu verwenden, sondern diese Daten in abrufbaren Datenbanken auch für andere Strafverfahren zugänglich zu machen, fordern die Datenschutzbeauftragten des Bundes und der Länder ergänzend zu §§ 81 e und f StPO für die automatisierte Speicherung und Nutzung von DNA-Identitätsdaten eine spezielle gesetzliche Regelung in der Strafprozeßordnung, um das Persönlichkeitsrecht der Betroffenen zu schützen:

1. Es muß ein grundsätzliches Verbot der Verformelung und Speicherung solcher Analyseergebnisse statuiert werden, die inhaltliche Aussagen über Erbanlangen ermöglichen.

   Im Hinblick auf die nicht auszuschließende Möglichkeit künftiger Rückschlüsse auf genetische Dispositionen ist bereits jetzt ein striktes Nutzungsverbot für persönlichkeitsrelevante Erkenntnisse vorzusehen, die aus den gespeicherten Verformelungen der DNA resultieren.

2. Wenn zum Zweck des Abgleichs mit Daten aus anderen Verfahren (also zu erkennungsdienstlichen Zwecken) DNA-Informationen automatisiert gespeichert werden sollen (DNA-Datenbank mit der Funktion, die bei Fingerabdrücken die AFIS-Datenbank des BKA besitzt), müssen darüber hinaus folgende Regelungen geschaffen werden:

   - Nicht jede DNA-Analyse, die zum Zweck der Aufklärung einer konkreten Straftat erfolgt ist, darf in diese Datei aufgenommen werden. Die Speicherung von Verformelungen der

DNA-Struktur in eine Datenbank darf nur dann erfolgen, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß der

- Beschuldigte künftig strafrechtlich in Erscheinung treten wird und daß die Speicherung aufgrund einer Prognose unter Zugrundelegung des bisherigen Täterverhaltens die künftige Strafverfolgung fördern kann.

- Eine Speicherung kommt insbesondere dann nicht in Betracht, wenn der Tatverdacht gegen den Beschuldigten ausgeräumt wurde. Bereits erfolgte Speicherungen sind zu löschen. Gleiches gilt für den Fall, daß die Anordnung der DNA-Untersuchung oder die Art und Weise ihrer Durchführung unzulässig war.

- Die Aufbewahrungsdauer von Verformelungen der DNA-Struktur ist konkret festzulegen (z. B. gestaffelt nach der Schwere des Tatvorwurfs).

3. Voraussetzung für Gen-Analysen muß in jedem Fall mindestens die richterliche Anordnung sein, unabhängig davon, ob die Daten in einem anhängigen Strafverfahren zum Zweck der Straftatenaufklärung, wie in § 81 f Absatz 1 Satz 1 StPO normiert, oder ob sie zum Zweck der künftigen Strafverfolgung (also zu Zwecken des Erkennungsdienstes) benötigt werden.

4. Eine DNA-Reihenuntersuchung von Personengruppen, deren Zusammensetzung nach abstrakt festgelegten Kriterien ohne konkreten Tatverdacht gegenüber einzelnen erfolgt, führt im Regelfall zur Erhebung von DNA-Daten zahlreicher völlig unbeteiligter und unschuldiger Bürger. Die Daten dieser Personen sind unmittelbar dann zu löschen, wenn sie für das Anlaßstrafverfahren nicht mehr erforderlich sind. Sie dürfen nicht in verfahrensübergreifenden DNA-Dateien gespeichert werden und auch nicht mit solchen Datenbeständen abgeglichen werden.

15.4 Speicherfristen im Grenzaktennachweis

Die Wasserschutzpolizei Hamburg nimmt im Hafen Aufgaben des Bundesgrenzschutzes wahr. Sie hat zu diesem Zweck Zugriff auf die bundesweite Verbunddatei "Aktennachweis Bundesgrenzschutz" (BAN), die auch Grenzaktennachweis (GAN) genannt wird, und nimmt selbst Speicherungen in dieser Datei vor. Überwiegend handelt es sich um Fälle, in denen Personen nach den Vorschriften des Ausländergesetzes zurückgewiesen werden, die als "blinde Passagiere" auf Schiffen in den Hamburger Hafen gekommen sind. Daneben gibt es Speicherungen über ausländerrechtliche Straftaten und sonstige Delikte, die z. B. von Schiffsführern begangen werden.

Wir haben den Umgang mit dieser Datei 1997 erstmals überprüft, nachdem das Gesetz über den Bundesgrenzschutz 1994 novelliert worden ist und 1996 neue Richtlinien über den Grenzaktennachweis erlassen worden sind. Als wesentliches Problem hat sich dabei die Einhaltung der Speicherfristen herausgestellt.

Üblicherweise trägt die Wasserschutzpolizei selbst die für den jeweiligen Sachverhalt geltende Speicherfrist von drei oder fünf Jahren in der Datei ein. Wenn keine späteren Ereignisse zur Verlängerung der Fristen führen, trifft einige Zeit vor Fristablauf eine Liste mit den Fällen ein, die zur Löschung anstehen. Anhand der Liste wird von der Wasserschutzpolizei überprüft, ob Gründe zur Weiterspeicherung vorliegen. Wenn keine Verlängerung erfolgt, wird der Datensatz automatisch bei Fristablauf gelöscht.

Diese Verfahrensweise wird in der Mehrzahl der Fälle eingehalten. Bei der Prüfung haben wir jedoch auch eine Reihe von Speicherungen vorgefunden, die trotz Fristablaufs noch vorhanden waren. In den Löschlisten waren sie nicht aufgeführt.

Als Ursache konnte folgender Ablauf rekonstruiert werden: In den nicht gelöschten Fällen hatten jeweils erkennungsdienstliche Behandlungen stattgefunden, weil die Identität der Betroffenen nicht aufgrund von amtlichen Ausweisen oder Pässen festgestellt werden konnte. Nachdem die Wasserschutzpolizei die Speicherung mit Fristfestlegung vorgenommen hatte, wurden die erkennungsdienstlichen Unterlagen an das Bundeskriminalamt (BKA) übersandt. Das BKA erfaßte die Fingerabdrücke im automatisierten Fingerabdruck-Identifizierungssystem (AFIS) und trug anschließend einen Vermerk über die Tatsache der erkennungsdienstlichen Behandlung im Grenzaktennachweis ein. Die Eintragung dieses Vermerks beim BKA führte dann offenbar dazu, daß die von der Wasserschutzpolizei festgelegte Frist getilgt und eine neue - längere - Frist durch das BKA festgesetzt wurde, obwohl das BKA keine eigenen Erkenntnisse zur betroffenen Person hatte.

Die Polizei hat wegen dieser Verfahrensweise Kontakt mit dem BKA aufgenommen. Das BKA hat mitgeteilt, daß inzwischen keine Vermerke mehr über die erkennungsdienstliche Behandlung aufgrund ausländerrechtlicher Vorschriften eingetragen werden. Somit dürfte das Problem für die Zukunft gelöst sein.

Die Unterlagen, die trotz Fristablaufs bei der Wasserschutzpolizei noch vorlagen, sind inzwischen gelöscht worden. Dem BKA ist eine Liste über diese Fälle übersandt worden, damit dort auch etwaige Eintragungen über erkennungsdienstliche Behandlungen überprüft und gelöscht werden.

15.5 Polizeiliche Datenerhebungen bei der Kontrolle von Schwarzfahrern

15.5.1 Beteiligung der Polizei an Schwerpunktkontrollen

Die Hamburger Hochbahn AG (HHA) führt in letzter Zeit vermehrt schwerpunktmäßige Kontrollen an U-Bahnhöfen durch, ob Fahrgäste im Besitz eines Fahrausweises sind. Hierbei werden über längere Zeiträume sämtliche Ausgänge des jeweiligen U-Bahnhofes kontrolliert, so daß ausnahmslos alle Personen, die den Bahnhof verlassen, überprüft werden. Bei Personen, die keinen Fahrschein haben, das erhöhte Beförderungsentgelt nicht zahlen und sich auch nicht ausweisen können, muß die HHA die Möglichkeit zur Feststellung der Personalien haben. Sie nimmt hierfür die Unterstützung der Polizei in Anspruch.

Wir haben die polizeiliche Datenverarbeitung aus Anlaß einer derartigen schwerpunktmäßigen Kontrolle überprüft, die im Januar 1997 am U-Bahnhof Horner Rennbahn stattgefunden hat. Dabei wurden insgesamt ca. 3500 Personen kontrolliert und 316 "Schwarzfahrer" angetroffen. In 87 Fällen erfolgte eine Personalienfeststellung durch die Polizei. Dies geschah regelmäßig durch Abfragen aus dem Melderegister.

Im Ergebnis haben wir gegen die Beteiligung der Polizei an diesen Kontrollen keine datenschutzrechtlichen Bedenken erhoben. Die Personalienfeststellungen und die Übermittlung der festgestellten Daten an die HHA sind zulässig, um ihr die Durchsetzung ihrer zivilrechtlichen Forderungen nach erhöhtem Beförderungsentgelt zu ermöglichen oder die Stellung von Strafanträgen wegen Leistungserschleichung zu ermöglichen.

Wesentlich in diesem Zusammenhang ist, daß die Inititative zur Personalienfeststellung auch bei derartigen schwerpunktmäßigen Einsätzen von den Hochbahnmitarbeitern ausgeht. Nicht ohne

weiteres zulässig wäre es dagegen, wenn die Polizei aus Anlaß von Fahrkartenkontrollen ohne Ersuchen der Hochbahnmitarbeiter im Einzelfall unterschiedslos von allen Reisenden oder allen "Schwarzfahrern" Personalien feststellen würde. Derartige flächendeckende Identitätsfeststellungen in Form einer sog. "Razzia" würden besondere Tatbestände voraussetzen, z. B. Tatsachen, die die Annahme rechtfertigen, daß an dem kontrollierten Ort Personen Straftaten von erheblicher Bedeutung verabreden, vorbereiten oder verüben. Derartige Tatsachen liegen - jedenfalls regelmäßig - im Bereich von U-Bahnhöfen bei Fahrkartenkontrollen nicht vor.

Auch die aus den polizeilichen Maßnahmen resultierenden Datenspeicherungen hielten sich im Rahmen des Erforderlichen. Insbesondere gab es keine Erfassung der überprüften Personen in polizeilichen Dateien. Die Einzelfälle, in denen Personalien festgestellt worden waren, wurden auf formularmäßig vorbereiteten Meldungen eingetragen, auf denen dokumentiert war, welcher Mitarbeiter der HHA die Überprüfung veranlaßt hat und welche polizeilichen Maßnahmen hierauf erfolgt sind. Die Formulare ermöglichen so, das polizeiliche Handeln im Bedarfsfall nachzuvollziehen. Sie führen aber nicht dazu, daß aus anderen Anlässen mit dem Namen der Betroffenen als Suchbegriff festgestellt werden kann, wann und wo sie sich aufgehalten haben.

15.5.2 Möglichkeiten zur Vereinfachung des Verfahrens

Bei der oben geschilderten Beteiligung der Polizei an Fahrkartenkontrollen beschränkt sich deren Rolle hauptsächlich darauf, anhand von Abfragen aus dem Melderegister die Personalien der überprüften Personen festzustellen und an die HHA weiterzugeben. Dies gilt nicht nur für Schwerpunkteinsätze, sondern auch bei punktuellen Kontrollen. Die HHA schätzt, daß täglich in ca. 50 Fällen eine Personalienfeststellung anhand der Meldedaten erforderlich ist. Seit langem gibt es Überlegungen, ob sich die HHA diesen "Umweg" über die Polizei nicht sparen kann, indem sie selbst aufgrund von Melderegisterauskünften die Personalien überprüft.

Inzwischen haben die Behörde für Inneres und die HHA ein Konzept erarbeitet, das für die Mehrzahl der Fälle zu dieser Vereinfachung des Verfahrens führt. Danach sollen die Kontrolleure ihre Anfragen an eine zentrale Stelle der HHA richten, die sich wiederum an eine Auskunftsbereitschaft des Melderegisters wendet. Durch besondere Vorkehrungen zur Identifizierung wird sichergestellt, daß nur berechtigte Mitarbeiter anfragen können. Da die Meldedienststellen nur werktags zwischen 7.00 und 20.00 Uhr erreichbar sind, soll in den übrigen Zeiten eine besondere Auskunftstelle bei der Polizei tätig werden, die die Anfragen telefonisch beantwortet. Nur wenn die Personalienfeststellung anhand des Melderegisters nicht möglich ist oder wenn die HHA Strafanzeige stellt, wird die Polizei wie bisher eingeschaltet.

Wir haben diesem Konzept im Grundsatz zugestimmt, das einen rationellen Ablauf gewährleistet und die Zeiten verkürzt, in denen die Betroffenen zur Personalienfeststellung festgehalten werden. Auch datenschutzrechtliche Gründe sprechen für die geplante Verfahrensweise: Der unmittelbare Kontakt zum Melderegister vermeidet, daß zusätzliche Verwaltungsvorgänge mit Datenspeicherungen bei der Polizei entstehen. Die zentrale Auskunftstelle bei der Polizei, die außerhalb der Erreichbarkeit der Meldedienststellen tätig wird, soll aus Anlaß der Auskunftserteilung keine Daten erfassen. Die Behörde für Inneres hat bestätigt, daß Auskünfte, die der HHA nicht unmittelbar aus dem Melderegister erteilt werden dürfen (z. B. bei Auskunftssperren), ihr auch nicht mittelbar über die Auskunftstelle der Polizei zugänglich gemacht werden.

Wir haben andererseits deutlich gemacht, daß das Konzept und insbesondere die Einrichtung der besonderen Auskunftstelle bei der Polizei nur für die besonderen Bedarfe der HHA im

Zusammenhang mit Fahrkartenkontrollen gelten kann und nicht auf andere Unternehmen übertragbar ist.

15.6 Sonstiges

Bei der Polizei wurden neben den oben genannten unter anderem folgende Dateien überprüft:
- Intensivtäterdatei
- Datei Graffiti.

16. Staatsanwaltschaft

16.1 Automation bei der Staatsanwaltschaft

Die von Hamburg gemeinsam mit Brandenburg, Hessen und Schleswig-Holstein betriebene Entwicklung eines automatisierten Verfahrens zur Vorgangsbearbeitung bei der Staatsanwaltschaft (sogenannte Mehrländer-Staatsanwaltschafts-Automation - MESTA) hat im Jahr 1997 zwar erhebliche Fortschritte gemacht. Bei Redaktionsschluß war allerdings noch kein Verfahrensteil eingeführt.

Es ist geplant, die erste Pilotanwendung im Bereich der bisherigen Zentralkartei zu installieren, in der die Grunddaten zu allen bei der Staatsanwaltschaft vorliegenden Verfahrensakten mit Angaben zur Person des Beschuldigten, zum Aktenzeichen, zum strafrechtlichen Vorwurf und zum Verfahrensausgang erfaßt werden. Die inhaltliche Bearbeitung staatsanwaltschaftlicher Ermittlungsvorgänge wird erst durch künftige Module des Automationsverfahrens unterstützt.

Unsere Beteiligung an dem Projekt hat sich auf folgende Fragen konzentriert, die jedoch bisher nicht befriedigend geklärt werden konnten:

Entgegen der ursprünglichen Ankündigung (15. TB, 16.2) ist immer noch keine Festlegung der Zugriffsbefugnisse erfolgt, die nach Zuständigkeiten und Personenrollen differenziert. Wir haben wiederholt den Grundsatz deutlich gemacht, daß es verfahrensübergreifende Zugriffe nur auf Daten von Beschuldigten geben kann, während die Daten von Tatopfern, Anzeigenerstattern und Zeugen nur im Rahmen der Zuständigkeit für die jeweiligen Ermittlungsverfahren angezeigt werden dürfen. Die Einführung von MESTA-Modulen zur Vorgangsbearbeitung ohne die Festlegung derart differenzierter Zugriffsbefugnisse darf es nicht geben.

In engem Zusammenhang mit der Vergabe von Zugriffsbefugnissen steht die Frage, ob Dateizugriffe protokolliert werden. Wir haben deutlich gemacht, daß kein Bedarf für Protokollierungen von Zugriffen besteht, die sich im Rahmen der aktuellen Zuständigkeit für ein bestimmtes Ermittlungsverfahren bewegen. Zugriffe auf den Bestand der bisherigen Zentralkartei, die nicht von einer Verfahrenszuständigkeit für den konkreten Einzelfall abhängig sind (Auskunftsfunktion), sollen dagegen protokolliert werden. Mit dem Projekt ist im Sommer 1997 vereinbart worden, daß die mit der Programmierung beaufragte Stelle ein Konzept vorlegt, aus dem der Aufwand für die Protokollierung der umfassenden Auskunftsfunktion ersichtlich ist. Auf dieser Grundlage sollte dann entschieden werden, ob die Protokollierung erfolgt. Bis zum Redaktionsschluß lag das Konzept jedoch nicht vor.

Im Verfahren MESTA sollen verschiedene Funktionen für Auswertungen und insbesondere Statistiken aufgrund der Datenbank fest installiert werden. Darüber hinaus gibt es Überlegungen, ein Werkzeug für freie, nicht vordefinierte Auswertungen zu benutzen. Man will sich die

unbegrenzte Möglichkeit zur Auswertung aller Daten nach allen in der Datenbank erfaßten Kriterien offenhalten.

Wir haben hierzu deutlich gemacht, daß der Einsatz einer derartigen "Data-Warehouse"-Funktion nur insoweit datenschutzrechtlich unkritisch ist, als die Auswertungsergebnisse keine Rückschlüsse auf personenbezogene Daten zulassen. Wenn dagegen als Ergebnis der Auswertung Listen mit Namen oder Aktenzeichen herauskommen, für die irgendwelche denkbaren Suchkriterien bestimmend sind (z. B. Beruf oder Herkunft von Tatopfern), werden nicht nur die erforderlichen Zugriffsbeschränkungen unterlaufen. Es wird auch vernachlässigt, daß die Anlegung einer staatsanwaltschaftlichen Datenbank allein zur Verfolgung von Straftaten gerechtfertigt ist. Sie stellt dagegen keinen "Datenpool" für personenbezogene Auswertungen dar, die auf politischen oder sonstigen strafverfahrensfremden Vorgaben beruhen. Eine Entscheidung, ob und unter welchen Voraussetzungen ein besonderes Auswertungsprogramm eingesetzt wird, war bei Redaktionsschluß noch nicht getroffen.

16.2 Neue Befugnisse zur Überwachung der Telekommunikation

16.2.1 Neue Regelungen

Im Rahmen der Neuregelung des Telekommunikationsrechts sind auch neue Rechtsvorschriften erlassen worden oder geplant, die die Befugnisse der Staatsanwaltschaft sowie von Polizeien und Nachrichtendiensten betreffen:

- Das Telekommunikationsgesetz (TKG) begründet die Mitwirkungspflichten der Betreiber von Telekommunikationsanlagen an Überwachungsmaßnahmen. Es verpflichtet zur Auskunftserteilung über Bestandsdaten und regelt den Zugriff auf Kundendateien.

- Im Teledienstedatenschutzgesetz (TDDSG) und im Postgesetz (vgl. 23.1) sind besondere Auskunftspflichten an Staatsanwaltschaften, Polizeien und Nachrichtendienste über Bestandsdaten nach dem Vorbild des TKG ursprünglich geplant gewesen, aber aufgrund der Kritik der Datenschutzbeauftragten schließlich ebenso wie im Mediendienstestaatsvertrag (MDStV) unterblieben.

- Im Begleitgesetz zum Telekommunikationsgesetz (TKG-Begleitgesetz) ist entsprechend der Forderung der Datenschutzbeauftragten keine Befugnis zur Aufzeichnung von Aktivmeldungen im Mobilfunk für sogenannte "Bewegungsbilder" geschaffen worden. Die beabsichtigte Neuregelung der Auskunftserteilung über Verbindungsdaten zu Zwecken der Strafverfolgung (vgl. 15. TB, 16.1) ist erneut verschoben worden. Der bisherige § 12 Fernmeldeanlagengesetz soll bis zum 31. Dezember 1999 fortgelten.

Wir haben uns zu diesen Einzelfragen in den jeweiligen Gesetzgebungsverfahren ausführlich geäußert. Eine Darstellung der Problematik kann an dieser Stelle unterbleiben, da sie in der vom Hamburgischen Datenschutzbeauftragten gemeinsam mit dem Datenschutzbeauftragten des debis Systemhauses herausgegebenen Broschüre "Datenschutz bei Multimedia und Telekommunikation" erfolgt ist. Auf das Kapitel dieser Broschüre über die "Befugnisse der Sicherheitsbehörden nach neuem Telekommunikationsrecht" wird insoweit verwiesen.

16.2.2 Neue Überwachungstechnik

In seiner Stellungnahme zum Entwurf eines TKG-Begleitgesetzes überraschte der Bundesrat mit einer bisher unbekannten Forderung: Eine Anordnung zur Überwachung der Telekommunikation

sollte dazu berechtigen, durch technische Maßnahmen die zu einem Funktelefon gehörige Identitätsnummer festzustellen und dadurch die Handy-Rufnummer zu erfahren. Dies sollte auch möglich sein, wenn dabei das Fernmeldegeheimnis unbeteiligter Dritter technisch unvermeidbar beeinträchtigt würde.

Hinter dieser Forderung verbarg sich der Wunsch, ein bisher nicht zugelassenes Gerät mit der Bezeichnung "IMSI-Catcher" zu legitimieren. Die Funktionsweise dieses "IMSI-Catchers" läßt sich wie folgt skizzieren: Funktelefone müssen sich immer bei den jeweils nächsten Basisstationen der Netzbetreiber anmelden, um für eingehende Gespräche erreichbar zu sein. Dies geschieht mit der sogenannten "IMSI" (International Mobile Subscriber Identity), der netzinternen Kennung des jeweiligen Teilnehmers. Der "IMSI-Catcher" schaltet die jeweils nächste Basisstation aus und baut stattdessen eine eigene Funkzelle auf. Die Funktelefone teilen nun ihre "IMSI" dem "Catcher" mit. Auf diese Weise wird die bisher nicht bekannte netzinterne Kennung des Teilnehmers ermittelt. Allerdings bewirkt die Manipulation nicht nur, daß sich ein bestimmtes gesuchtes Funktelefon beim "IMSI-Catcher" anmeldet, vielmehr werden sämtliche Handys im Umkreis des "IMSI-Catchers" eingefangen.

Um den eigentlich gesuchten Anschlußinhaber zu ermitteln, können Gespräche der einzelnen Funktelefone nacheinander abgehört werden. Der "IMSI-Catcher" wird hierfür vom sogenannten "Fangmodus" in den "Abhörmodus" umgeschaltet, wofür ein einfacher Softwarewechsel ausreicht. Das abzuhörende Handy wird vom "IMSI-Catcher" veranlaßt, unverschlüsselt mit ihm zu kommunizieren. Für das abgehörte Handy sind allerdings nur abgehende Gespräche möglich, eingehende Anrufe werden blockiert. Die übrigen gefangenen Handys können in diesem Zeitraum weder Gespräche empfangen noch absenden.

Wir haben uns entschieden gegen die Überlegungen gewandt, eine rechtliche Grundlage für den Einsatz dieses "IMSI-Catchers" zu schaffen. Die herkömmliche Abhörtechnik setzt die Begrenzung der Abhörmaßnahme auf bestimmte Anschlüsse voraus. Damit wird vermieden, daß Anschlüsse in die Abhörmaßnahme einbezogen werden, die gar nicht gemeint sind. Der "IMSI-Catcher" zieht dagegen zwangsläufig alle in seinem Umkreis befindlichen Anschlüsse in die Abhörmaßnahme ein.

Die Identifizierung des gesuchten Anschlusses durch Abhören führt in unvertretbarem Maße zu Eingriffen in das Fernmeldegeheimnis völlig unbeteiligter Personen, die weder den Anschluß des Verdächtigen benutzen, noch mit ihm kommunizieren. Dies kann nicht als unvermeidbare Beeinträchtigung verniedlicht werden. Auch wenn die Identifizierung des gesuchten Anschlusses nicht durch Abhören erfolgt, müssen Unbeteiligte über die Erfassung ihrer Rufnummern hinaus damit rechnen, daß weitere Ermittlungen zu ihrer Person angestellt werden, um herauszufinden, wer aus der Gruppe der registrierten Mobiltelefon-Nutzer der Gesuchte ist.

Die einfachen Möglichkeiten, beim Einsatz des "IMSI-Catchers" zwischen "Fangmodus" und "Abhörmodus" umzuschalten, lassen befürchten, daß Telefonate regelmäßig als Eilmaßnahme abgehört werden, bevor die richterliche Anordnung vorliegt, was bisher die seltene Ausnahme war. Die Arbeitsteilung zwischen Strafverfolgungsbehörden und Netzbetreibern bei herkömmlichen Abhörmaßnahmen gewährleistete durch ein faktisches "Mehraugen-Prinzip" eine wirksame Mißbrauchskontrolle. Wenn die Netzbetreiber dagegen durch den "IMSI-Catcher" ausgeschaltet werden und nicht einmal feststellen können, ob und wo sich ein "IMSI-Catcher" im Einsatz befindet, entfällt auch diese Schutzvorkehrung.

Die Netzbetreiber selbst haben darauf hingewiesen, daß der Betrieb von "IMSI-Catchern" erhebliche technische Probleme für sie auslöst: z. B. ist eine gezielte Freigabe gefangener aber nicht abzuhörender Handys nicht möglich; auch das Auflösen der vom "IMSI-Catcher" aufgebauten

illegalen Funkzelle beendet die Blockade der betroffenen Handys nicht. Damit wird die technische Integrität des Netzes gefährdet und dessen Verfügbarkeit für die Nutzer eingeschränkt, die z. B. nicht einmal einen Notruf abgeben können.

Nicht zuletzt spricht gegen den Einsatz des "IMSI-Catchers", daß er den Bedarf der Strafverfolgungsbehörden zur Identifizierung bisher unbekannter Netzteilnehmer nicht erfüllen kann. Zur Begründung wurde im Bundesrat angeführt, daß er eingesetzt werden soll, wenn Verdächtige (z. B. Drogenhändler) über eine Guthabenkarte für ein Handy verfügen, bei der sie sich nicht gegenüber den Netzbetreibern zu Abrechnungszwecken identifizieren müssen. Um das Guthaben nicht binnen kurzem zu verbrauchen, benutzen sie ihr Handy nur, um Gespräche zu empfangen. Es gibt somit keine Informationen über den Nutzer in Kundenverzeichnissen. Man meint nun, mit dem "IMSI-Catcher" weiterzukommen. Doch dies wird nicht gelingen, da der "IMSI-Catcher" alle eingehenden Anrufe blockiert und nur ausgehende Telefonate abhören kann.

Die Forderung des Bundesrates, Regelungen für den Einsatz des "IMSI-Catchers" zu schaffen, ist im Gesetzgebungsverfahren zum TKG-Begleitgesetz vom Bundestag nicht aufgegriffen worden. Die Bundesregierung hat allerdings angekündigt, daß sie den Einsatz von "IMSI-Catchern" zur Ermittlung technischer Identifikationsmerkmale als Ersatz für unbekannte Rufnummern - also ohne Abhörfunktion - anstrebt und prüfen werde, ob es hierfür einer Änderung der Strafprozeßordnung bedarf. Bisher sind allerdings "IMSI-Catcher", die keine Abhörfunktion ermöglichen und die beschriebenen negativen Auswirkungen vermeiden, nicht bekannt geworden.

Zu berücksichtigen ist, daß die vorhandene Technik auch von unberechtigten Privatpersonen mißbraucht werden kann, was dann zu den beschriebenen massiven Eingriffen in das Fernmeldegeheimnis und den negativen Auswirkungen auf die Netzsicherheit führen würde. Aus datenschutzrechtlicher Sicht anzustreben ist daher eine Änderung des einheitlichen europäischen Mobilfunk-Standards (GSM) dahingehend, daß sich auch die Basisstation gegenüber dem Handy authentifizieren muß, um so das Vortäuschen einer illegalen Basisstation durch den "IMSI-Catcher" auszuschließen. Falls dies nicht erreichbar ist, könnte jedenfalls eine Anzeige auf dem Handy weiterhelfen, wenn Gespräche unverschlüsselt übertragen werden.

16.3 Auskünfte an Betroffene über den Inhalt von Führungszeugnissen für Behörden

Immer wieder wenden sich Bürger an uns, weil es Unklarheiten über den Inhalt von Führungszeugnissen gibt. Führungszeugnisse werden ausschließlich vom Bundeszentralregister erteilt. Wenn Eintragungen vorhanden sind, handelt es sich in aller Regel um rechtskräftige Verurteilungen durch Strafgerichte; daneben können bestimmte Verwaltungsentscheidungen (z. B. Paßversagungen oder waffen- und gewerbrechtliche Entscheidungen) im Bundeszentralregister eingetragen werden. In keinem Fall handelt es sich um polizeiliche Verdachtsspeicherungen; diese nimmt die Polizei in ihren eigenen Dateien vor, die rechtlich und tatsächlich völlig selbständig vom Bundeszentralregister bestehen. Der allgemein gebräuchliche Begriff des "polizeilichen Führungszeugnisses" ist also unzutreffend und führt häufig zu falschen Vorstellungen.

Unproblematisch ist das Führungszeugnis für Private. Es wird bei der örtlichen Meldebehörde beantragt, die die Identität des Antragstellers überprüft. Das Bundeszentralregister sendet es dann direkt an den Betroffenen. In dieses Führungszeugnis, das z. B. zur Vorlage bei einem privaten Arbeitgeber benutzt wird, werden eine Reihe von Eintragungen im Bundeszentralregister nicht aufgenommen: z. B. Verwarnungen mit Strafvorbehalt; geringfügige Geld- oder Freiheitsstrafen, die zur Bewährung ausgesetzt wurden, wenn keine weitere Strafe eingetragen ist.

Daneben gibt es das Führungszeugnis zur Vorlage bei Behörden. Es hat gegenüber dem Führungszeugnis für Private einen erweiterten Inhalt. Z. B. gibt es auch Auskunft über geringfügige Strafen, die nicht in ein Führungszeugnis für Private aufgenommen werden, wenn es sich um Straftaten handelte, die bei der Ausübung eines Gewerbes begangen wurden und das Führungszeugnis für die behördliche Entscheidung über eine Gewerbeerlaubnis dienen soll. Diese Führungszeugnisse für Behörden werden zwar von den Betroffenen beantragt, aber nicht ihnen, sondern nur der Behörde übersandt.

Dies führt bei Betroffenen nicht selten zu der Vermutung, das Führungszeugnis habe irgendeinen "geheimen" Inhalt, den sie nicht erfahren könnten. Die Vermutung ist unzutreffend. Vielmehr haben die Betroffenen verschiedene Möglichkeiten, auch den Inhalt behördlicher Führungszeugnisse zu erfahren. Zum einen können sie das Führungszeugnis bei der Behörde einsehen, an die es adressiert wird. Wenn sie es einsehen wollen, bevor es an die Behörde gesandt wird, können sie verlangen, das es zunächst an ein von ihnen benanntes Amtsgericht geschickt wird, wo sie Einblick nehmen und entscheiden können, ob es an die Behörde weitergeleitet wird. Diese Möglichkeit besteht allerdings nur dann, wenn das Führungszeugnis Eintragungen enthält.

Ferner hat die Behörde die Möglichkeit, ohne Beteiligung der Betroffenen ein Führungszeugnis anzufordern. Voraussetzung ist, daß sie es zur Erledigung hoheitlicher Aufgaben benötigt und eine Aufforderung an den Betroffenen, ein Führungszeugnis vorzulegen, nicht sachgemäß ist oder erfolglos bleibt. Dieses Führungszeugnis können Betroffene nur bei der Behörde einsehen.

Schließlich gibt es die sogenannte unbeschränkte Auskunft aus dem Bundeszentralregister. Sie umfaßt alle im Register vorhandenen Eintragungen, insbesondere auch solche, die nach Fristablauf getilgt - aber nicht im datenschutzrechtlichen Sinne gelöscht - worden sind. Die Tilgung führt also nur dazu, daß die Eintragung nicht mehr im Führungszeugnis erscheint, im Register bleibt sie gespeichert. Zur Einholung einer unbeschränkten Auskunft sind u. a. die Gerichte, die Staatsanwaltschaften, die Kriminalpolizei, die Verfassungsschutzbehörden und oberste Bundes- und Landesbehörden berechtigt.

Auch die Betroffenen selbst können eine umfassende Auskunft über sämtliche im Bundeszentralregister über sie gespeicherten Daten erhalten. Hierzu müssen sie ein Amtsgericht benennen, wo sie die Auskunft einsehen können. Nach der Einsichtnahme wird die Auskunft vom Amtsgericht vernichtet. Dieses Verfahren gewährleistet, daß die umfassende Auskunft nicht im privaten Rechtsverkehr verwendet werden kann. Andernfalls bestünde die Gefahr, daß z. B. private Arbeitgeber von ihren Mitarbeiteren die Vorlage einer umfassenden Auskunft verlangen (vgl. 14. TB, 15.3.1). Hiermit würden sämtliche Beschränkungen des für Private vorgesehenen Führungszeugnisses umgangen.

17. Justiz

17.1 Bild-Ton-Aufzeichnungen von Vernehmungen im Strafverfahren

Die Datenschutzbeauftragten des Bundes und der Länder haben am 23./24. Oktober 1997 auf unseren Vorschlag eine Entschließung über "Informationelle Selbstbestimmung und Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren" gefaßt. Diese Entschließung nimmt zu wesentlichen Gesichtspunkten der aktuellen rechtspolitischen Diskussion über den Schutz insbesondere von kindlichen Opferzeugen in Verfahren wegen Sexualstraftaten Stellung.

Bild-Ton-Aufzeichnungen von Vernehmungen, die in der Hauptverhandlung zu Beweiszwecken abgespielt werden, können die psychische Belastung der Aussagepersonen und Beeinträchtigungen der Beweisqualität, die bei wiederholter Vernehmung drohen, deutlich verringern. Andererseits stellen Bild-Ton- Aufzeichnungen einen erheblichen Eingriff in das Persönlichkeitsrecht dar. Sie spiegeln die unmittelbare Betroffenheit der vernommenen Personen in Mimik und Gestik umfassend wider.

Die Datenschutzbeauftragten fordern deshalb wirksame Vorkehrungen zum Schutz des Persönlichkeitsrechts bei der Verwendung von Bild-Ton-Aufzeichnungen. Sollen diese nicht zu Dokumentationszwecken, sondern im Interesse der Aussagepersonen selbst angefertigt werden, bedarf es hierfür deren Einwilligung nach umfassender, zuverlässig zu dokumentierender Aufklärung.

In jedem Falle sind die Aufzeichnungen so zu verwenden, daß der Eindruck des Aussagegeschehens nicht gezielt verfremdet oder verzerrt wird, z. B. durch Zeitlupe, Zeitraffer, Einzelbildabfolge, Standbild oder Zoom. Hat der Zeuge sich auf sein gesetzliches Zeugnisverweigerungsrecht berufen, ist eine weitere Nutzung der Aufnahme weder zu Beweiszwecken noch als gedächtnisunterstützender Vorhalt zulässig. Soweit der Gesetzgeber eine Weitergabe von Videokopien an Verfahrensbeteiligte, insbesondere zu Verteidigungszwecken, und eine Aufbewahrung der Aufzeichnungen nach rechtskräftigem Abschluß des Strafverfahrens überhaupt zuläßt, darf dies nur in engen Grenzen und mit strikter Zweckbindung erfolgen.

17.2 Sonstiges

Berlin hat im Bundesrat einen Gesetzesantrag zur Einführung des elektronisch überwachten Hausarrests bei Strafgefangenen mit kurzzeitiger Verbüßungsdauer eingebracht (Bundesrats-Drucksache 698/97).

Bei einer etwaigen landesrechtlichen Umsetzung sollte die grundlegende Entscheidung über den elektronisch überwachten Hausarrest wegen seiner weitreichenden Auswirkungen für die Intimsphäre der Gefangenen und ihrer Angehörigen von der Bürgerschaft getroffen werden.

Bereits im vorangehenden Gesetzgebungsverfahren des Bundes sind die Ausgestaltung und die Rechtswirkungen dieses neuen Vollzugsinstruments datenschutzrechtlich zu klären. Dies gilt insbesondere mit Blick auf die erforderliche gesetzliche Grundlage für Hausbesuche zur Nachtzeit sowie für Blut- und Urinkontrollen. Sicherzustellen wäre auch, daß der Staat im Falle einer späteren Aufhebung der strafgerichtlichen Verurteilung verschuldensunabhängig eine Entschädigung für Nachteile infolge des Hausarrests zu leisten hat.

18. Gesundheitswesen

18.1 Outsourcing von Krankenhausaufgaben

Aus finanziellen und Platz-Gründen bemühen sich Krankenhäuser zunehmend, eigene Aufgaben durch Dritte durchführen zu lassen (15. TB, 19.3). Dies gilt etwa für die Zusammenarbeit mit externen Labors, die externe Archivierung von Patientenakten, die Mikroverfilmung von Akten, die Datenträgervernichtung und die Wartung von EDV-Anlagen. In der Diskussion ist auch die Wahrnehmung der Aufgaben des betrieblichen Datenschutzbeauftragten durch krankenhausfremde Personen.

18.1.1 Ärztliche Schweigepflicht

Die Patientendaten im Krankenhaus unterliegen dem besonderen Schutz der ärztlichen Schweigepflicht, § 203 Strafgesetzbuch (StGB). Dieser Schutz wirkt fort im strafprozessualen Zeugnisverweigerungsrecht von Ärzten und im Verbot, ärztliche Unterlagen über beschuldigte Patienten zu beschlagnahmen.

§ 203 Abs. 1 StGB bedroht die Person mit Strafe, die als Arzt oder sein "berufsmäßig tätiger Gehilfe" "unbefugt ein fremdes Geheimnis ... offenbart". Eine Offenbarung liegt bereits dann vor, wenn einem Dritten ein ungehinderter Zugang und Zugriff auf die Daten ermöglicht wird; einer direkten Datenübergabe durch den Arzt bedarf es also nicht.

Ob ein solches Offenbaren durch das Krankenhauspersonal "unbefugt" oder befugt erfolgt, richtet sich nach dem jeweiligen Krankenhausgesetz des Landes. Die allgemeinen Regelungen der Datenschutzgesetze zur Datenübermittlung und Auftragsdatenverarbeitung bilden keine ausreichende Befugnisnorm, da sie den besonderen Schutz durch § 203 StGB nicht berücksichtigen. Die bereichsspezifischen Datenschutzvorschriften im Hamburgischen Krankenhausgesetz (HmbKHG) beziehen sich dagegen ausdrücklich auf den Patientendatenschutz und kommen damit als Befugnisnormen im Sinne des
§ 203 StGB in Betracht. Die gegenteilige Rechtsauffassung des Oberlandesgerichts Düsseldorf (Urteil vom 6. August 1996), ein Landesgesetz könne keine Befugnisnorm für § 203 StGB (Bundesgesetz) sein, entspricht nicht der herrschenden Meinung.

18.1.2 Auftragsdatenverarbeitung oder Datenübermittlung

Entscheidend für die datenschutzrechtliche Beurteilung der auszugliedernden Krankenhausaufgabe nach dem HmbKHG ist: Handelt es sich um eine Funktionsübertragung mit eigenen Gestaltungs- und Entscheidungsrechten des Empfängers oder um eine streng weisungsgebundene, nur umsetzende Auftragsdatenverarbeitung für das Krankenhaus? Eine Auftragsdatenverarbeitung wird in § 9 HmbKHG grundsätzlich zugelassen. Eine "Funktionsübertragung" stellt dagegen eine Datenübermittlung dar, deren Zulässigkeit § 11 HmbKHG an wenige, abschließend genannte Übermittlungszwecke bindet.

Die Inanspruchnahme fremder Laborleistungen ist jedenfalls dann eine bloße Auftragsdatenverarbeitung, wenn es sich um ein weitgehend automatisiertes Massen- und Routinegeschäft handelt, das keine fachkompetente ärztliche Bewertung im externen Labor erfordert; eine ggf. später notwendige Bewertung durch den behandelnden Arzt ändert daran nichts. Die externe Archivierung von Patientenakten einschließlich der Herausgabe und Vernichtung nach festen schriftlichen Vorgaben des Auftraggebers ist ebenso als Auftragsdatenverarbeitung zu bewerten wie auch die Mikroverfilmung von Akten und die Datenträgervernichtung. Die Vergabe von Wartungsarbeiten oder Hilfstätigkeiten bei der Datenverarbeitung ist nach § 3 Abs. 4 HmbDSG ebenfalls wie eine Auftragsdatenverarbeitung zu behandeln.

18.1.3 Externe betriebliche Datenschutzbeauftragte

Anders zu beurteilen ist dagegen das Outsourcing der Aufgabe des betrieblichen Datenschutzbeauftragten: Seine Kontroll- und Prüfrechte, Schulungspflichten und Beratungsaufgaben sind nur mit eigener Entscheidungs- und Gestaltungsfreiheit denkbar.

Die Übermittlung von Patientendaten zum Zwecke der betrieblichen Datenschutzkontrolle ist jedoch in § 11 HmbKHG nicht vorgesehen. (Die Übermittlung von Patientendaten an den

Hamburgischen Datenschutzbeauftragten bzw. an die Aufsichtsbehörde für den Datenschutz ist dagegen nach § 11 Nr. 9 HmbKHG zulässig.)

Die in der datenschutzrechtlichen Literatur vertretene Auffassung, der betriebliche Datenschutzbeauftragte eines Krankenhauses sei "berufsmäßig tätiger Gehilfe" des Arztes, also selbst der ärztlichen Schweigepflicht unterworfen, und könne deswegen auch eine externe Person sein, teilen wir nicht: Ein externer Datenschutzbeauftragter wird gerade nicht Teil der speichernden Stelle (des Krankenhauses), eine Offenbarung von Patientendaten ihm gegenüber bleibt vielmehr eine Übermittlung und Offenbarung im Sinne des § 203 StGB und bedarf deswegen einer besonderen Befugnis.

Eine große Wirtschaftsberatungsgesellschaft, die auch Krankenhäusern die Übernahme der Funktion eines betrieblichen Datenschutzbeauftragten anbietet, argumentiert umgekehrt: Die Funktionsübertragung sei zulässig, weil ein Zugriff auf Patientendaten nicht erfolge. Angesichts der weitreichenden gesetzlichen Aufgaben eines betrieblichen Datenschutzbeauftragten erscheint auch dies nicht richtig: Eine Kontrolle etwa der Aufnahmedaten oder der Datenübermittlung an die Krankenkassen umfaßt zumindest Stichproben mit Echtdaten.

Die Übertragung der Funktion eines betrieblichen Datenschutzbeauftragten auf eine externe Person kann zwar durchaus Vorteile haben (Stichworte: Datenschutz als eigene Berufsaufgabe, Erfahrung, Kompetenz und Unabhängigkeit). Nach Auffassung des Hamburgischen Datenschutzbeauftragten läßt die gegenwärtige Rechtslage eine solche Übertragung wegen der ärztlichen Schweigepflicht jedoch nicht zu.

18.1.4 Datensicherungsmaßnahmen bei Auftragsdatenverarbeitung

Anders ist es bei der Auftragsdatenverarbeitung, etwa durch externe Labors, krankenhausferne private Archiv- oder Mikrofilm-Unternehmen und Aktenvernichter. Hier sind nach § 9 HmbKHG die Datensicherungsmaßnahmen entscheidend. Sie sind im schriftlichen Auftrag im einzelnen festzulegen. Soweit technisch möglich und medizinisch wie wirtschaftlich vertretbar, ist den Auftragnehmern eine Einsichtnahme in die Patientendaten zu verwehren.

Folgende Fälle kommen häufig vor:

- externe Labors

  Bei der Inanspruchnahme fremder Laborleistungen ist zu prüfen, ob der Name des Patienten, dessen Blut- oder Gewebeprobe untersucht wird, für die Zuordnung erforderlich ist. So wird in Laborgemeinschaften niedergelassener Ärzte häufig nur mit Patienten-Nummern bzw. Barcodes gearbeitet, ohne daß Fälle fehlerhafter Zuordnung bekannt geworden sind. Auch bei der massenweisen Laboruntersuchung von Blutproben von Asylbewerbern wurden gegen die Codierung der Namen keine medizinischen Einwände erhoben. In individuellen Behandlungsfällen mag dies anders sein. Notwendig ist jeweils die gesonderte Prüfung, ob dem externen Labor der Patientenname mitgeteilt werden muß, wie sich aus der allgemeinen Prüfungspflicht gemäß dem neuen § 5 Abs. 4 HmbDSG ergibt.

- Mikroverfilmung

  Bei der Mikroverfilmung ist eine Einsichtnahme in die Patientenakten kaum vermeidbar. Hier sind als flankierende Maßnahme erhöhte Anforderungen zu stellen an die

Transportkontrolle, ggf. die Aufsicht durch Krankenhauspersonal und einen möglichst kurzfristigen Verbleib der Patientenakten in den Räumen des Auftragnehmers.

- Aktenvernichtung

  Bei der Aktenvernichtung ist ebenfalls die Form der Anlieferung und die Art der Vernichtung, aber auch die Frist zwischen beiden bedeutsam. Das notwendige Vernichtungsprotokoll des Auftragnehmers sollte diese Zeiten, ferner die Menge und Art der vernichteten Akten festhalten.

- EDV-Wartung

  Bei der EDV-Wartung durch externe Unternehmen sind alle technischen und organisatorischen Möglichkeiten auszuschöpfen, die einen Zugriff auf Patientendaten auf zwingend erforderliche Fälle beschränken. Solche Maßnahmen können sein: Gestaffelte Zugriffsrechte auf das System, Wartung zunächst nur mit Testdaten, Löschung der Patientendaten (nach Sicherungskopie) bei Wartung außerhalb des Krankenhauses, Abkoppelung des PC vom Netz vor einer Wartung.

  Zusätzliche Maßnahmen sind bei der Einrichtung einer Fernwartung über Datenleitung zu treffen. Ein Zugriff per Fernwartung muß immer vom Auftraggeber initiiert, gesteuert und am Bildschirm begleitet werden. Die Wartung ist zu protokollieren.

- externe Archivierung

  Bei der externen Archivierung von Patientenakten ist wegen der langen Lagerungszeit vor allem darauf zu achten, daß Patientendaten während der Archivierung nicht gezielt ausgeforscht werden können - also etwa nach dem Namen des (z. B. prominenten) Patienten. Damit kann auch ein gewisser Ausgleich dafür geschaffen werden, daß das Beschlagnahmeverbot von ärztlichen Unterlagen nicht mehr gilt, sobald die Unterlagen das Krankenhaus verlassen haben.

  Als Schutzmaßnahme bietet sich hier an, die Patientenakten bereits im Krankenhaus ausschließlich mit einem verschlüsselten Kennzeichen zu versehen, das einen Personenbezug für Dritte ausschließt. Übernimmt der Auftragnehmer die so ausgezeichneten Akten, kann weder er noch ein unbefugter Dritte (und auch kein Staatsanwalt oder Polizist) die Unterlagen eines bestimmten Patienten heraussuchen. Die Entschlüsselung ist nur dem Krankenhaus möglich - etwa zur Anforderung benötigter Akten. Die Entschlüsselungs-Software bzw. -Liste ist im Krankenhaus "beschlagnahmefest".

  Ein weiteres Schutzniveau wird erreicht, wenn die einzelnen Patientenakten in Umschlägen bzw. Behältnissen verwahrt werden, die allein das verschlüsselte Kennzeichen tragen, durch eine Öffnung zerstört werden und nur vom Krankenhaus wieder zu beschaffen sind. Eine andere mögliche Lösung ist die Verwahrung mehrerer / vieler Akten in Containern, die von Krankenhaus-Mitarbeitern gefüllt und abgeschlossen und bei Bedarf nur als ganzes angefordert und wieder geöffnet werden. Diese Datensicherung wird in anderen Bundesländern bereits praktiziert.

Bei allen Plänen, Krankenhausaufgaben an Dritte zu vergeben, ist eine Beratung mit dem Hamburgischen Datenschutzbeauftragten schon deshalb zu empfehlen, weil sie kostspieligen späteren Datensicherungsmaßnahmen vorbeugen kann.

18.2 Arztpraxis-EDV

Seit 1996 haben wir als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich den EDV-Einsatz in Arztpraxen näher untersucht. Das Thema ist aber auch für den Datenschutz im öffentlichen Bereich von Bedeutung, da Praxis-Software auch in Ambulanzen der staatlichen Krankenhäuser verwendet wird.

In Prüfungen und Beratungsgesprächen in Arztpraxen, durch eine schriftliche Befragung von Software-Herstellern und durch Kontakte zur Kassenärztlichen Vereinigung Hamburg und zu Ärzteverbänden haben wir ein Bild gewonnen, das eine ganze Reihe von Schwachstellen und Defiziten hinsichtlich des Patientendatenschutzes offenbart.

Besondere Aktualität gewann das Thema im Juli 1997 durch eine Fernsehsendung, in der ein EDV-Wartungsunternehmen für Arztpraxis-Software verdächtigt wurde, als verlängerter Arm einer Sekte auf Patientendaten zuzugreifen. Auch wenn dies nicht bewiesen wurde, zeigten unsere Untersuchungen, daß ein solches Mißbrauchs-Szenario technisch keineswegs realitätsfremd ist.

In einer Pressekonferenz im Juni 1997 und mit einem Vortrag bei der "Sommerakademie 97: Computermedizin und Patientengeheimnis" des schleswig-holsteinischen Datenschutzbeauftragten haben wir unsere Erkenntnisse veröffentlicht. Die Fortbildungsakademie der Ärztekammer Hamburg lud uns zum 12. November 1997 zu einer Sonderveranstaltung "Computertechnik in der Arztpraxis und die Problematik des Datenschutzes" ein. Wegen geringen Interesses mußte die Veranstaltung abgesagt werden.

18.2.1 Datenschutzrecht für die Praxis-EDV

Patientendaten in EDV-Systemen für Arztpraxen unterliegen der ärztlichen Schweigepflicht, wie sie den Ärzten in der Berufsordnung auferlegt und durch § 203 StGB abgesichert wird (siehe oben 18.1.1). In § 2 der Berufsordnung wird eine Offenbarung von Patientendaten nur dann zugelassen, wenn sie aufgrund einer gesetzlichen Befugnisnorm, einer Schweigepflichtentbindung durch den Patienten oder "zum Schutz eines höherwertigen Rechtsguts" erfolgt. Dies gilt auch für die Kommunikation unter Ärzten - selbst in einer Gemeinschaftspraxis. Eine gesetzliche Befugnisnorm zur Datenübermittlung "auf maschinell verwertbaren Datenträgern" gibt z. B. § 295 Sozialgesetzbuch V, der die Abrechnung der Vertragsärzte mit der Kassenärztlichen Vereinigung regelt.

Ärztliche Aufzeichnungen auf elektronischen Datenträgern - also die Verwendung von Praxis-EDV - bedürfen nach § 11 Abs. 5 der Berufsordnung "besonderer Sicherungs- und Schutzmaßnahmen, um deren Veränderung, Vernichtung oder unrechtmäßige Verwendung zu verhindern".

Auch das Datenschutzrecht fordert in § 9 Bundesdatenschutzgesetz (BDSG) technisch-organisatorische Maßnahmen zur Gewährleistung der Datensicherheit. Die Anlage zu dieser Vorschrift nennt 10 Kontrollbereiche (die "zehn Gebote"): von der Zugangs- und Datenträgerkontrolle über die Zugriffs- und Übermittlungskontrolle bis zur Transport- und Organisationskontrolle. Normadressat und damit verantwortlich für die Datensicherheit ist "die speichernde Stelle", im vorliegenden Zusammenhang also die Arztpraxis, bzw. deren ärztliche Leitung.

Konkretisiert werden die datenschutzrechtlichen Anforderungen aus § 9 BDSG in "Empfehlungen zu ärztlicher Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis" mit einem Anhang zur "Organisation des EDV-Einsatzes in der Arztpraxis", die 1996 von der Bundesärztekammer veröffentlicht wurden. Der Anhang entspricht früheren Empfehlungen der Kassenärztlichen Bundesvereinigung.

Die Empfehlungen der Bundesärztekammer weisen auch auf eine weitere, oft nicht bekannte Norm hin: Nach § 36 BDSG ist in jeder größeren Arztpraxis, in der mindestens 5 Arbeitnehmer mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ein betrieblicher Datenschutzbeauftragter zu bestellen. Dieser muß "die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit" besitzen und hat im Gesetz näher beschriebene Rechte und Pflichten gegenüber der Leitung der Praxis.

Ebenfalls wenig bekannt ist der Umfang des datenschutzrechtlichen Auskunftsrechts des Patienten nach § 34 BDSG. Es bezieht sich auf alle in einer Datei und "zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen". Eine Differenzierung in objektivierbare und subjektiv wertende Eintragungen des Arztes kennt das BDSG - anders als das Auskunftsrecht aus dem Arztvertrag - nicht. Nach § 34 BDSG ist die Auskunft in der Regel schriftlich zu erteilen, und sie ist unentgeltlich.

18.2.2 Schwachstellen in der Datensicherheit von Arztpraxen

Folgende häufig anzutreffenden Defizite in der Datensicherheit von Arztpraxen mußten wir feststellen:

- Fremdwartung

  In vielen Arztpraxen sind keine ausreichenden EDV-Kenntnisse vorhanden, die es ermöglichen, Wartungsarbeiten in begrenztem Umfang selbst durchzuführen. Häufig sind die dafür erforderlichen Systemverwalter-Kennungen und -Paßwörter überhaupt nicht bekannt. Muß jedoch bei jeder Unregelmäßigkeit, jeder neuen Software-Version ein Wartungstechniker bemüht werden, geht die Herrschaft über die Praxis-Software faktisch auf das Wartungsunternehmen über. Dies widerspricht der datenschutzrechtlichen Verantwortung der speichernden Stelle.

  Wartungstechniker haben in vielen Fällen Zugriff auf Patientendaten bzw. können sich diesen problemlos und unbemerkt verschaffen, zumal sie häufig auch dann mit umfassenden Superuser-Rechten arbeiten, wenn dies gar nicht erforderlich ist. Schon hierin liegt eine Verletzung der ärztlichen Schweigepflicht (siehe oben 18.1.1). Auch nach den Empfehlungen der Bundesärztekammer sollte eine Wartung demgegenüber soweit wie irgend möglich mit Testdaten erfolgen.

  Besonders riskant ist eine Fernwartung. Um die Möglichkeiten eines mißbräuchlichen Zugriffs auf Patientendaten zu verringern, muß sichergestellt sein, daß die Initiative für den Datenzugriff ausschließlich vom Praxispersonal ausgeht und daß die Fernwartungsaktivitäten protokolliert und vor Ort am Bildschirm begleitet werden.

  Leider nicht selbstverständlich ist auch, daß bei der Reparatur von Geräten außer Haus oder beim Austausch von Festplatten die gespeicherten (Patienten-)Daten zuvor physikalisch gelöscht bzw. die alten Datenträger zerstört werden.

- Einsatzbedingungen in der Arztpraxis

  Der bzw. die Rechner der Praxis-EDV sollten in separaten, gut gesicherten Räumen untergebracht sein, um das Diebstahls- und Mißbrauchsrisiko zu vermindern.

  Eine Zugriffskontrolle erfolgt nach unserer Erfahrung meist nur durch ein - oft triviales - Gruppenpaßwort, das nie geändert wird. Ausgeschiedene Mitarbeiter können so auch später noch Patienten- oder Abrechnungsdaten manipulieren, etwa wenn sie sich abends beim Reinigungspersonal als Praxis-Mitarbeiter ausgeben.

- Systemsicherheit

  Oft bietet die Praxis-Software selbst nicht die notwendige Systemsicherheit. So sollte neben einer ordnungsgemäßen Paßwort-Verwaltung auch die Option bestehen, Zugriffsrechte nach verschiedenen Benutzergruppen (Ärzte, Praxispersonal, Hilfskräfte) differenziert zu vergeben, um einen nicht erforderlichen Zugriff aller auf alle Daten zu vermeiden.

  Bildschirmschoner, die den Bildschirm in Ruhestellung verdunkeln, können oft von Patienten, die unbeobachtet in einem Behandlungsraum warten, durch einen beliebigen Tastendruck deaktiviert werden. Es können dann die Daten des Patienten erscheinen, der vorher in einem anderen Praxisraum behandelt wurde. Die Deaktivierung des Bildschirmschoners bedarf deswegen eines Paßwort- oder anderen Schutzes.

  Die Verschlüsselung von Patientendaten auf der Festplatte bietet kaum eine Praxis-Software an. Zumindest Datensicherungsträger (tägliches back-up) müssen aber entweder verschlüsselt und / oder in einem sicheren Behältnis (z. B. Tresor) aufbewahrt werden. Auch für eine Datenübertragung über öffentliche Netze fordert die Bundesärztekammer zu Recht eine Verschlüsselung und darüber hinaus eine Protokollierung.

  Eine Protokollierung sicherheitsrelevanter Benutzeraktivitäten auf Anwendungsebene sehen die meisten Software-Systeme aber ebenfalls nicht vor. Es wird weder der Zugriff auf medizinische Daten noch der Aufruf bestimmter Programme dokumentiert.

- Gemeinschaftspraxen

  Die freie Arztwahl des Patienten gilt auch bei Gemeinschaftspraxen, § 19 Abs. 2 Berufsordnung. Dies bedeutet, daß nur der jeweils behandelnde Arzt in der Lage sein darf, auf die Daten "seiner" Patienten zuzugreifen. Die häufig anzutreffende gemeinsame Patientendatenverwaltung innerhalb einer Gemeinschaftspraxis - mit Zugriffsmöglichkeiten aller Praxismitarbeiter auf alle Patientendaten - verstößt gegen die ärztliche Schweigepflicht. Die Einrichtung von getrennten Patientendateien ist besonders auch für einen Arztwechsel oder die Auflösung einer Gemeinschaftspraxis wichtig. Praxisinterne Vertretungsregelungen sollten mit den Patienten vorab geklärt werden.

- Revisionssicherheit

  Fühlt sich ein Patient falsch behandelt und klagt er gegen den behandelnden Arzt, so wird die Behandlungsdokumentation - hier in Form der elektronischen Karteikarte - zum entscheidenden Beweismittel. Die gängigen Praxis-Systeme bieten jedoch keinen ausreichenden Schutz vor nachträglichen Manipulationen an den gespeicherten

Patientendaten. Der Verweis des Arztes auf seine elektronische Behandlungs-Dokumentation hat keinen Beweiswert, wenn sie jederzeit spurenlos abgeändert, gelöscht oder ergänzt werden kann.

Eine revisionssichere Praxis-EDV erfordert demgegenüber die Möglichkeit, sämtliche beweistragenden medizinischen Dokumente mittels digitaler Signatur einschließlich fälschungssicherer Zeitangabe zu unterschreiben. Die digitale Signatur ist ein Verfahren, das mit Hilfe verschiedener Schlüssel die Authentizität des Urhebers und die Integrität des so unterzeichneten Dokuments bestätigt.

18.3 Sonstiges

- Hinsichtlich der Fernwartung der Patientenüberwachungsanlage im UKE habe ich eine zweite Beanstandung ausgesprochen, da die bereits seit zwei Jahren vom UKE in Aussicht gestellte Auswertungssoftware zur Überwachung der Fernwartungsverbindung nicht fertiggestellt werden konnte. Daraufhin wurde das bisherige Konzept zur Erstellung der geforderten Auswertungssoftware in Zusammenarbeit mit dem UKE-Rechenzentrum nochmals grundlegend überarbeitet. Da sich erstmals auch der nordamerikanische Hersteller der Patientenüberwachungsanlge bereit erklärt hat, bei der Gestaltung einer datenschutzgerechten Lösung mitzuarbeiten, besteht durchaus die Möglichkeit, das Thema "UKE-Fernwartung" nach mehr als fünf Jahren (vgl. 11., 13.-15. TB) doch noch abschließen zu können.

- Im September 1997 führten wir eine datenschutzrechtliche Prüfung der Kassenärztlichen Vereinigung Hamburg durch. Nach Abstimmung des inzwischen fertiggestellten Sachberichts werden wir die rechtliche Bewertung vornehmen und Maßnahmen zur Verbesserung des Datenschutzes benennen.

- Mit dem Drogenbeauftragten und dem Gesundheits- und Umweltamt Eimsbüttel haben wir das geplante neue Meldeverfahren bei der Methadonsubstitution Drogenabhängiger abgestimmt. Datenschutzrechtlicher Kernpunkt ist die Codierung der Patientennamen bei der Meldung der Substituierten an die zentrale Erfassungsstelle durch die behandelnden Ärzte. Die Umsetzung der Verabredungen steht derzeit noch aus.

- Im Februar 1997 haben wir alle staatlichen Krankenhäuser darauf hingewiesen, daß die Novellierung des Hamburgischen Datenschutzgesetzes nun die Bestellung einer bzw. eines betrieblichen Datenschutzbeauftragten in jedem Krankenhaus erforderlich macht. Diese Person hat die im BDSG genannten Rechte und Pflichten, sie muß fachkundig und zuverlässig und in ausreichendem Maße von anderen Aufgaben freigestellt sein. Noch sind nicht alle Krankenhäuser der Pflicht zur Bestellung nachgekommen.

Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

19. Versicherungswirtschaft

19.1 Registrierung von Versicherungsvermittlern

Noch immer ist die Frage, ob die Bundesregierung die EG-Empfehlung vom 18. Dezember 1991 durch ein Gesetz umsetzen wird, nicht endgültig geklärt (vgl. 15. TB, 22.1). Die Länder Niedersachsen und Saarland haben einen entsprechenden Gesetzesantrag über den Bundesrat eingebracht, über den noch nicht entschieden wurde.

Daher ist die Frage, ob das bereits 1995 gegründete Zentrale Register für Versicherungsvermittler in Deutschland e.V. auf gesetzlicher Grundlage oder rein privatrechtlicher Basis seine Tätigkeit aufnehmen wird, weiterhin offen. Die Versicherungswirtschaft beabsichtigt jedoch, sofern das Gesetz nicht verabschiedet wird, die Registrierung Ende 1998 aufzunehmen.

Die Versicherungswirtschaft sieht in der EG-Empfehlung eine Vorschrift, nach der als Verbraucherschutzmaßnahme alle Versicherungsvermittler in einem zentralen Register erfaßt werden sollen, die den vorgegebenen Mindestanforderungen entsprechen. Hierzu zählen fachliche Qualifikation, festgelegte Verantwortlichkeit bei Schädigung des Verbrauchers durch falsche Beratung und die finanzielle Absicherung zur Erstattung entsprechender Schadenersatzforderungen.

Um für die Registrierung von Versicherungsvermittlern unter datenschutzrechtlichen Gesichtspunkten vorbereitet zu sein, lag der Versicherungswirtschaft an einer Abstimmung ihres Konzepts mit den Datenschutzaufsichtbehörden.

Im Entwurf der Richtlinien für das Register wird davon ausgegangen, daß die einzelnen Vermittler ihre Daten im Wege eines Auftrags zur Verfügung stellen und von dem Register beauskunften lassen. Die Versicherungswirtschaft wollte diese Beauftragung als einen Auftrag im Sinne des § 11 Bundesdatenschutzgesetz (BDSG) verstanden wissen. Da das Register aber durch die Mitglieder des entsprechenden Vereins, also durch die Verbände betrieben wird, kann die Verantwortung für die datenschutzgerechte Behandlung der personenbezogenen Daten nicht auf die einzelnen Vermittler als "Auftraggeber" übertragen werden.

Diese Auffassung der Obersten Aufsichtsbehörden für den Datenschutz wurde mit den Vertretern der Versicherungswirtschaft erörtert. Die Aufsichtsbehörden gehen davon aus, daß lediglich ein Auftrag ohne Anwendung des § 11 BDSG anzunehmen ist.

Die Versicherungswirtschaft hat sich zu dieser Frage nicht abschließend geäußert. Sie ist der Auffassung, daß es auf eine Entscheidung dieses Problems nicht ankommt, solange die Möglichkeit besteht, daß der Vermittler selbst für die Richtigkeit der Daten einstehen muß.

Neben der Kritik an der vorgesehenen rechtlichen Konstruktion haben die Datenschutzaufsichtsbehörden der Versicherungswirtschaft auch ihre Zweifel an der verfassungs- und kartellrechtlichen Zulässigkeit des Registers ohne gesetzliche Grundlage mitgeteilt. Ein neu vorgelegter Entwurf für die Regelung des Registers geht auf einige datenschutzrechtliche Hinweise der Aufsichtsbehörden ein; er enthält aber noch problematische Punkte, die Gegenstand weiterer Erörterungen mit der Versicherungswirtschaft sind.

Eines dieser Probleme ist nach wie vor, daß es keine Ausnahme von der Registerpflicht gibt. Die Versicherungswirtschaft betont zwar, daß die Registrierung den Interessen der Vermittler selbst dient, die sich damit ein Qualitätsmerkmal erwerben. Dann müßte aber den Vermittlern eine wirkliche Wahlmöglichkeit für die Registrierung eröffnet werden. Vermittlern, die sich am Register nicht beteiligen, dürften bei der Berufsausübung auf Dauer keinerlei Nachteile entstehen. Angesichts des Ziels der Versicherungswirtschaft, nur mit registrierten Vermittlern zusammenzuarbeiten, ist dies jedoch schwer vorstellbar. Eine Nachprüfung, ob nichtregistrierte Vermittler diskriminiert werden oder nicht, wäre nahezu unmöglich. Dies spricht ebenfalls dagegen, daß es sich um ein nachweisbar freiwilliges Registrierungsverfahren handelt.

19.2 Sonstiges

Weiter wurden im Bereich der Versicherungwirtschaft folgende Themen behandelt:

- Mit dem Gesamtverband der Deutschen Versicherungswirtschaft wurden die datenschutzrechtlichen Aspekte der Präsentierung von Versicherungen im Internet insbesondere im Hinblick auf die Anforderungen des Multimediarechts erörtert.

- Der Einsatz opto-elektronischer Speichermedien wirft aus Sicht der Obersten Aufsichtsbehörden noch datenschutzrechtliche Fragen auf, die bisher nicht abschließend geklärt werden konnten.

- Obwohl die von der Versicherungswirtschaft eingesetzten Schweigepflicht-Entbindungserklärungen inhaltlich begrenzt sind, gehen die Unternehmen bei Schadensfällen in den Befragungen von Ärzten zu weit. Die Versicherungswirtschaft ist demgegenüber der Auffassung, daß die Fragen an die Ärzte durch die von dem Versicherungsnehmer abzugebende Erklärung gedeckt sind. Dieser Dissens soll möglichst bald geklärt werden.

20. Schufa

20.1 Scoring-Verfahren

Die Schufa setzt seit dem 1. November 1996 das Scoring-Verfahren bei ausgewählten Pilot-Anwendern ein. Bei diesem Verfahren handelt es sich um ein System zur Bonitätsprüfung. Grundlagen des Verfahrens sind statistisch-mathematische Methoden zur Prognose des zukünftigen Verhaltens von Kreditnehmern, insbesondere zur Ermittlung eines statistischen Ausfallrisikos. Zu diesem Zweck wurde das Ergebnis jahrelang beobachteter Erfahrungen im Umgang mit Kreditnehmern statistisch aufbereitet und in mathematischen Formeln zusammengefaßt, so daß Vorhersagen über das zukünftige Verhalten von Kreditnehmern in Form eines Scorewertes schon bei Angabe nur weniger kreditrelevanter Daten des Betroffenen möglich sind.

Zusätzliche Daten werden von den Betroffenen für das Schufa-Scoring-Verfahren nicht erhoben. Bei der Ermittlung des Scorewertes werden auch keine soziodemographischen Daten einbezogen, z. B. "schlechte Wohnadressen".

Das Scoring-Verfahren der Schufa war im Berichtszeitraum Gegenstand ausführlicher Erörterungen zwischen den Obersten Aufsichtsbehörden und der Schufa. Vorher hatte die Schufa die Aufsichtsbehörden zeitig und ausführlich über ihr Vorhaben informiert.

Der nach den statistischen Auswertungsmethoden ermittelte Scorewert ist eine Punktzahl, die dem Vertragspartner der Schufa zusätzlich zur üblichen Schufa-Auskunft bei Anfragen übermittelt wird. Derzeit werden Scorewerte zwischen 1 (schlechtester Wert) und 1000 (bester Wert) ausgegeben.

Zu Personen, bei denen bereits Informationen zu einem nicht-vertragsgemäßen Verhalten im Schufa-Datenbestand vorhanden sind (z. B. Kreditkündigung, Scheckkartenmißbrauch, eidesstattliche Versicherung) wird kein Scorewert errechnet. In diesen Fällen ist die zu berechnende Wahrscheinlichkeitsprognose systemlogisch derzeit nicht möglich. Zu Personen, zu denen die Schufa keine Daten gespeichert hat, werden ebenfalls keine Scorewerte errechnet.

Die einzelnen Scorewerte werden nicht im Schufa-Datenbestand gespeichert. Die Scorewerte werden bei jeder Anfrage neu ermittelt, da sich sowohl der Datensatz des Betroffenen als auch die

statistisch-mathematischen Bezugsgrößen zwischenzeitlich verändert haben können. Zu Datensicherungszwecken werden die Scorewerte aber in log files (Protokolldateien) erfaßt.

Datenschutzrechtlich ist die Übermittlung des Scorewertes durch die Schufa an den Anfragenden nach § 28 BDSG zu beurteilen; § 29 BDSG ist hierfür nicht anwendbar, da die Scorewerte nicht geschäftsmäßig zum Zwecke der Übermittlung gespeichert werden. Zwischen den Obersten Aufsichtsbehörden und der Schufa besteht Einigkeit, daß der bei einer Anfrage zu einer bestimmten Person ermittelte Scorewert ein personenbezogenes Datum im Sinne des § 3 Abs. 1 BDSG ist.

Nach § 28 Abs. 1 Nr. 2 BDSG bestehen gegen die Übermittlung des Scorewertes keine grundsätzlichen Bedenken, da in der Regel kein Grund zu der Annahme bestehen wird, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Nutzung und Übermittlung überwiegt.

Eingehend diskutiert wurde die Frage der Notwendigkeit einer Änderung der "Schufa-Klausel" durch Hinweis auf das Scoring-Verfahren als Nutzungsform. Durch die zu unterzeichnende Schufa-Klausel willigt der Betroffene in die Übermittlung seiner Vertragsdaten an die Schufa ein. Die Erhebung und Übermittlung zusätzlicher von der Schufa-Klausel bisher nicht erfaßter Daten für das Scoring-Verfahren ist zwar nicht beabsichtigt. Die vorhandenen Daten werden aber zu einem weiteren Zweck genutzt.

Die Schufa-Klausel enthält den Hinweis, daß die Schufa die Daten speichert, um den ihr angeschlossenen Vertragspartnern Informationen zur Beurteilung der Kreditwürdigkeit von Kunden geben zu können. Da auch die Nutzung des Datenbestandes zur Ermittlung der Scorewerte diesem Zweck dient, bestand im Ergebnis Übereinstimmung zwischen den Aufsichtsbehörden und der Schufa, daß eine Änderung der Schufa-Klausel nicht zwingend erforderlich ist.

Zur Verbesserung der Transparenz für die Betroffenen haben die Aufsichtsbehörden aber eine Ergänzung der Merkblatts zum Schufa-Verfahren mit Informationen zum Scoring und Aushändigung des Merkblatts im Zusammenhang mit der Unterzeichnung der Schufa-Klausel gefordert. Die Überarbeitung des Merkblatts erfolgt durch den Zentralen Kreditausschuß (ZKA) als Herausgeber.

Noch nicht abschließend erörtert wurde die Frage der Beauskunftung des Scorewertes gegenüber dem Betroffenen. Die Schufa vertritt hierzu die Auffassung, daß keine Rechtspflicht auf Mitteilung des Scorewertes bei einer Auskunft an den Betroffenen über die zu seiner Person gespeicherten Daten nach § 34 BDSG bestehe. Die Scorewerte würden zusammen mit den im Einzelfall übermittelten Daten lediglich zu Zwecken der Datensicherheit und der Datenschutzkontrolle in log files gespeichert, so daß eine Auskunftspflicht nach § 34 Abs. 4 in Verbindung mit § 33 Abs. 2 Nr. 2 BDSG entfalle. Außerdem sei die Auswertung der log files zum Zwecke der Beauskunftung eines Scorewertes mit unangemessenem Verwaltungsaufwand verbunden. Der Scorewert könne zwar grundsätzlich rekonstruiert werden, wenn das Datum der Auskunft an den Vertragspartner bekannt sei. Zweifelhaft sei jedoch, ob eine nachträgliche Errechnung stets zutreffend sei, da sich sowohl der Datensatz des Betroffenen als auch die statistischen Bezugsgrößen zwischenzeitlich verändert haben könnten. Denkbar sei daher, daß der Betroffene zum Zeitpunkt der Selbstauskunft einen ganz anderen Scorewert erhalte als z. B. seine Bank bei einer früheren Anfrage.

Die Aufsichtsbehörden sind demgegenüber der Auffassung, daß eine Auslegung des § 34 BDSG, die den Sinn und Zweck der Vorschrift nicht berücksichtige und sich allein am Wortlaut orientiere, nicht zu vertreten sei. Sinn und Zweck des Auskunftsrechts sei es, daß der Betroffene die für ihn notwendige Kenntnis für die Wahrnehmung seiner sonstigen Rechte (Berichtigung, Sperrung oder

Löschung) bekomme. Es dürfte für ihn kaum nachvollziehbar sein, daß zwar ein Schufa-Vertragspartner jederzeit einen Scorewert über ihn erhalten kann, er selber diese Information von der Schufa aber nicht erfährt. Vor allem in den Fällen, in denen der Betroffene im unmittelbaren Anschluß an die Schufa-Auskunft an einen Vertragspartner seinen Scorewert erfrage, sei dies kaum vermittelbar.

Die Diskussion zwischen der Schufa und den Aufsichtsbehörden über die Beauskunftung des Scorewertes wird fortgesetzt. Ebenfalls noch erörtert wird die Frage, ob der an einen B-Vertragspartner der Schufa (z. B. an den Versandhandel) übermittelte Scorewert unter datenschutzrechtlichen Gesichtpunkten ausschließlich unter Einbeziehung von Vertragsdaten aus A-Verträgen (z. B. mit Kreditinstituten) errechnet werden darf. Weiter soll geklärt werden, ob und wie das Scoring-Verfahren mit dem Verbot der "automatisierten Einzelentscheidung" gemäß Art. 15 der EG-Datenschutzrichtlinie vereinbar ist.

20.2 Sonstiges

Die Obersten Aufsichtsbehörden haben beim Bundesjustizministerium angefragt, wann mit einer Neuregelung der Schuldnerverzeichnisverordnung zu rechnen ist. Sollte die Neuregelung nicht in absehbarer Zeit erfolgen, werden die Aufsichtsbehörden die bisherige Praxis einzelner Schufa-Gesellschaften, Online-Verfahren mit Schuldnerverzeichnisdaten auf der Basis von Handelskammerlisten zu betreiben, nicht mehr tolerieren.

21. Kreditwirtschaft

21.1 Allfinanzkonzepte und Einwilligungserklärung

Die verschiedenen Einwilligungserklärungen im Rahmen der Allfinanzkonzepte der Kreditinstitute (vgl. 15. TB, 25.1) wurden 1997 abschließend mit den Obersten Aufsichtsbehörden für den Datenschutz behandelt. Dabei geht es um die Kundendaten, die die Kreditinstitute an andere Finanzdienstleister, z. B. Bausparkassen und Versicherungen für deren Geschäftszwecke übermitteln.

Erfreulicherweise konnte erreicht werden, daß die möglichen Datenempfänger bereits in der Erklärung selbst genannt werden sollen. Darüber hinaus sind auch Umfang und Inhalt der zu übermittelnden Daten für den Kunden überschaubarer geworden. Neben der Aufzählung bestimmter Datenarten heißt es jetzt "... oder vergleichbare Daten". Damit ist gewährleistet, daß einerseits die Kreditwirtschaft in der Lage ist, Übermittlungen in gewissem Rahmen veränderten Bedingungen anzupassen. Andererseits erlebt aber der Kunde keine unliebsamen Überraschungen, weil "vergleichbar" nur solche Daten sind, die sich in ihrer Sensibilität für den Betroffenen ähneln.

Die jeweilige Allfinanzklausel kann jetzt vom Kunden auch gestrichen werden, ohne daß er Nachteile befürchten muß. Damit wird die Wahlfreiheit hinsichtlich dieser Klausel für den Kunden gewährleistet.

Zu bedauern ist, daß die Kreditwirtschaft nicht bereit gewesen ist, den Forderungen nach einer Ankreuzlösung nachzukommen. Nur diese hätte eine differenzierte Wahlmöglichkeit des Bürgers gewährleistet. Vorschläge gingen dahin, den Kunden sowohl über den Datenempfänger, als auch den Umfang der zu übermittelnden Daten frei entscheiden zu lassen.

21.2 Elektronische Geldkarte

Zu der seit 1. Januar 1997 im Einsatz befindlichen elektronischen Geldkarte des deutschen Kreditwesens und deren Datenschutzrisiken haben wir bereits berichtet (14. TB, 25.1). Im Oktober 1996 wurde in einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder zum Datenschutz bei elektronischen Geldbörsen insbesondere der Einsatz anonymer Zahlungsverfahren gefordert (15. TB, Seite 67 f.).

Bei der elektronischen Geldkarte werden sogenannte Schattenkonten geführt, die es ermöglichen, das Kaufverhalten jedes einzelnen Kunden nachzuvollziehen. Daraufhin wurde im Zuge der Datenschutzdiskussion seitens des Kreditwesens verstärkt auf sogenannte White-Cards verwiesen, die im Vergleich zur traditionellen Geldkarte ohne Kontoverbindung herausgegeben werden sollen. Dies würde auch der Forderung der Datenschützer nach Wahlfreiheit zwischen verschiedenen Verfahren mit unterschiedlichem Datenschutzniveau entsprechen.

Zwar teilten Vertreter des Zentralen Kreditausschusses mit, daß diese Karte in das Angebot aufgenommen wurde und für Volksbanken und Raiffeisenbanken im Großraum Hamburg seit November 1996 mehr als 4000 kontoungebundene Geldkarten produziert wurden. Leider konnten sie jedoch kein Kreditinstitut benennen, das bisher White-Cards herausgegeben hat. Auch eine Umfrage unter mehreren Hamburger Kreditinstituten hat ergeben, daß sie zwar die neuen EC-Karten mit Geldbörsenfunktion, aber bisher keine kontoungebundene Geldkarte ausgegeben haben. Zudem werden die Kunden meistens darüber im Unklaren gelassen, daß White-Cards überhaupt existieren.

Damit Einkäufe auch in Zukunft anonym bleiben können, fordert die Aufsichtbehörde die Hamburger Kreditinstitute auf, ihren Kunden die datenschutzfreundliche White-Card künftig anzubieten.

21.3 Sonstiges

- Das Thema einer Beschränkung des Zugriffs auf Kontoinformationen wird intensiv weiter verfolgt. Die Kreditwirtschaft hat nunmehr zugesagt, das Anliegen einer Prüfung zu unterziehen.

- Videoüberwachung in Kreditinstituten.

- Prüfung eines meldepflichtigen Hamburger Kreditinstitutes.

22. Wohnungswirtschaft

22.1 Schufa-Selbstauskünfte von Mietinteressenten

Seit geraumer Zeit befassen wir uns mit der Praxis einiger Vermieter in Hamburg, von Mietinteressenten regelmäßig die Vorlage einer Schufa-Selbstauskunft zu verlangen (vgl. 13. TB, 22.1). Dabei konnten wir zunächst erreichen, daß sich die Baubehörde nach einem bürgerschaftlichen Ersuchen an zahlreiche wohnungswirtschaftliche Verbände gewandt hat, um darauf hinzuwirken, daß zukünftig Wohnungsunternehmen auf die Einholung einer Schufa-Selbstauskunft verzichten. Die städtischen Wohnungsunternehmen haben entweder bisher keine Schufa-Selbstauskünfte angefordert oder haben inzwischen darauf verzichtet.

Die ersten Reaktionen der wohnungswirtschaftlichen Verbände hatten allerdings gezeigt, daß zahlreiche Vermieter auch zukünftig die Option haben wollen, Schufa-Selbstauskünfte von Mietinteressenten verlangen zu dürfen. Bei den Gesprächen mit Vertretern der

Wohnungswirtschaft, die von der Baubehörde moderiert werden und noch nicht abgeschlossen sind, zeichnet sich immerhin bereits folgendes ab:

Die Wohnungswirtschaft ist im wesentlichen daran interessiert, die "schwarzen Schafe" vor Mietvertragsabschluß zu erkennen. Hierfür liegt ihr an einer Bonitätsprüfung, die auf den jeweiligen Einzelfall abstellt. Deshalb benötigt die Wohnungswirtschaft lediglich in den Fällen, in denen die ansonsten vorgelegten Unterlagen für eine abschließende Aussage über die Bonität des Wohnungsbewerbers nicht ausreichen, die Schufa-Selbstauskunft als zusätzliches Entscheidungskriterium.

Obwohl dies bereits ein Fortschritt gegenüber der uns bisher bekannt gewordenen Praxis darstellt, sind wir zusätzlich in Gespräche mit der Schufa eingetreten, um zu klären, ob dort ein speziell auf die Wohnungswirtschaft zugeschnittenes Auskunftsverfahren installiert werden kann. Die Schufa ist an einem solchen Verfahren sehr interessiert, da sie davon ausgeht, daß ca. 2/3 der jährlich bundesweit erteilten 630.000 Selbstauskünfte zu wohnungswirtschaftlichen Zwecken genutzt werden. Angedacht ist, ein solches Verfahren auf die Übermittlung von Negativdaten zu beschränken und vorher die Einwilligung des Betroffenen einzuholen.

Sobald sich in unseren Gesprächen in Hamburg ein neues Schufa-Auskunftsverfahren für Mietinteressenten konkreter abzeichnet, werden wir dies im Düsseldorfer Kreis der Obersten Aufsichtsbehörden abstimmen. Über das Ergebnis werden wir im nächsten Tätigkeitsbericht weiter berichten.

22.2 Sonstiges

Nach wie vor erreichen uns zahlreiche Anfragen von Wohnungsuchenden zu Fragebögen, in denen sie den Vermietern unterschiedliche Angaben über ihre persönlichen und wirtschaftlichen Verhältnisse preisgeben sollen (vgl. 11. TB, 30.2).

In solchen Fällen haben wir den Vermietern unter Hinweis auf die Rechtsprechung erläutert, daß das Fragerecht der Vermieter durch das Selbstbestimmungsrecht des Mieters begrenzt wird. Insbesondere ist zu beachten, daß den Mieter Aufklärungspflichten nur für solche Umstände treffen, die für das Mietverhältnis wesentlich sind und deren Offenbarung dem Mieter zuzumuten ist. Unsere Hinweise haben in den von uns aufgegriffenen Fällen ausnahmslos zu einer datenschutzgerechten Überarbeitung der Fragebögen geführt.

23. Postdienste

23.1 Entwurf eines neuen Postgesetzes

Im Berichtszeitraum haben sich Bundestag und Bundesrat mit dem Entwurf eines neuen Postgesetzes (PostG-E) (vgl. Bundestags-Drucksache 13/7774) befaßt. Die gesetzliche Neuregelung ist im Hinblick auf die zum 1. Januar 1998 notwendige ordnungspolitische Neuordnung des Postsektors erforderlich. Der Bundesbeauftragte für den Datenschutz hat die Gesetzesberatungen begleitet und versucht zu erreichen, daß die spezifischen Regelungen zum Postgeheimnis und zum Datenschutz nicht hinter dem üblichen Standard zurückbleiben. Dies ist in zweierlei Hinsicht noch nicht gelungen.

1. Der Bundesrat hatte in seiner Stellungnahme vom 16. Mai 1997 verlangt, daß in § 41 Abs. 1 Satz 3 PostG-E durch Rechtsverordnung Mindestfristen zur Speicherung von Daten festgelegt werden sollen, um beispielsweise den Strafverfolgungsbehörden, Polizeien und

Nachrichtendiensten einen Zugriff auf diese Daten zu ermöglichen. Diese Forderung läuft darauf hinaus, daß die Postdienstunternehmen Daten, die sie überhaupt nicht benötigen und die bisher nie gespeichert worden sind (wer hat wem wann Post zugesandt), allein im staatlichen Interesse für eine bestimmte Mindestdauer speichern.

Ein ähnliches Verlangen ist bereits aus dem Gesetzgebungsverfahren zum Telekommunikationsgesetz (TKG) bekannt und ist damals auf entschiedenen Widerspruch bei den Datenschutzbeauftragten gestoßen. Letztendlich wurde im TKG auf die Festlegung von Mindestspeicherfristen verzichtet. Umso unverständlicher ist, daß diese Forderung bei den Beratungen zum PostG-E erneut erhoben wurde.

2. Der Gesetzentwurf sieht in § 42 Abs. 3 und 4 in Anlehnung an § 91 Abs. 4 TKG vor, die datenschutzrechtliche Kontrolle der Postdienstunternehmen nicht den nach § 38 Abs. 6 BDSG benannten Aufsichtsbehörden, sondern dem Bundesbeauftragten für den Datenschutz zu übertragen.

   Die ersten Erfahrungen mit der praktischen Umsetzung dieser Regelung im Telekommunikationsbereich machen deutlich, daß damit eine Fülle von Abgrenzungsfragen hinsichtlich der Zuständigkeiten des Bundesbeauftragten für den Datenschutz und der Aufsichtsbehörden der Länder aufgeworfen worden sind. Diese Unsicherheiten spiegeln sich in Meinungsverschiedenheiten über die Zuständigkeit für die Aufsicht wider. Es ist zu befürchten, daß die von der Bundesregierung favorisierte Regelung zu den gleichen Unsicherheiten bei der Datenschutzaufsicht über Postdienstunternehmen führen wird. Der Bundesrat hat diese Befürchtung in seiner Stellungnahme vom 16. Mai 1997 geteilt.

Wir haben die in Hamburg zuständigen Ressorts gebeten, im Verlauf der weiteren Gesetzesberatungen im Vermittlungsausschuß, der vom Bundesrat angerufen wurde (vgl. Bundestags-Drucksache 13/8800), sich zum einen der Forderung nach der Einführung von Mindestspeicherfristen in § 41 Abs. 1 Satz 3 PostG-E nicht anzuschließen. Zum anderen sollte erreicht werden, daß der Bundesrat seine Auffassung hinsichtlich der Datenschutzaufsicht für Postdienstunternehmen bekräftigt, damit diese Aufgabe den Aufsichtsbehörden der Länder zugewiesen wird.

23.2 Sonstiges

Immer wieder wenden sich Bürger an uns, weil sie Fragen zur Datenverarbeitung bei der Deutschen Post AG haben. Besonders häufig erfolgte dies im Zusammenhang mit der Verteilung einer Postwurfsendung im April 1997 an alle 34 Millionen Haushalte im Bundesgebiet, mit der die Deutsche Post AG die richtige Schreibweise der Adressen abfragen wollte. In diesen Fällen müssen wir regelmäßig an den Bundesbeauftragten für den Datenschutz verweisen, der nach wie vor allein für die datenschutzrechtliche Kontrolle der Deutschen Post AG zuständig ist.

24. Nahverkehr

24.1 Bargeldloses Zahlungsverfahren beim Hamburger Verkehrsverbund (HVV)

Im 13. TB (26.2.2) hatten wir über die Einführung des bargeldlosen Zahlungsverfahrens beim HVV berichtet. Seitdem haben sich einige grundlegende Veränderungen ergeben, die insbesondere den Verkauf von Einzelfahrscheinen betreffen.

Im HVV-Bereich hat zwischenzeitlich die Hamburger Hochbahn AG (HHA) in einem Feldversuch das bargeldlose Zahlungssystem der PayCard erprobt. Hierbei handelt es sich um eine multifunktionale, wiederaufladbare Chipkarte, mit der man bundesweit bargeldlos telefonieren sowie Busse und Bahnen benutzen kann. Partner sind die Deutsche Telekom AG, die Deutsche Bahn AG und mehrere Nahverkehrsunternehmen.

Zwei Varianten wurden dem Kunden zur Auswahl angeboten: Er kann die Karte mit PIN-Nummer und Kontoanbindung an jedem Kartentelefon aufladen; andererseits hat der Kunde auch die Möglichkeit, in einer Servicestelle eine Karte gegen Barzahlung - ähnlich einer Telefonkarte - zu kaufen.

Die Telekom ist die zentrale Stelle für das Aufladen der Karten und gleichzeitig auch für das Verteilen der eingenommenen Geldwerte auf die einzelnen Verkehrsbetriebe zuständig. Das Auslesen der einzelnen Subbörsen, die für die jeweiligen Verkehrsbetriebe nach einem Verteilschlüssel angelegt worden sind, erfolgt aggregiert und nicht personenbezogen. Auch im Fahrkartenautomaten werden keine Angaben über den Kauf von Einzelfahrscheinen gespeichert. Es wird lediglich im Preisspeicher des Automaten die Anzahl der verkauften Einzelfahrscheine festgehalten und zwar ebenfalls aggregiert.

Der jetzt eingeschlagene Weg ist sehr datenschutzfreundlich. Die Erstellung von Bewegungsprofilen sowie sonstige Gefährdungen des allgemeinen Persönlichkeitsrechts müssen nicht befürchtet werden, wenn Fahrscheine mit der PayCard bargeldlos bezahlt werden. Daneben ist sichergestellt, daß der Fahrgast seine Fahrkarte auch weiterhin mit Bargeld bezahlen kann.

Mittelfristig ist geplant, die PayCard bei allen Verkehrsunternehmen im HVV sowohl an den Fahrkartenautomaten als auch in den Bussen zu akzeptieren. Darüber hinaus soll auch Inhabern von EC-Karten mit Geldkarten-Funktion der Kauf von Einzelfahrscheinen ermöglicht werden. Allerdings müßte hierfür eine Umrüstung der Automaten erfolgen. Der Einsatz der EC-Karte hätte den datenschutzrechtlichen Nachteil, daß dabei nach den Vorgaben der Banken und Sparkassen zahlreiche personenbezogene Daten in sogenannten Schattenkonten gespeichert werden, weil aufgrund des komplexen Clearingverfahrens jeder ausgehändigte Einzelfahrschein separat erfaßt wird (vgl. 14. TB, 25.1).

Aus unserer Sicht ist eine solche Speicherung personenbezogener Datensätze nicht notwendig. Deshalb haben wir die HHA gebeten, zum einen gegenüber dem Zentralen Kreditausschuß (ZKA) auf den Verzicht von Schattenkonten zu drängen. Zum anderen sollte geprüft werden, ob nicht zumindest darauf verzichtet werden kann, den Zeitpunkt des Fahrscheinkaufs sowie die Nummer des Automaten zu speichern.

Die HHA wird in Abstimmung mit den anderen Verkehrsunternehmen und dem HVV unsere Überlegungen bei einer Entscheidung über den Einsatz der Geldkarte einbeziehen und uns weiter an der Entwicklung des Verfahrens beteiligen.

24.2 Sonstiges

Der Hamburger Verkehrsverbund (HVV) führt bei Kunden, die ermäßigte Abonnementskarten im Ausbildungsverkehr erwerben wollen, in festgelegten Abständen eine Befragung durch. Damit will der HVV höhere Zuschüsse vom Bund und den Ländern Hamburg, Schleswig-Holstein und Niedersachsen erhalten.

Besorgte Bürger, die uns immer wieder auf diese Praxis ansprechen, können wir beruhigen. Schon vor Jahren (vgl. 5. TB, 6.8.3) konnten wir bei einer Prüfung des Verfahrens feststellen, daß die Zuordnung zu einer Person praktisch nicht mehr möglich ist, wenn die Fragebögen beim HVV eingegangen sind. Da sich seitdem die Praxis nicht geändert hat, muß kein Auszubildender befürchten, daß er durch die Teilnahme an der Befragung in seinen Persönlichkeitsrechten verletzt wird.

25. Warndateien

Zunehmend richten Unternehmen, die Auskunfts- und Warndateien betreiben wollen, Anfragen an die Aufsichtsbehörde. Unternehmen planen Auskunftsdienste z. B. mit Daten über das Zahlungsverhalten von Mobilfunkkunden, über die Zahlungsweise von Buchhändlern an Verlage oder mit Daten über Inkassoverfahren. Gespeichert werden sollen in der Regel nicht nur Negativdaten der Betroffenen, sondern auch (positive) Vertragsdaten. Eine Anfrage betraf die Wohnungswirtschaft mit einer Vermieterschutzdatei, in der Angaben zum Mieterverhalten (z. B. ruhestörender Lärm, häufig Streit mit den Nachbarn) und der Zahlungsmoral (z. B. gelegentliche Mietrückstände, Räumungsklage) gespeichert und an die beteiligten Vermieter übermittelt werden sollten.

Datenschutzrechtlich handelt es sich bei diesen Tätigkeiten um geschäftsmäßige Datenspeicherungen zum Zwecke der Übermittlung nach § 29 BDSG. Nach § 29 Abs. 1 Nr. 1 BDSG ist das geschäftsmäßige Speichern personenbezogener Daten zum Zwecke der Übermittlung nur zulässig, wenn kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Speicherung hat. Auch für die Übermittlung gilt nach § 29 Abs. 2 BDSG, daß neben dem berechtigten Interesse des Empfängers an der Auskunft kein schutzwürdiges Interesse des Betroffenen an dem Ausschluß der Übermittlung vorliegen darf.

Problematisch sind Warndateien nach diesen Vorschriften insbesondere dann, wenn keine nachvollziehbaren Kriterien darüber bestehen, unter welchen Umständen Daten in der Datei gespeichert werden, und wenn die Betroffenen nicht über die Speicherung informiert werden. Wenn nicht ein eindeutiger Betrug(sversuch) vorliegt, werden die Betroffenen in vielen Fällen ein schutzwürdiges Interesse an dem Ausschluß der Speicherung und Übermittlung ihrer personenbezogenen Daten haben. Im Datenbestand der Auskunftei über das Zahlungsverhalten der Mobilfunkkunden sollte z. B. zunächst das Merkmal "High Spender", d. h. Vieltelefonierer, gespeichert und weitergegeben werden; es konnten aber keine objektiven Kriterien für dieses Merkmal angegeben werden, so daß es auch den regelmäßig zahlenden Vieltelefonierer betreffen konnte.

Grundsätzlich fordern wir daher von den Betreibern von Auskunftsdiensten objektive Kriterien für die zu speichernden Merkmale, umfassende Information der Betroffenen über die Tätigkeit der Auskunftei und die Einholung einer Einwilligungserklärung. Im Mobilfunkbereich ist daran gedacht, eine entsprechende Erklärung in den Vertragstext zwischen den Mobilfunkanbietern und deren Kunden aufzunehmen.

Die Annahme, daß gegen die Speicherung in einer Warndatei bei Vorliegen der Einwilligungserklärung des Betroffenen keine Einwände bestehen, gilt jedoch nicht uneingeschränkt. Warndateien über Mieter halten wir auch dann in der Regel nicht für zulässig, wenn der Vermieter ein Einverständnis des Mieters für die Übermittlung seiner Daten an die Auskunftei eingeholt hat. Da die Beschaffung einer neuen Wohnung für Personen, die in einer Vermieterschutzdatei erfaßt würden, nahezu unmöglich wäre, würde das elementare Rechtsgut "Wohnung" durch eine derartige Datei erheblich gefährdet. Hinzu kommt, daß Mieter ihre

Einwilligung zur Datenübermittlung in eine Vermieterschutzdatei völlig freiwillig erteilen müßten; im Zusammenhang mit dem Abschluß eines Mietvertrages haben sie aber kaum die Möglichkeit zu einer derartigen selbständigen Entscheidung.

26. Haushaltsumfragen

Im Berichtsjahr erfolgten von verschiedenen Firmen Haushaltsbefragungen. Darin wurden in zumeist über 100 Fragen auch sehr sensible Daten über das Urlaubs- und Reiseverhalten, Freizeitaktivitäten, Auto, Gesundheit, Finanzsituation, Wohnung, Kauf- und Konsumverhalten, Schulbildung und Berufsausübung gestellt. Zahlreiche Bürger wandten sich an die Aufsichtsbehörde und wollten wissen, ob die Umfragen den datenschutzrechtlichen Bestimmungen entsprechen.

Bei den Befragungen handelte es sich nicht, wie von vielen vermutet, um reine Marktforschung. Die erhobenen Daten sollen für Direktwerbezwecke verwendet werden. Daher muß für die Befragten klar erkennbar sein, daß die Angaben nicht anonym, sondern personenbezogen ausgewertet und für welchen Zweck sie verwendet werden. Ein mit allen Obersten Aufsichtsbehörden für den Datenschutz abgestimmtes Erfordernis ist die unterschriebene Einwilligung auf dem Fragebogen, und zwar von allen volljährigen bzw. einsichtsfähigen Betroffenen.

Niemand ist verpflichtet, solche Fragebögen auszufüllen. Die Beantwortung der Fragen ist freiwillig. Wer etwas gegen die Nutzung seiner Daten für Marketing- und Werbezwecke hat, kann deren Nutzung nach § 28 Abs. 3 BDSG
- auch nach Absendung seiner Antworten - widersprechen.

27. Register nach § 32 BDSG und Prüftätigkeit

27.1 Register und Meldepflicht

Die Aufsichtsbehörde führt nach § 38 Abs. 2 BDSG ein Register der Stellen, die personenbezogene Daten geschäftsmäßig zum Zwecke 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
203 Unternehmen gemeldet. Unterteilt nach der Art der meldepflichtigen Tätigkeit ergibt sich folgendes Bild:

Speicherung zum Zwecke der Übermittlung

Auskunfteien/Warndienste 8
Direktmarketing/Adreßhändler 29

Speicherung zum Zwecke der anonymisierten Übermittlung

Markt- und Meinungsforschung 12

Auftragsdatenverarbeitung

Servicerechenzentren 25
Akten- und Datenträgervernichter 14
Mikroverfilmer 5

Datenerfasser 20
sonst. Auftragsdatenverarbeitung 90

27.2 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 ..... -
Direktmarketing/Adreßhändler 11
Markt- und Meinungsforschung 2
Servicerechenzentren 5
Akten- und Datenträgervernichter 4
Mikroverfilmer ..... -
Datenerfasser ..... -
sonstige Auftragsdatenverarbeitung 23
gesamt 45

Im Rahmen dieser regelmäßigen Überwachung hat die Aufsichtsbehörde Hamburg ein Versicherungsunternehmen als Auftragsdatenverarbeiter eingehend geprüft. Dabei haben sich etliche Mängel ergeben, die zu Forderungen der Aufsichtsbehörde geführt haben.

Hervorzuheben ist insbesondere, daß dem betrieblichen Datenschutzbeauftragten von dem Unternehmen nicht ausreichend Zeit für die Erfüllung seiner Tätigkeit zur Verfügung gestellt wird. Dadurch wird der betriebliche Datenschutzbeauftragte ganz erheblich in der Wahrnehmung seiner nach § 37 BDSG vorgeschriebenen Aufgaben eingeschränkt. Beispielsweise war er bisher nicht in der Lage, seine Aufgaben zur Schulung und Auswahl von Mitarbeitern zu erfüllen. Darüber hinaus könnte es zu erheblichen Interessenkollisionen kommen, weil der betriebliche Datenschutzbeauftragte gleichzeitig Datenschutzbeauftragter mehrerer konzernverbundener Unternehmen ist, die zugleich Auftraggeber des Unternehmens sind.

Mängel haben sich auch bei den Verträgen ergeben, die zur Auftragsdatenverarbeitung gemäß § 11 BDSG zu schließen sind.

Aus datensicherheitstechnischer Sicht wurde das Verfahren zur Vergabe neuer Paßwörter sowie die unverschlüsselte Übertragung von sensiblen Versichertendaten (beispielsweise Gesundheitsdaten aus Lebensversicherungsverträgen) zwischen dem Rechenzentrum der Versicherung und den Geschäftsstellen kritisiert. Nicht zuletzt vor dem Hintergrund einer zunehmenden Nutzung von Wählnetzen sind personenbezogene Daten während der Übertragung nicht immer ausreichend geschützt. Dieses Risiko ist durch Einsatz kryptographischer Verfahren zu reduzieren, die seit einiger Zeit auf dem Markt einsatzreif verfügbar sind. Auf die Bedeutung von Verschlüsselungsverfahren haben die Datenschutzbeauftragten des Bundes und der Länder bereits in einer Entschließung im Mai 1996 hingewiesen.

Während die Entschließung der Datenschutzbeauftragten bereits im öffentlichen Bereich zu zahlreichen Verbesserungen geführt hat, sind nun verstärkt Unternehmen aufgefordert, personenbezogene Daten mehr als bisher verschlüsselt zu übertragen. Dies gilt auch für Versicherungen, die sensible Versichertendaten mehr als bisher vor mißbräuchlichem Zugriff schützen müssen.

Die geprüfte Versicherung hat zugesichert, im Rahmen der mittelfristig geplanten Neukonzeption ihres Geschäftsstellennetzes die Realisierung entsprechender Verschlüsselungsmechanismen eingehend zu prüfen.

Die Häufigkeit der bei den übrigen geprüften Unternehmen festgestellten Mängel ergibt sich aus der nachstehenden Übersicht:

Auftrag nach § 11 BDSG 13
Meldungen nach § 32 BDSG 12
Verpflichtung nach § 5 BDSG 10
Betrieblicher Datenschutzbeauftragter 10
Zugangssicherungsmaßnahmen 7
Paßwortregelungen und Zugriffsrechte 9
schriftliche Regelungen zum Umgang mit DV-Anlagen 3
sonstige technische und organisatorische Maßnahmen 3

Bei 7 Unternehmen brauchte die Aufsichtsbehörde keine Forderungen zu erheben.

Geschäftsverteilung (Stand: 13. Dezember 1997)

Der Hamburgische Datenschutzbeauftragte
Baumwall 7, 20459 Hamburg

Tel.: 040/3504-2044
BN: 9.41-2044
Fax: 040/3504-2372
BN: 9.41-2372

	Durchwahl
Dienststellenleiter: Dr. Hans-Hermann Schrader	-2044-
Stellvertreter: Peter Schaar	-2231-
Verwaltungsangelegenheiten der Dienststelle	-2223-
DV-Verfahren der Dienststelle	-2063-
Informationsmaterial	-2045- -2047-
Justiz, Strafvollzug, Verfassungsschutz, Meldewesen, Wahlen	-2046-
Polizei, Staatsanwaltschaft, Verkehrsverwaltung	-2581-
Bauverwaltung, Vermessungswesen, Personenstandswesen	-2223-
Telekommunikation, Medien, Ausländerwesen	-2231-
Finanz- und Steuerwesen, zentrale Informationstechnik (LIT)	-2236-
Betriebssysteme, Netzwerke, Chipkarten, Verschlüsselungstechnik	-2564-
Gesundheitswesen, Kultur	-2558-
Personalwesen, Gleichstellung, Archivwesen, Wirtschaftsverwaltung	-2562-
Soziales, medizinischer Arbeitsschutz, Hochschule, Schule und Berufsbildung	-2563-
Versicherungswirtschaft, Kreditwesen, Umwelt	-2556-
Auskunftteien, SCHUFA, Handel, Statistik	-2541-
Direktmarketing, Versandhandel, Wohnungswirtschaft, freie Berufe	-2089-
Markt- und Meinungsforschung, Mikroverfilmung, Aktenvernichtung, Beratung betrieblicher Datenschutzbeauftragter	-2468-

Stichwortverzeichnis

Veröffentlichungen zum Datenschutz

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

Broschüren

Hamburgisches Datenschutzrecht
Datenschutz in der Arztpraxis *
Mobilfunk und Datenschutz
Datenschutz bei Multimedia und Telekommunikation

Berichte und Dokumente

Bericht über den Datenschutz bei Automation und Vernetzung der hamburgischen Verwaltung - IuK-Datenschutzbericht -*

Informationsblätter

Tips zum Adressenhandel *
Datenschutz im privaten Bereich
Handels- und Wirtschaftsauskunfteien
Der betriebliche Datenschutzbeauftragte

Internet

Zu den Informationen des Hamburgischen Datenschutzbeauftragten im Internet - www.hamburg.de/Behoerden/HmbSDB - wird auf die Darstellung in diesem Tätigkeitsbericht (1.4.2) verwiesen.

Veröffentlichungen von Mitarbeitern

Unsere Mitarbeiter Herr Kühn und Herr Dr. Schläger haben das Buch "Datenschutz in vernetzten Computersystemen" im Datakontext-Fachverlag herausgegeben.

Varianten zur Selbstbestimmung

Selbst Selbstachtung Selbstanalyse Selbstanzeige Selbstauskunft Selbständigkeit Selbstbedienung Selbstbehauptung Selbstbeherrschung Selbstbeschränkung Selbstbesinnung Selbstbestätigung **Selbstbestimmung Selbstbestimmungsrecht** Selbstbeteiligung Selbstbetrug Selbstbewußtsein Selbstbezichtigung Selbstbindung Selbstdarstellung **Selbstdatenschutz** Selbstdisziplin Selbsteinschränkung Selbsteinschätzung Selbstentfaltung Selbsterfahrung Selbsterforschung Selbsterhaltung Selbsterkenntnis Selbstfindung Selbstgefühl Selbstherrlichkeit Selbsthilfe **Selbstinformation** Selbstkontrolle Selbstkritik Selbstlosigkeit Selbstmitleid Selbstorganisation Selbstüberprüfung Selbstregulierung Selbstsicherheit Selbstsucht Selbsttäuschung Selbstüberschätzung Selbstüberwindung **Selbstverantwortung** Selbstvergessenheit Selbstverpflichtung Selbstverständnis Selbstverteidigung Selbstvertrauen Selbstvervollkommnung Selbstverwaltung Selbstverwirklichung Selbstwahrnehmung Selbstwertgefühl Selbstzufriedenheit Selbstzweifel